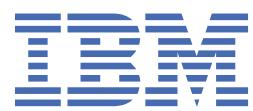


AIX Versión 7.2

*Gestión de red*



**Nota**

Antes de utilizar esta información y el producto al que hace referencia, lea la información del apartado “Avisos” en la página 793.

Esta edición se aplica a AIX Versión 7.2 y a todos los releases y modificaciones posteriores, a menos que se indique lo contrario en nuevas ediciones.

Copyright © 2011 IBM Corporation y sus licenciatarios, incluido Sendmail, Inc., y los Gerentes de University of California. Reservados todos los derechos.

© Copyright International Business Machines Corporation 2015, 2019.

# Contenido

<b>Acerca de este documento.....</b>	<b>vii</b>
Resaltado.....	vii
Distinción entre mayúsculas y minúsculas en AIX.....	vii
ISO 9000.....	vii
<b>Gestión de red.....</b>	<b>1</b>
Novedades.....	1
Conceptos de red y comunicación.	1
Redes físicas .....	3
Sistemas de red.....	4
Emuladores.....	5
Mandatos de red comunes.....	6
Gestión de correo.....	7
Programas agente de usuario de correo.....	8
Funciones de correo.....	11
Tareas de gestión de correo.....	45
Alias de correo.....	46
Cola de correo.....	48
Registro de correo.....	53
API de filtro de correo sendmail.....	55
Distintivos de depuración para sendmail.....	100
Internet Message Access Protocol y Post Office Protocol.....	101
Mandatos de gestión de correo .....	105
Archivos y directorios de correo.....	105
Mandatos de IMAP y POP.....	107
Protocolo de control de transmisiones/Protocolo Internet (Transmission Control Protocol/ Internet Protocol) .....	107
Terminología de TCP/IP.....	108
Planificación de la red TCP/IP .....	108
Instalación de TCP/IP.....	109
Configuración de TCP/IP.....	109
Autentificación y los rcmds seguros.....	112
Personalización de TCP/IP.....	114
Métodos para comunicarse con otros sistemas y usuarios.....	116
Transferencia de archivos.....	121
Impresión de archivos en un sistema remoto.....	125
Impresión de archivos de un sistema remoto.....	126
Visualización de información de estado.....	127
Protocolos TCP/IP.....	128
Tarjetas adaptadoras de red de área local TCP/IP.....	170
Interfaces de red TCP/IP.....	173
Direccionamiento TCP/IP.....	179
Resolución de nombres TCP/IP.....	184
Planificación y configuración para la resolución de nombres de LDAP (esquema de IBM SecureWay Directory).....	215
Planificación y configuración de la resolución de nombres NIS_LDAP (esquema RFC 2307).....	217
Asignación de direcciones y parámetros TCP/IP - Protocolo de configuración dinámica de sistemas principales.....	218
Protocolo de configuración dinámica de sistemas principales (Dynamic Host Configuration Protocol) versión 6 .....	321

Daemon DHCP de proxy de entorno de ejecución previa al arranque .....	347
Daemon de capa de negociación de imagen de arranque.....	390
Daemons TCP/IP.....	431
Direccionamiento TCP/IP.....	433
IPv6 móvil.....	443
Dirección IP virtual.....	446
EtherChannel, Agregación de enlaces IEEE 802.3ad, Teaming.....	449
Protocolo Internet a través de InfiniBand (IPoIB).....	471
Iniciador de software iSCSI y destino del software.....	474
Protocolo de transmisión de control de corriente (Stream Control Transmission Protocol).....	481
Descubrimiento de MTU de vía de acceso.....	486
Calidad de servicio de TCP/IP.....	487
Resolución de problemas de TCP/IP.....	497
Mandatos TCP/IP.....	507
Mandatos de transferencia de archivos.....	510
Mandatos de inicio de sesión remoto.....	511
Mandatos de estado.....	511
Mandato de comunicaciones remotas.....	511
Mandatos de impresión.....	511
Daemons TCP/IP.....	511
Métodos de dispositivo.....	513
Petición de comentarios.....	513
Programas de utilidad básicos de red (Basic Networking Utilities) .....	513
Cómo funciona BNU.....	514
Estructura de archivos y directorios en BNU.....	514
Configuración de BNU.....	517
Mantenimiento de BNU.....	530
Nombres de vías de acceso de BNU.....	533
Daemons de BNU.....	534
Seguridad en BNU.....	536
Comunicación entre sistemas locales y remotos.....	538
Intercambio de archivos entre sistemas locales y remotos.....	539
Informes sobre el estado de intercambios de mandatos y archivos.....	541
Intercambio de mandatos entre sistemas locales y remotos.....	542
Resolución de problemas en BNU.....	547
SNMP para gestión de red.....	552
SNMPv3.....	553
SNMPv1.....	571
Sistema de archivos de red.....	592
Servicios NFS.....	592
Soporte de Listas de control de acceso de NFS.....	593
Soporte de sistema de archivos de antememoria.....	594
Soporte de archivos correlacionados NFS.....	595
Servicio de proxy NFS.....	596
Tipos de montajes NFS.....	596
Exportación y montaje de NFS.....	597
Archivo /etc(exports.....	599
Archivo /etc/xtab.....	600
Archivo /etc/nfs/hostkey.....	600
Archivo /etc/nfs/local_domain.....	600
Archivo /etc/nfs/realm.map.....	600
Archivo /etc/nfs/princmap.....	600
Archivo /etc/nfs/security_default.....	600
Protocolo de llamada a procedimiento remoto.....	601
Protocolo eXternal Data Representation.....	601
Daemon portmap.....	601
Aplicaciones y control de NFS.....	601
Soporte de NFS versión 4.....	604

Periodo de gracia del servidor NFS.....	604
Soporte DIO y CIO de NFS.....	605
Duplicación NFS y espacio de nombres global.....	606
Delegación de servidor-cliente NFS.....	612
Sistemas de archivos de red a corto plazo STNFS.....	614
Lista de comprobación para configurar NFS.....	615
Iniciar los daemons NFS en el arranque de sistema.....	615
Configuración de un servidor NFS.....	616
Configuración de un cliente NFS.....	616
Correlación de identidad.....	617
Exportación de un sistema de archivos NFS.....	617
Configuración de una red para RPCSEC-GSS.....	618
Eliminación de la exportación de un sistema de archivos NFS.....	621
Cambio de un sistema de archivos exportado.....	622
Acceso de usuario root a un sistema de archivos exportado.....	622
Montaje explícito de un sistema de archivos NFS.....	623
Subsistema automount.....	624
Establecimiento de montajes NFS predefinidos.....	625
Desmontaje de un sistema de archivos montado explícita o automáticamente.....	631
Eliminación de montajes NFS predefinidos.....	631
PC-NFS.....	631
Correlaciones de montaje automático de LDAP.....	633
WebNFS.....	634
Gestor de bloqueos de red.....	635
Seguridad de NFS.....	638
Resolución de problemas de NFS.....	638
Archivos NFS.....	647
Mandatos NFS.....	648
NFS, daemons.....	649
Subrutinas NFS.....	650
Protocolo SMB.....	650
Sistema de archivos de bloque de mensajes de servidor.....	650
Sistema de archivos de cliente SMB (Server Message Block).....	653
Comunicaciones asíncronas.....	658
Velocidades de línea no POSIX.....	659
Adaptadores asíncronos.....	660
Opciones de comunicaciones asíncronas.....	660
Consideraciones para la selección de un producto.....	662
Consideraciones topológicas.....	665
Comunicación serie.....	665
Dispositivo de terminal TTY.....	671
Módems .....	682
Opciones de terminal stty-cxma.....	704
Subsistema del protocolo PPP (Point-to-Point Protocol) asíncrono.....	707
Serial Line Internet Protocol (SLIP).....	710
Asynchronous Terminal Emulation.....	724
Programa de utilidad de pantalla dinámica.....	739
Controlador del dispositivo Serial over Ethernet.....	745
Entorno de control genérico de enlace de datos.....	749
Criterios de GDLC.....	751
Interfaz GDLC.....	751
Controles de enlace de datos GDLC.....	752
Operaciones de punto de entrada ioctl de interfaz GDLC.....	752
Servicios del kernel especiales de GDLC.....	755
Gestión de controladores de dispositivos DLC.....	756
Consulta de los adaptadores de comunicaciones y redes.....	757
Adaptadores PCI.....	758
Adaptadores asíncronos.....	759

uDAPL (user-level Direct Access Programming Library).....	784
API de uDAPL compatibles con AIX.....	784
Atributos específicos del proveedor para uDAPL.....	785
Soporte para el adaptador RoCE PCIe2 de 10 GbE.....	786
NIC + OFED RDMA de AIX .....	787
RoCE de AIX.....	789
Soporte al adaptador RoCE PCIe3 40 GbE.....	790
<b>Avisos.....</b>	<b>793</b>
Consideraciones de la política de privacidad.....	794
Marcas registradas.....	795
<b>Índice.....</b>	<b>797</b>

# Acerca de este documento

---

Este documento proporciona a los programadores de aplicaciones información completa sobre cómo habilitar aplicaciones para la globalización para el sistema operativo AIX. También proporciona a los administradores de sistemas información completa sobre cómo habilitar entornos en red para la globalización para el sistema operativo AIX. Los programadores y administradores de sistemas pueden utilizar este manual para obtener conocimientos sobre las directrices y principios de globalización. Los temas incluyen entornos locales, conjuntos de códigos, subrutinas, convertidores, correlación de caracteres, información específica del entorno cultural y recurso de mensajes.

## Resaltado

---

En este documento se utilizan los convenios de resaltado de texto siguientes:

Item	Descripción
<b>Negrita</b>	Identifica mandatos, subrutinas, palabras clave, archivos, estructuras, directorios y otros elementos cuyos nombres están predefinidos en el sistema. También identifica objetos gráficos como, por ejemplo, botones, etiquetas e iconos que el usuario selecciona.
<i>Cursiva</i>	Identifica parámetros cuyos nombres o valores reales debe suministrar el usuario.
Monoespaciado	Identifica ejemplos de determinados valores de datos, ejemplos de texto parecido al que aparece, ejemplos de partes de código de programa parecidas a las que escribiría un programador, mensajes del sistema o información que debe escribir el usuario.

## Distinción entre mayúsculas y minúsculas en AIX

---

En el sistema operativo AIX todo es sensible a las mayúsculas y minúsculas, lo que significa que establece una distinción entre las letras en mayúsculas y en minúsculas. Por ejemplo, puede utilizar el mandato **ls** para listar archivos. Si escribe LS, el sistema responderá que no se encuentra el mandato. Asimismo, **FILEA**, **FiLea** y **filea** son tres nombres de archivos distintos, aunque residan en el mismo directorio. Para evitar que se produzcan acciones no deseadas, no olvide nunca de emplear las mayúsculas y minúsculas adecuadas.

## ISO 9000

---

En el desarrollo y la fabricación de este producto se han utilizado sistemas de calidad registrados que cumplen la norma ISO 9000.



# Gestión de red

Esta colección de temas ayuda a los administradores de sistemas y a los usuarios a realizar una serie de tareas de comunicación en la red. Los administradores de sistemas pueden hallar en esta colección de temas información sobre cómo realizar tareas como, por ejemplo, configurar los valores de TCP/IP, mejorar la seguridad de la red y supervisar el sistema. Los usuarios pueden hallar información completa sobre cómo realizar tareas como, por ejemplo, utilizar aplicaciones de comunicaciones y servicios para el sistema operativo.

## Novedades en la gestión de red

Conozca la información nueva o a la que se han aplicado modificaciones importantes para la recopilación de temas sobre gestión de redes.

### Cómo ver las novedades o las modificaciones

Para ayudarle a ver dónde se han realizado cambios técnicos, el centro de información utiliza:

- La imagen >| señala el lugar en el que empieza la información nueva o cambiada.
- La imagen |< señala el lugar en el que acaba la información nueva o cambiada.

### Noviembre 2020

La siguiente información es un resumen de las actualizaciones realizadas a esta colección de temas:

- Se ha añadido información sobre la tecnología de agregación **Teaming** en el tema “[EtherChannel, Agregación de enlaces IEEE 802.3ad, Teaming](#)” en la página 449.

### Noviembre 2019

La siguiente información es un resumen de las actualizaciones realizadas a esta colección de temas:

- Se ha añadido información sobre el archivo `submit.cf` en los temas siguientes:
  - [“Gestión de correo”](#) en la página 7
  - [“Archivos y directorios de correo”](#) en la página 105
  - [“Inicio del daemon sendmail durante el arranque del sistema”](#) en la página 46
- Se ha añadido información sobre el [“Controlador del dispositivo Serial over Ethernet”](#) en la página 745. Puede utilizar un Ethernet Device Server (EDS) para crear un dispositivo serie virtual y dispositivos teletipo en las particiones lógicas de AIX.
- En los temas siguientes, se ha añadido información sobre la compatibilidad con varios iniciadores de software iSCSI:
  - [“Configuración de varios dispositivos de iniciador de software iSCSI”](#) en la página 477
  - [“Configuración del iniciador de software iSCSI”](#) en la página 475

## Conceptos de red y comunicación

Esta información está pensada para los administradores del sistema, que no están familiarizados con los principios generales de red. Si está familiarizado con la red de UNIX, puede omitir esta información.

Una red es la combinación de dos o más sistemas y los enlaces de conexión de los mismos. Una red *física* es el hardware (equipo como adaptadores, cables y líneas de teléfono) que compone la red. El software y el modelo conceptual componen la red *lógica*. Existen distintos tipos de redes y emuladores que proporcionan funciones diferentes.

La complejidad de las redes de sistemas modernas ha dado origen a varios modelos conceptuales para explicar cómo funcionan las redes. Entre estos modelos, uno de los más comunes es el Modelo de referencia OSI (Open Systems Interconnection - Interconexión de sistemas abiertos) de la International Standards Organization (Organización internacional para los estándares), que también se conoce como modelo de siete capas OSI.

Las siete capas del modelo OSI se describen del modo siguiente:

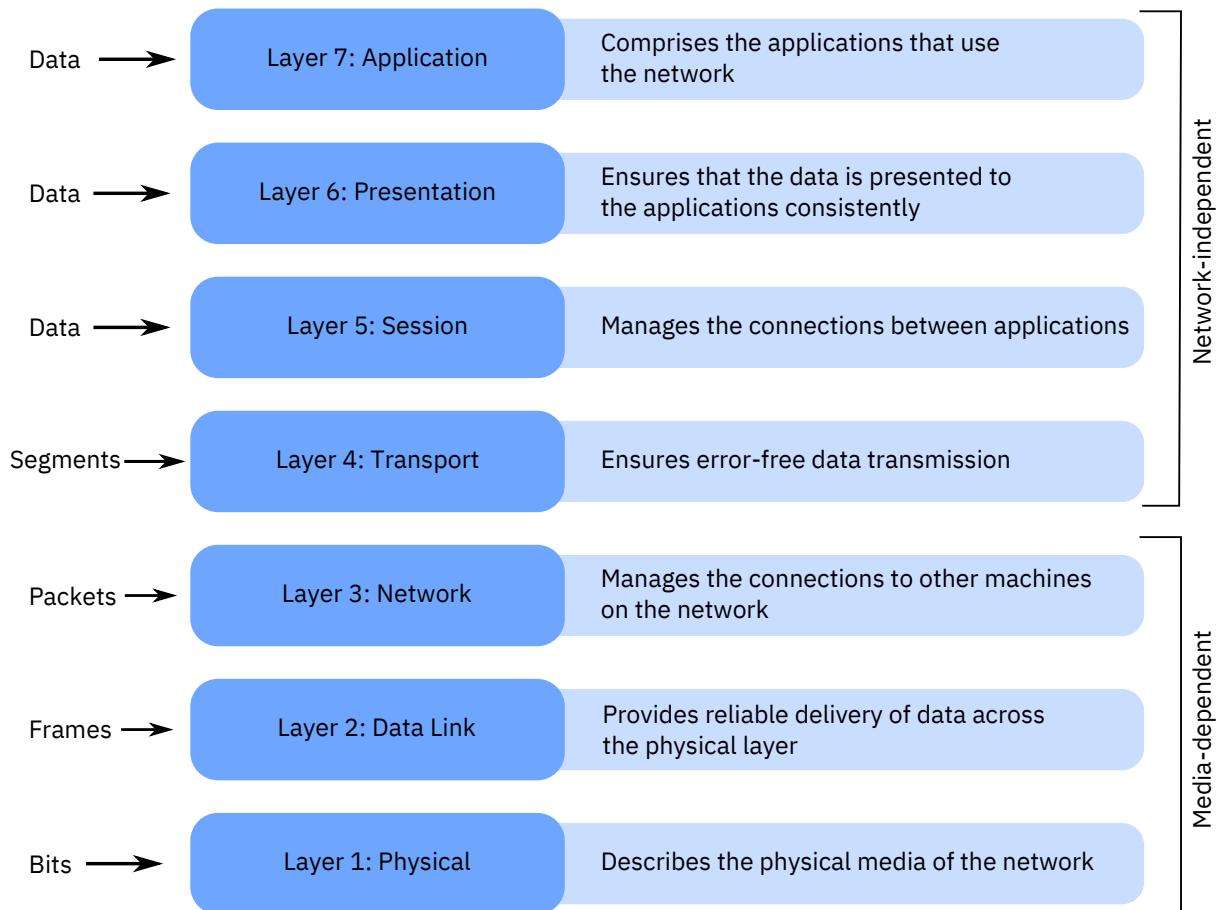


Figura 1. Modelo de referencia OSI

**Nota:** Mientras que el Modelo de referencia OSI es útil para describir conceptos de red, muchos protocolos de red no siguen exactamente el modelo OSI. Por ejemplo, al describir TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet), las funciones de las capas de Aplicación y Presentación se combinan, igual que se combinan las capas de Sesión y de Transporte y las capas de Enlace de datos y Física.

Las redes permiten varias funciones de comunicaciones de aplicaciones y de usuarios, por ejemplo:

#### Enviar correo electrónico

Puede enviar un mensaje a otro usuario. Los dos usuarios pueden encontrarse en el mismo sistema, en sistemas distintos en edificios distintos o incluso en países distintos. Las capas subyacentes de software y hardware, así como la red física, hacen posible que el usuario pueda generar, enviar, recibir y procesar mensajes, cartas, memorándums, invitaciones y archivos de datos. Esta comunicación puede establecerse con cualquier otro usuario que resida en la red física.

#### Emular otro terminal o iniciar la sesión en otro sistema

A través de una red de comunicaciones, un sistema puede emular o imitar a otro y acceder a la información como si se tratase de un tipo de sistema o terminal distinto. El inicio de sesión remoto proporciona a los usuarios una interfaz de línea de mandatos interactiva para iniciar la sesión en un sistema remoto y acceder a los mismos programas y archivos que si estuvieran utilizando la máquina de forma local.

## **Transferir datos**

Puede transferir datos de un sistema a otro. Es posible migrar archivos, directorios y sistemas de archivos completos de una máquina a otra a través de una red, lo que permite realizar copias de seguridad remotas de los datos y garantiza la redundancia en caso de que se produzca una anomalía en la máquina. La protección con contraseña suele proporcionarse como parte del protocolo. A menudo, el protocolo de transferencia de archivos incluye funciones de visualización y de control que permiten a los usuarios con acceso de lectura/grabación visualizar, definir o suprimir archivos y directorios.

## **Ejecutar programas que residen en un nodo remoto**

Existen distintos protocolos que permiten a los usuarios y a las aplicaciones de un sistema invocar procedimientos y aplicaciones de otros sistemas. Esto puede resultar muy útil en numerosos entornos, además de que supone la descarga de una gran cantidad de rutinas de amplia utilización del sistema en las aplicaciones científicas y de ingeniería.

## **Entrada de datos**

La entrada de datos consiste en entrar datos directamente en los archivos de datos locales o remotos. El incremento de precisión y de eficiencia es la consecuencia natural de una transferencia de datos de un solo paso.

## **Consultas de datos**

Las consultas de datos obligan a buscar en los archivos de datos la información especificada. La actualización de datos implica la modificación, adición o supresión de datos almacenados en los archivos locales o remotos.

## **Entrada de proceso por lotes remota**

La entrada de proceso por lotes remota consiste en entrar lotes de datos desde una ubicación remota, actividad que normalmente se realiza por la noche o durante períodos de poca utilización del sistema. Debido a la diversidad de posibilidades, las comunicaciones y las redes no son sólo deseables sino necesarias.

## **Compartimiento de recursos**

El compartimiento de recurso es otra función de las redes. Los usuarios pueden compartir datos así como programas, espacio de almacenamiento de archivos y dispositivos periféricos tales como impresoras, módems, terminales y discos duros.

## **Compartimiento de datos**

El compartimiento de recursos del sistema es efectivo en la reducción de costes porque elimina los problemas de conservación de varias copias de programas y conserva la coherencia de los datos (en el caso de compartimiento de programas y archivos).

## **Comunicaciones con otros sistemas operativos**

Una red puede tener conectados distintos tipos de sistemas. Los sistemas pueden ser de fabricantes diferentes o ser modelos diferentes del mismo fabricante. Los programas de comunicaciones subsanan las diferencias entre los sistemas operativos de dos o más tipos de sistemas. A veces estos programas requieren que se haya instalado anteriormente otro programa en la red. Otros programas pueden necesitar que existan en la red determinados protocolos de conectividad de comunicaciones, por ejemplo TCP/IP o SNA (Systems Network Architecture).

## **Redes físicas**

La red física consta de los cables (cable coaxial, par trenzado, fibra óptica y líneas telefónicas) que conectan el distinto hardware que reside en la red, el adaptador utilizado en los sistemas conectados a la red (sistemas principales) y los concentradores, repetidores, direccionadores o puentes utilizados en la red.

Las redes físicas varían en el tamaño y en el tipo de hardware utilizado. Las dos clases comunes de redes son las *redes de área local* (LAN) y las *redes de área amplia* (WAN). Una LAN es una red donde las comunicaciones están limitadas a una área geográfica de tamaño moderado de 1 a 10 km (1 a 6 millas), por ejemplo un solo edificio de oficinas, almacén o recinto universitario. Una WAN es una red que proporciona la posibilidad de comunicaciones de datos en áreas geográficas mayores que las atendidas por las LAN, por ejemplo en todo un país o entre continentes. También existe una clase intermedia de

redes, denominadas *redes de área metropolitana* (MAN). En general en esta guía no se distinguen las MAN; se agrupan con las WAN.

Normalmente las LAN utilizan hardware de Ethernet estándar, Ethernet IEEE 802.3 o de Red en anillo para la red física, mientras que las WAN y las redes asíncronas utilizan las redes de comunicaciones proporcionadas por las empresas portadoras comunes. El funcionamiento de la red física en ambos casos lo suelen controlar los estándares de red de organizaciones tales como EIA (Electronics Industry Association) o ITU (International Telecommunication Union).

## Sistemas de red

Todas las comunicaciones de red implican el uso de hardware y software. El soporte de comunicaciones de red lo determinan el hardware y el software necesarios para ejecutar dicho hardware y para intercambiar información con la red.

El *hardware* consta del equipo físico conectado a la red física. El *software* consta de los programas y los controladores de dispositivo asociados con el funcionamiento de un sistema determinado. El hardware de sistema consta de adaptadores o de otros dispositivos que proporcionan una vía de acceso o una interfaz entre el software de sistema y la red física. Un *adaptador* requiere una tarjeta de E/S en el sistema. Un adaptador prepara todos los datos de entrada y de salida; efectúa las búsquedas de direcciones; proporciona controladores, receptores y protección frente a sobrecargas; da soporte a distintas interfaces y, en general, exime al procesador del sistema de la mayoría de las tareas relacionadas con las comunicaciones.

Los términos siguientes se utilizan en toda la información de gestión de red:

### Protocolos

Los protocolos son conjuntos de reglas semánticas y sintácticas que definen cómo se entrega la información, cómo se adjunta para que alcance su destino de forma segura y la vía de acceso que sigue. Los protocolos también coordinan el flujo de mensajes y los acuses de recibo.

### Direcciones

Un dominio de red es una agrupación administrativa de varias redes de sistemas o hosts dentro de la misma infraestructura. Los dominios ponen los recursos de proceso de datos en una red bajo un control común.

Por ejemplo, la estructura de Internet ilustra cómo los dominios definen la dirección IP (Protocolo Internet). Internet es una extensa red compuesta por muchas redes distintas más pequeñas. Para facilitar las rutas y el direccionamiento, las direcciones de internet se estructuran jerárquicamente en dominios, con categorías muy amplias en la parte superior, por ejemplo com para usuarios de comercio, edu para usuarios de enseñanza y gov para usuarios del gobierno. En el dominio com hay muchos dominios más pequeños correspondientes a empresas individuales; por ejemplo ibm. En el dominio ibm.com hay incluso dominios más pequeños, correspondientes a las direcciones de Internet de distintas ubicaciones, por ejemplo austin.ibm.com oaleigh.ibm.com. En este nivel, puede identificar nombres de hosts. En este contexto, un sistema principal es cualquier sistema conectado a la red. En austin.ibm.com, es posible que haya sistemas principales con los nombres hamlet y lear, con las direcciones hamlet.austin.ibm.com y lear.austin.ibm.com.

### Pasarelas y puentes

En internet residen una gran variedad de redes, que normalmente utilizan distinto hardware y ejecutan distinto software. Las pasarelas y los puentes permiten a estas distintas redes comunicarse entre sí. Un puente es una unidad funcional que conecta dos LAN que posiblemente utilizan el mismo procedimiento de control de enlace lógico (LLC), por ejemplo Ethernet, pero diferentes procedimientos de control de accesos al medio (MAC). Una pasarela tiene un rango más amplio que un puente. Opera por encima de la capa de enlace y, cuando es necesario, convierte la interfaz y el protocolo utilizados por una red en los utilizados por otra red distinta. Las pasarelas permiten las transferencias de datos entre las diversas redes que constituyen Internet.

### Direccionamiento de datos

La utilización de nombres de dominio para el direccionamiento y de pasarelas para la conversión facilita en gran medida el direccionamiento de los datos que se están transfiriendo. El direccionamiento es la asignación de una vía de acceso por la que un mensaje alcanza su destino. El nombre de dominio define de forma efectiva el destino de mensaje. En una red grande como Internet,

la información se direcciona de una red de comunicaciones a la siguiente hasta que llega a su destino. Cada red de comunicaciones comprueba el nombre de dominio y, basándose en los dominios con los que la red está familiarizada, direcciona la información hasta la siguiente detención lógica. De este modo, cada red de comunicaciones que recibe los datos contribuye al proceso de direccionamiento.

### Nodos locales y remotos

Una red física la utilizan los sistemas principales que residen en dicha red. Cada sistema principal es un nodo de la red. Un nodo es una ubicación direccionable de una red de comunicaciones que proporciona servicios de proceso de sistema principal. Las intercomunicaciones de estos diversos nodos se definen como locales o remotas. *Local* pertenece a un dispositivo, archivo o sistema al que se accede directamente desde el sistema, sin utilizar una línea de comunicaciones. *Remoto* pertenece a un dispositivo, archivo o sistema al que el sistema accede a través de una línea de comunicaciones. Los archivos locales residen en el sistema, mientras que los archivos remotos residen en un servidor de archivos o en otro nodo con el que se comunica utilizando una red física, por ejemplo Ethernet, Red en anillo o línea telefónica.

### Cliente y servidor

Un servidor es un sistema que contiene datos o proporciona recursos a los que deben acceder otros sistemas de la red. Un cliente es un sistema que solicita servicios o datos de un servidor. Los tipos de servidor comunes son servidores de archivos que almacenan archivos, servidores de nombres que almacenan nombres y direcciones, servidores de aplicaciones que almacenan programas y aplicaciones y servidores de impresión que planifican y dirigen los trabajos de impresión al destino.

Un cliente puede solicitar código de programa actualizado o el uso de aplicaciones de un servidor de código. Para obtener un nombre o una dirección, un cliente se pone en contacto con un servidor de nombres. Un cliente también puede solicitar archivos y datos para la entrada de datos, las consultas o la actualización de registros de un servidor de archivos.

## Emuladores

Un *emulador* es una aplicación de software que permite al sistema funcionar como si se estuviera utilizando un terminal o una impresora diferente. Un *emulador de terminal* se conecta a un sistema principal para acceder a los datos o las aplicaciones. Algunos de estos emuladores proporcionan un recurso para transferir archivos con el sistema principal. Otros facilitan una interfaz de programas de aplicación (API) que hace posible la comunicación entre programas y la automatización de tareas del sistema principal. Un *emulador de impresora* permite al sistema principal imprimir archivos en una impresora local o almacenarlos en formato imprimible para imprimirlos o editarlos posteriormente.

### Mandatos TCP/IP para emulación

El software TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet) incluye los mandatos **telnet** y **rlogin**, que le permiten conectarse y acceder a un sistema TCP/IP remoto.

Item	Descripción
<b>telnet</b>	Permite a un usuario iniciar la sesión en un sistema principal remoto implementando el protocolo <b>TELNET</b> . Se diferencia del mandato <b>rlogin</b> en que es un mandato autorizado. Un mandato <i>autorizado</i> es aquél que cumple todos los niveles de seguridad configurados en el sistema. Los sistemas que necesitan seguridad adicional solamente deben ejecutar mandatos autorizados. El Departamento de Defensa de EE.UU. es el encargado de definir y mantener los estándares de los programas, procesos y mandatos autorizados.
<b>tn</b>	Realiza la misma función que el mandato <b>telnet</b> .
<b>rlogin</b>	Permite a un usuario iniciar la sesión en un sistema principal remoto. Es diferente del mandato <b>telnet</b> en que se trata de un mandato <i>no autorizado</i> y puede inhabilitarse si el sistema necesita seguridad adicional.

Para obtener más información sobre **TCP/IP**, consulte el apartado “Protocolo de control de transmisiones/Protocolo Internet (Transmission Control Protocol/Internet Protocol)” en la página 107.

**Nota:** El mandato **bterm** emula terminales en modalidad bidireccional (bidi).

### Mandatos BNU para emulación

El software BNU (Programas de utilidad básicos de red) incluye los mandatos **ct**, **cu** y **tip**, que le permiten conectarse a un sistema remoto que utilice el sistema operativo AIX.

Item	Descripción
<b>ct</b>	Permite a un usuario de un terminal remoto, por ejemplo un 3161, comunicarse con otro terminal a través de una línea telefónica. De este modo, el usuario del terminal remoto puede iniciar la sesión y trabajar en el otro terminal.  El mandato <b>ct</b> es similar al mandato <b>cu</b> pero no es tan flexible. Por ejemplo, no puede emitir mandatos en el sistema local mientras está conectado a un sistema remoto mediante el mandato <b>ct</b> . Sin embargo, puede indicar al mandato <b>ct</b> que continúe marcando hasta que se establezca la conexión o especificar más de un número de teléfono a la vez.
<b>cu</b>	Conecta el terminal a otro terminal conectado a un sistema UNIX o que no sea UNIX.  Una vez establecida la conexión, puede estar conectado en ambos sistemas al mismo tiempo, ejecutando mandatos en cualquiera de los dos sin desactivar el enlace de comunicaciones BNU. Si el terminal remoto también se está ejecutando bajo UNIX, puede transferir archivos ASCII entre los dos sistemas. También puede utilizar el mandato <b>cu</b> para conectar varios sistemas permitiendo de este modo que se puedan ejecutar mandatos en cualquiera de los sistemas conectados.
<b>tip</b>	Conecta el terminal a un terminal remoto y permite trabajar en el terminal remoto como si estuviera conectado directamente.  Puede utilizar el mandato <b>tip</b> para transferir archivos al sistema remoto y desde dicho sistema. Puede utilizar archivos script para registrar las conversaciones que mantiene con el mandato <b>tip</b> .

**Nota:** Para utilizar el mandato **tip** debe haber iniciado una sesión en el sistema remoto.

Para obtener más información sobre BNU, consulte el “[Programas de utilidad básicos de red \(Basic Networking Utilities\)](#)” en la página 513.

### Mandatos de red comunes

Utilice los mandatos siguientes para visualizar información básica sobre los usuarios, los sistemas y el registro.

Tabla 1. Mandatos de comunicación utilizados habitualmente	
Mandato	Descripción
<a href="#">whoami</a>	Muestra el nombre de inicio de sesión.
<a href="#">uname</a>	Muestra el nombre del sistema si el sistema está en una red.

Tabla 1. Mandatos de comunicación utilizados habitualmente (continuación)

Mandato	Descripción
<b>host</b> <i>nombre_sistema</i>	<p>Determina si el sistema local tiene acceso al sistema especificado.</p> <pre># host nombre_sistema</pre> <p>Si el sistema tiene la información adecuada, se devuelve una salida similar a la siguiente:</p> <pre>&lt;nombre_sistema&gt; es 192.9.200.4 (300,11,310,4)</pre> <p>A continuación, puede enviar un mensaje al sistema. El sistema utiliza la dirección 192.9.200.4 para direccionar el correo. Si el sistema carece de la información, se devuelve una salida similar a la siguiente:</p> <pre>&lt;nombre_sistema&gt;: host desconocido</pre>
<b>finger</b> <i>nombre_sistema</i>   <i>nombre_usuario</i>	<p>Muestra los usuarios que tienen una sesión iniciada en un sistema o host específico o información sobre un usuario específico.</p> <pre># finger nombre_sistema</pre> <p>Se devuelve una salida similar a la siguiente:</p> <pre>bosch    Consola Mar 15 13:19 valle    pts0      Mar 15 13:01 marin   tty0      Mar 15 13:01</pre> <pre>finger brown@&lt;nombre_sistema&gt;</pre> <p>O</p> <pre>finger bosch</pre> <p>Se devuelve una salida similar a la siguiente:</p> <pre>Nombre de inicio de sesión: bosch En la vida real: Marta Bosch Directorio:/home/bosch    Shell: /bin/ksh Activo desde May 8 07:13:49 en consola Sin planificación.</pre>

Están disponibles varias aplicaciones para permitir al sistema emular otros tipos de terminales.

## Gestión de correo

El recurso de correo proporciona un método para intercambiar correo electrónico con usuarios del mismo sistema o de varios sistemas conectados por una red. Aquí se describen el sistema de correo, la interfaz de usuario de correo estándar, el **IMAP (Internet Message Access Protocol)** y el **POP (Post Office Protocol)**.

El sistema de correo es un recurso de entrega de correo entre redes que consta de una interfaz de usuario, un programa de direccionamiento de mensajes y un programa de entrega de mensajes (o programa de correo). El sistema de correo transmite mensajes de un usuario a otro en el mismo sistema principal, entre sistemas principales y a través de límites de red. También realiza una cantidad limitada de edición de cabeceras de mensajes para poner el mensaje en un formato que sea apropiado para el sistema principal de recepción.

Una *interfaz de usuario* de correo permite a los usuarios crear y enviar mensajes a otros usuarios y recibir mensajes de esos otros usuarios. El sistema de correo proporciona dos interfaces de usuario, **mail** y **mhmail**. El mandato **mail** es una interfaz de usuario de correo estándar disponible en todos los sistemas UNIX. El mandato **mhmail** es la interfaz de usuario de MH (Message Handler - Manejador de mensajes), una interfaz de usuario de correo ampliada diseñada para usuarios expertos.

Un *programa de direccionamiento de mensajes* direcciona los mensajes a los destinos. El programa de direccionamiento de mensajes del sistema de correo es el programa **sendmail**, que forma parte del BOS (Base Operating System - sistema operativo base) y se instala con el BOS. El programa **sendmail** es un daemon que utiliza información del archivo de configuración `/etc/mail/sendmail.cf` o `/etc/mail/submit.cf`, y del archivo `/etc/mail/aliases` para realizar el direccionamiento necesario.

En función del tipo de ruta al destino, el mandato **sendmail** utiliza diferentes *programas de correo* para entregar los mensajes.

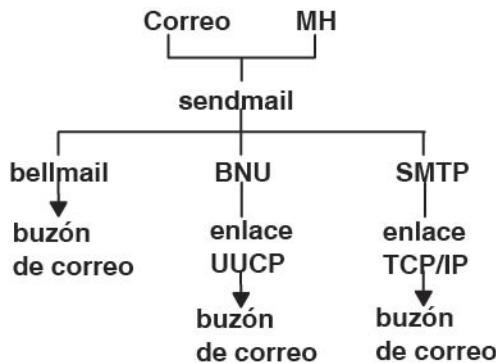


Figura 2. Programas de correo utilizados por el mandato **sendmail**

Esta ilustración es un tipo de gráfico de organización de arriba a abajo con Mail y MH en la parte superior. Las ramificaciones de éstos son bellmail, BNU y SMTP. Debajo del nivel anterior están el buzón local, el enlace UUCP y el enlace **TCP/IP** respectivamente. Debajo del enlace UUCP está el buzón remoto y bajo el enlace **TCP/IP** está el buzón remoto.

Como ilustra la figura:

- Para entregar correo local, el programa **sendmail** direcciona los mensajes al programa **bellmail**. El programa **bellmail** entrega todo el correo local añadiendo mensajes al buzón del sistema del usuario, que está en el directorio `/var/spool/mail`.
- Para entregar correo a través de un enlace UUCP (UNIX-to-UNIX Copy Program - Programa de copia de UNIX a UNIX), el programa **sendmail** direcciona los mensajes utilizando BNU (Basic Network Utilities - Programas de utilidad básicos de red).
- Para entregar el correo direccionado a través de **TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet)**, el mandato **sendmail** establece una conexión **TCP/IP** al sistema remoto y, a continuación, utiliza **SMTP (Simple Mail Transfer Protocol - Protocolo simple de transferencia de correo)** para transferir el mensaje al sistema remoto.

## Programas agente de usuario de correo

Para poder utilizar el sistema de correo, deberá seleccionar un programa agente de usuario. Puede utilizar un programa de correo (**mail**), el manejador de mensajes (**mh**) o el mandato **bellmail**.

Un programa agente de usuario proporciona recursos para crear, recibir, enviar y archivar correo. Además, necesitará un programa agente de transporte, **sendmail**, que distribuye el correo de entrada procedente de otros sistemas o paquetes y distribuye cada elemento del correo de salida y luego lo transmite a un programa similar en uno o más sistemas remotos.

**Nota:** Los programas **mail** y **mh** son incompatibles en el modo en que almacenan el correo; deberá elegir uno de estos manejadores de correo.

### **Interfaz de programa de correo (mail)**

El programa **mail** le proporciona una interfaz de usuario para manejar el correo entre un usuario de red local y un usuario de sistema remoto.

Un mensaje de correo puede ser texto, entrado utilizando un editor, o un archivo ASCII. Además de un mensaje escrito o un archivo, también puede enviar:

<b>Item</b>	<b>Descripción</b>
<b>mensaje del sistema</b>	Informa a los usuarios de la actualización del sistema. Un mensaje del sistema es parecido a un mensaje de difusión general, aunque en este caso sólo se envía en la red local.
<b>correo secreto</b>	Se utiliza para enviar información confidencial. Los mensajes de correo secretos están cifrados. El destinatario debe entrar una contraseña para poder leerlos.
<b>mensaje de vacaciones</b>	Informa a los usuarios de que está ausente por vacaciones. Cuando el sistema recibe correo durante su ausencia, éste reenvía un mensaje al origen. En este mensaje se indica que usted está de vacaciones. Todos los mensajes de correo que se reciban mientras esté de vacaciones también pueden reenviarse.

Cuando reciba correo utilizando los submandatos de **mail**, puede:

- Dejar el correo en el buzón del sistema.
- Leer y suprimir el correo.
- Reenviar el correo.
- Añadir comentarios al correo.
- Almacenar el correo en el buzón personal (mbox).
- Almacenar el correo en una carpeta que ha creado.
- Crear y mantener un archivo de alias o un archivo de distribución que dirija el correo y los mensajes de correo.

La instalación de **sendmail** es automática.

Para obtener más información sobre el programa **mail**, consulte el apartado “[Funciones de correo](#)” en la página 11.

### **Manejador de mensajes (mh)**

El programa mh es un conjunto de mandatos que le permite realizar cada función de proceso de correo directamente desde la línea de mandatos.

Estos mandatos proporcionan un rango más amplio de funciones que los submandatos de **mail**. Además, debido a que se pueden emitir en cualquier momento en que se visualiza el indicador de mandatos, se obtiene una mayor eficacia y flexibilidad a la hora de crear correo y de procesar el correo recibido. Por ejemplo, puede leer un mensaje de correo, buscar un archivo o ejecutar un programa para hallar una solución en concreto; así como responder al mensaje, y todo desde el mismo shell.

El programa **mh** le permite crear, distribuir, recibir, ver, procesar y almacenar mensajes utilizando los mandatos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>ali</b>	Lista los alias y sus direcciones.
<b>anno</b>	Anota los mensajes.
<b>ap</b>	Analiza y modifica el formato a las direcciones.
<b>burst</b>	Separa digests en mensajes.
<b>comp</b>	Inicia un editor para la creación o modificación de un mensaje.

<b>Item</b>	<b>Descripción</b>
<b>dist</b>	Redistribuye un mensaje entre direcciones adicionales.
<b>dp</b>	Analiza y modifica el formato a las fechas.
<b>folder</b>	Selecciona y lista carpetas y mensajes.
<b>folders</b>	Lista todas las carpetas y mensajes del directorio de correo.
<b>forw</b>	Reenvía mensajes.
<b>inc</b>	Incorpora el correo nuevo a una carpeta.
<b>mark</b>	Crea, modifica y visualiza secuencias de mensajes.
<b>mh1</b>	Produce un listado de mensajes con formato.
<b>mhmail</b>	Envía o recibe correo.
<b>mhpath</b>	Imprime los nombres de vía de acceso completos de mensajes y carpetas.
<b>msgchk</b>	Comprueba los mensajes.
<b>msh</b>	Crea un shell de manejador de correo (mh).
<b>next</b>	Muestra el siguiente mensaje.
<b>packf</b>	Comprime el contenido de una carpeta en un archivo.
<b>pick</b>	Selecciona mensajes por el contenido y crea y modifica secuencias.
<b>prev</b>	Muestra el mensaje anterior.
<b>refile</b>	Mueve archivos entre carpetas.
<b>repl</b>	Responde a un mensaje.
<b>rmf</b>	Elimina carpetas y los mensajes que contienen.
<b>rmm</b>	Elimina mensajes del estado activo.
<b>scan</b>	Produce un listado explorable de una línea por mensaje.
<b>send</b>	Envía un mensaje.
<b>show</b>	Muestra mensajes.
<b>sortm</b>	Clasifica mensajes.
<b>vmh</b>	Inicia una interfaz visual para utilizarla con mandatos de mh.
<b>whatnow</b>	Inicia una interfaz de solicitud para la disposición de borrador.
<b>whom</b>	Manipula direcciones de mh.

### **Mandato bellmail**

El mandato **bellmail** es el mandato de correo original AT&T UNIX, que maneja correo para usuarios del mismo sistema y también para usuarios de sistemas remotos a los que se puede acceder por medio de BNU (Basic Network Utilities), que a veces se conoce como UUCP (UNIX-to-UNIX Copy Program - Programa de copia de UNIX a UNIX).

Estos programas sólo soportan redes de sistemas conectados mediante líneas de comunicaciones punto a punto alquiladas o de marcación. El mandato abre un shell cuyos submandatos le permiten:

- Tomar datos de la entrada estándar (escritos o redirigidos de un archivo existente), añadir una o varias direcciones (proporcionadas como argumentos en el propio mandato) y una indicación de la hora y, a continuación, añadir una copia al archivo de buzón de sistema de cada destinatario (/var/spool/mail/*IDUsuario*).
- Leer elementos de correo desde el archivo de buzón del sistema.
- Añadir elementos de correo al archivo de buzón personal (\$HOME/mbox) o a un archivo especificado.

- Enviar correo utilizando BNU a un usuario de otro sistema.
- Redirigir automáticamente todo el correo del buzón del sistema al buzón de otro sistema añadiendo una sentencia `.forward` al principio del archivo de buzón del sistema.

Sin embargo, deberá tener cierta experiencia como usuario de UNIX antes de poder utilizar al máximo este manejador de correo. Para obtener más información, consulte el mandato [\*\*bellmail\*\*](#).

## Funciones de correo

Aquí se presentan las características del programa **mail**.

El programa **mail** le permite recibir, crear y enviar correo a los usuarios de un sistema local o remoto.

### Almacenamiento de correo

El correo puede almacenarse de distintas formas dependiendo de cada situación.

Cuando se envía correo a su dirección, éste se almacena en un directorio del sistema especificado para el correo. Este directorio contiene un archivo para cada usuario del sistema local. En él se guarda todo el correo recibido hasta que el usuario lleva a cabo alguna acción con él.

### Buzón del sistema

El buzón del sistema es parecido al buzón de una oficina postal: la oficina postal se encarga de entregar la correspondencia que va dirigida a la persona propietaria de dicho buzón.

De forma similar, el buzón del sistema es un archivo en el que los mensajes se entregan a un determinado usuario. Si el archivo no existe cuando llega correo, el sistema lo crea. Al eliminar todos los mensajes, el archivo se suprime.

Los buzones del sistema residen en el directorio `/var/spool/mail`. El nombre del buzón coincide con el ID de usuario que está asociado a él. Por ejemplo, si su ID de usuario es `carmen`, su buzón del sistema es:

```
/var/spool/mail/carmen
```

### Buzón personal predeterminado

El buzón personal es parecido a la bandeja de entrada de una oficina. La bandeja de entrada sirve para guardar el correo que ha recibido, pero que todavía no ha archivado.

Cada usuario dispone de un buzón personal. Cuando se lee el correo del buzón de correo, el correo se graba en el buzón personal, `$HOME/mbox` (`$HOME` es el directorio de inicio de sesión), si no se ha marcado para suprimirse o para guardarse en un archivo. El archivo `mbox` sólo existe cuando contiene un mensaje.

### Archivo `dead.letter` para mensajes incompletos

Si necesita interrumpir la creación de un mensaje para llevar a cabo otras tareas, el sistema guarda los mensajes incompletos en el archivo `dead.letter` del directorio `$HOME`.

Si el archivo `dead.letter` no existe, se crea. Posteriormente, puede editarlo para terminar el mensaje.

**Atención:** No utilice el archivo `dead.letter` para almacenar mensajes. El contenido de este archivo se sobregrababa cada vez que se emitía una interrupción para guardar un mensaje parcial en el archivo `dead.letter`.

### Carpetas de correo

Las carpetas le permiten guardar los mensajes de forma organizada. Mediante el uso del programa de correo, puede poner un mensaje en una carpeta desde el buzón del sistema, un buzón personal o desde otra carpeta.

Cada carpeta es un archivo de texto. Cada carpeta se coloca en el directorio que especifique en el archivo `.mailrc` con la opción **set folder**. Es preciso crear este directorio antes de utilizar carpetas para almacenar mensajes. Una vez creado el directorio, el programa de correo crea las carpetas en dicho directorio a medida que las necesita. Si no especifica un directorio en el archivo `.mailrc`, las carpetas se crean en el directorio actual. Consulte el apartado “Organización del correo” en la página 17.

**Nota:** Hay varios programas disponibles para enviar y recibir correo, incluidos MH (Message Handler - Manejador de mensajes) y el programa **bellmail**. La elección del programa dependerá de la instalación y la configuración de su sistema. Para obtener información sobre la configuración del sistema, póngase en contacto con el administrador del sistema.

### Manejo y recepción de correo

El programa **mail** le permite examinar cada mensaje de un buzón y, a continuación, suprimir o archivar un mensaje en un directorio de correo personal.

El shell de mandatos notifica la llegada de correo. La notificación se visualiza antes del siguiente mensaje de solicitud, a condición de que se haya establecido la variable de entorno MAIL y a condición de que haya transcurrido el intervalo especificado por MAILCHECK desde la última vez que el shell ha comprobado el correo. El mensaje de notificación corresponde al valor de la variable de entorno MAILMSG. En función del shell que esté utilizando (bourne, korn o shell C), la notificación tendrá un aspecto parecido al siguiente:

```
TIENE CORREO NUEVO
```

### Arranque del buzón

Utilice el mandato **mail** para leer y eliminar mensajes del buzón del sistema.

No utilice el buzón del sistema para almacenar mensajes. Almacene los mensajes en el buzón personal y en carpetas de correo.

#### Comprobación del correo en el buzón del sistema

Utilice el mandato **mail** para comprobar el correo en el buzón del sistema.

En el indicador de la línea de mandatos del sistema, entre el mandato **mail**:

```
mail
```

Si en el buzón del sistema no hay correo, el sistema responde con el mensaje siguiente:

```
No existe correo para SuID
```

Si en el buzón del sistema hay correo, el sistema visualiza un listado de los mensajes que contiene:

```
Mail Type ? para obtener ayuda.  
"/usr/mail/lance": 3 messages 3 new (3 mensajes 3 nuevos)  
>N 1 karen Tue Apr 27 16:10 12/321 "Reunión dpto."  
N 2 luisa Tue Apr 27 16:50 10/350 "Noticias sist."  
N 3 marc Tue Apr 27 17:00 11/356 "Herramientas disp."
```

El mensaje actual siempre lleva el prefijo con un símbolo mayor que (>). Cada entrada de una línea visualiza los campos siguientes:

Item	Descripción
------	-------------

**estado** Indica la clase del mensaje.

**número** Identifica el elemento de correo en el programa.

**remitente** Identifica la dirección de la persona que ha enviado el correo.

**fecha** Especifica la fecha en la que se ha recibido el mensaje.

**tamaño** Define el número de líneas y caracteres que contiene el mensaje (incluida la cabecera).

**asunto** Identifica el asunto del mensaje, si lo hay.

El estado puede tener uno de estos valores:

**Item Descripción****m****N** Un mensaje nuevo.**P** Un mensaje que se guardará en el buzón del sistema.**U** Un mensaje no leído. Se trata de un mensaje que figuraba ya en el buzón la última vez que ha utilizado el programa de correo, pero cuyo contenido no se ha examinado.**\*** Un mensaje guardado o grabado en un archivo o carpeta.

Un mensaje sin indicador de estado es un mensaje que se ha leído pero que no se ha suprimido ni guardado.

*Comprobación del correo en el buzón personal o en la carpeta de correo*

Puede utilizar el mandato **mail** para comprobar el correo en el buzón personal o la carpeta de correo.

En el indicador de la línea de mandatos del sistema, puede utilizar el mandato **mail** de los modos mostrados en los pasos siguientes:

1. Para visualizar un listado de los mensajes del buzón personal, \$HOME/mbox, entre:

```
mail -f
```

Si no hay correo en el buzón personal, el sistema responde con un mensaje similar al siguiente:

```
"/u/jorge/mbox": 0 messages (0 mensajes)
```

O

```
A file or directory in the path name does not exist  
(No existe un archivo o un directorio en el nombre de vía de acceso)
```

2. Para visualizar un listado de los mensajes de la carpeta dept, entre:

```
mail -f +dept
```

Si no hay correo en el carpeta de correo, el sistema responde con un mensaje similar al siguiente:

```
A file or directory in the path name does not exist  
(No existe un archivo o un directorio en el nombre de vía de acceso)
```

**Opciones de visualización de contenido de buzón**

En el indicador del buzón, puede entrar submandatos de buzón para gestionar el contenido del buzón.

**Prerrequisitos**

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El programa de correo (mail) debe haberse iniciado.
3. El buzón debe tener correo.

**Rangos de mensajes**

Utilice el submandato **h** para ver un mensaje contenido en una lista de mensajes que determine para que no tenga que examinar todos los mensajes.

Puede utilizar el submandato **h** desde el indicador del buzón de las maneras que se muestran en los ejemplos siguientes:

**Item Descripción**

**h** Se visualizan unos 20 mensajes al mismo tiempo. El número real visualizado lo determina el tipo de terminal que se está utilizando y la opción **set screen** del archivo .mailrc. Si entra el submandato **h** otra vez, se visualizará el mismo rango de mensajes.

**Item Descripción**

**h 21** Se visualiza desde el mensaje 21 hasta el mensaje 40, ambos incluidos, siempre y cuando tenga dicha cantidad de mensajes en el buzón. Continúe entrando el submandato **h** con el siguiente número de mensaje hasta que se visualicen todos los mensajes.

**h 1** Para volver al primer grupo de 20 mensajes, entre cualquier número en el rango de 1 a 20.

*Desplazamiento por el buzón*

Utilice el submandato **z** para desplazarse por el buzón.

En el indicador de buzón, puede utilizar el submandato **z** de los modos que se muestran en los ejemplos siguientes:

**Item Descripción****m**

**z** Se visualizan unos 20 mensajes al mismo tiempo. El número real visualizado lo determina el tipo de terminal que se está utilizando y la opción **set screen** del archivo **.mailrc**. Entre el submandato **z** otra vez para desplazarse a los 20 mensajes siguientes.

**z +** El argumento **+** (más) le desplaza a los 20 mensajes siguientes. Se visualiza desde el mensaje 21 hasta el mensaje 40, ambos incluidos, siempre y cuando tenga dicha cantidad de mensajes en el buzón. Continúe entrando el submandato **z+** hasta que se visualicen todos los mensajes. El sistema responderá con el mensaje siguiente:

On last screenful of messages. (Última pantalla completa de mensajes.)

**z -** El argumento **-** (menos) le desplaza a los 20 mensajes anteriores. Al llegar al primer grupo de mensajes, el sistema responderá con el mensaje siguiente:

On first screenful of messages. (Primera pantalla completa de mensajes.)

*Filtro de mensajes para información específica*

En el indicador de buzón, puede utilizar el submandato **f** de los modos mostrados en los ejemplos siguientes para filtrar mensajes de acuerdo con la información que desea.

**Item Descripción**

**f** Visualiza información de cabecera para el mensaje actual.

**f 1 4 7** Visualiza información de cabecera para los mensajes específicos 1, 4 y 7.

**f 1-10** Visualiza información de cabecera para un rango de mensajes de 1 a 10.

**f \*** Visualiza todos los mensajes.

**f eva** Aparecen los mensajes del usuario eva, si los hay. Los caracteres entrados para una dirección no necesitan coincidir exactamente con la dirección; por consiguiente, la petición de la dirección eva, en letras mayúsculas o minúsculas, coincide con todas las direcciones siguientes:

Eva  
eva@topdog  
heva  
eVa

<b>Item</b>	<b>Descripción</b>
<b>freun</b>	Si existen, se visualizan mensajes donde el campo <b>Subject:</b> contiene las letras reun. No es necesario que los caracteres entrados para un patrón coincidan exactamente con el campo <b>Subject:</b> . Sólo deben estar contenidos en el campo <b>Subject:</b> en letras mayúsculas o minúsculas; por consiguiente, la petición del asunto reun coincide con todos los asuntos siguientes:

```
Reunión el jueves
Venid a la reunión mañana
Me encontraréis en ST. LOUIS
```

#### *Números de mensaje actuales*

El submandato = visualiza números de mensaje.

En el indicador del buzón, puede utilizar el submandato = de la manera que se muestra en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>m</b>	= Aparece el número del mensaje actual.

#### *Número total de mensajes en el buzón*

Utilice el submandato **folder** para comprobar cuántos mensajes hay en el buzón.

En el indicador del buzón, puede utilizar el submandato **folder** de la manera que se muestra en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
-------------	--------------------

<b>folder</b>	Lista información sobre la carpeta o el buzón. El sistema responderá con un mensaje parecido al siguiente:
---------------	--

```
"/u/lance/mbox": 29 messages (29 mensajes).
```

#### *Lectura de opciones de correo*

El correo se puede leer de distintas formas. Aquí se describen ejemplos de cada método.

Elija el método que le resulte más cómodo y utilícelo para leer el correo. Antes de intentar leer el correo, asegúrese de que las siguientes condiciones sean ciertas:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El programa de correo (mail) debe haberse iniciado.
3. El buzón del sistema debe tener correo.

#### *Lectura de los mensajes del buzón*

Utilice el submandato **t** o **p** para leer mensajes del buzón.

En el indicador del buzón, puede utilizar los submandatos **t** o **p** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
-------------	--------------------

<b>3</b>	Si utiliza el número del mensaje, aparece el texto de ese mensaje predeterminado.
<b>t</b>	Si utiliza el submandato <b>t</b> , de forma predeterminada aparece el texto del mensaje actual.
<b>t 3</b>	Aparece el texto del mensaje 3.
<b>t 2 4 9</b>	Aparece el texto de los mensajes 2, 4 y 9.
<b>t 2-4</b>	Aparece el texto del rango de mensajes del 2 al 4.

<b>Item</b>	<b>Descripción</b>
<b>t</b>	De forma predeterminada, si utiliza el submandato <b>p</b> aparece el texto del mensaje actual.
<b>p 3</b>	Aparece el texto del mensaje 3.
<b>p 2 4 9</b>	Aparece el texto de los mensajes 2, 4 y 9.
<b>p 2-4</b>	Aparece el texto del rango de mensajes del 2 al 4.

#### *Lectura del siguiente mensaje del buzón*

Utilice el submandato **n** para leer el siguiente mensaje del buzón.

En el indicador de buzón, puede utilizar el submandato (**n**)ext o de signo más (+) como se muestra en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>n o +</b>	Visualiza el texto del siguiente mensaje, al tiempo que este mensaje pasa a ser el mensaje actual.

También puede pulsar la tecla Intro para ver el texto del mensaje siguiente.

#### *Lectura del mensaje anterior del buzón*

Utilice el submandato - para leer el mensaje anterior.

En el indicador del buzón, puede usar el submandato - de la forma mostrada en el ejemplo siguiente:

<b>Ite</b>	<b>Descripción</b>
<b>m</b>	- Aparece el texto del mensaje anterior.

#### *Supresión de correo*

Al suprimir un mensaje, puede suprimir el mensaje actual, suprimir un mensaje específico o suprimir un rango de mensajes.

También puede suprimir el mensaje actual y visualizar el mensaje siguiente mediante la combinación de submandatos. Asegúrese de que se cumplen las condiciones siguientes:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El buzón del sistema debe tener correo.
3. El programa de correo (mail) debe haberse iniciado.

#### *Supresión de mensajes*

Para suprimir mensajes utilice diversos formatos del submandato **d**.

En el indicador del buzón, puede utilizar el submandato (**d**)elete de las maneras que se muestran en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>d</b>	Se suprime el mensaje actual.
<b>dp o dt</b>	Se suprime el mensaje actual y aparece el mensaje siguiente. Esto también se puede llevar a cabo incluyendo la opción <b>set autoprint</b> en el archivo .mailrc, que establecerá el submandato <b>d</b> para que funcione como la combinación de submandatos <b>dp</b> o <b>dt</b> .
<b>d 4</b>	Suprime el mensaje 4, específicamente.
<b>d 4-6</b>	Suprime un rango de mensajes de 4 a 6.
<b>d 2 6 8</b>	Suprime los mensajes 2, 6 y 8.

### *Cómo deshacer la supresión de mensajes*

Utilice el submandato **u** para deshacer la supresión de mensajes.

En el indicador del buzón, puede utilizar el submandato **u** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>u</b>	Se deshace la supresión del mensaje actual.
<b>u 4</b>	Se deshace la supresión del mensaje 4, específicamente.
<b>u 4-6</b>	Deshace la supresión de un rango de mensajes de 4 a 6.
<b>u 2 6 8</b>	Se deshace la supresión de los mensajes 2, 6 y 8.

### *Salida del correo*

Asegúrese de que se cumplen los requisitos siguientes antes de salir del programa de correo (mail).

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El buzón del sistema debe tener correo.
3. El programa de correo (mail) debe haberse iniciado.

### *Cómo salir del correo y guardar los cambios*

Utilice el submandato **q** para salir del correo y guardar los cambios.

Si sale del buzón del sistema:

<b>Item</b>	<b>Descripción</b>
<b>q</b>	El submandato <b>q</b> sale del buzón del sistema y vuelve al sistema operativo. Al salir del buzón, todos los mensajes que haya marcado para suprimir se eliminan del buzón y dejan de ser recuperables. El programa de correo guarda los mensajes que ha leído en el buzón personal (mbox). Si todavía no ha leído el correo, los mensajes permanecen en el buzón del sistema hasta que se lleva a cabo alguna acción con ellos.

Si sale del buzón personal o de una carpeta de correo:

<b>Item</b>	<b>Descripción</b>
<b>q</b>	Cuando se utiliza el submandato <b>q</b> en el buzón personal o en una carpeta de correo, los mensajes leídos y los no leídos permanecen en el buzón o en la carpeta hasta que se realiza alguna acción con ellos.

### *Cómo salir del correo sin guardar los cambios*

Utilice el submandato **x** o **ex** para salir del correo sin realizar cambios en el buzón.

<b>Item</b>	<b>Descripción</b>
<b>x</b> o <b>ex</b>	El submandato <b>x</b> o <b>ex</b> le permite salir del buzón y volver al sistema operativo sin cambiar el contenido original del buzón. El programa ignora cualquier petición que haya hecho antes de la petición <b>x</b> ; sin embargo, si ha guardado un mensaje en otra carpeta, esta operación se llevará a cabo.

### *Organización del correo*

Utilice carpetas para guardar los mensajes de forma organizada.

Puede crear tantas carpetas como necesite. Es recomendable asignar a cada carpeta un nombre que haga referencia al tema de los mensajes que contiene, de forma similar a como se organizan los archivadores en el sistema de archivado de una oficina. Cada carpeta es un archivo de texto que se coloca en el directorio que se especifica en el archivo .mailrc con la opción **set folder**. Es preciso crear este directorio antes de utilizar carpetas para almacenar mensajes. Una vez creado el directorio, el programa de correo crea las carpetas en dicho directorio a medida que las necesita. Si no especifica un directorio

con la opción **set folder** en el archivo `.mailrc`, la carpeta se crea en el directorio actual. Mediante el uso del programa de correo, puede poner un mensaje en una carpeta del buzón del sistema, de un buzón personal o de otra carpeta.

Puede añadir el contenido de un mensaje a un archivo o carpeta utilizando los submandatos **s** o **w**. Estos dos submandatos añaden información a un archivo existente o crean un archivo nuevo si no existe ninguno. La información que esté en el archivo en ese momento no se destruye. Si guarda un mensaje desde el buzón del sistema en un archivo o carpeta, el mensaje se suprime del buzón del sistema y se transfiere al archivo o carpeta especificados. Si guarda un mensaje del buzón personal o de la carpeta en otro archivo o carpeta, el mensaje no se suprime del buzón personal, sino que se copia en el archivo o la carpeta que se especifique. Si utiliza el submandato **s**, puede leer la carpeta como si fuera un buzón, porque los mensajes y la información de cabecera se añaden al final de la carpeta. Si utiliza el submandato **w**, puede leer la carpeta como si fuera un archivo, porque el mensaje se añade sin la información de cabecera al final del archivo.

Antes de organizar el correo, asegúrese de que se cumplen los requisitos siguientes:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El buzón del sistema, el buzón personal o la carpeta que ha definido deben tener correo.
3. El programa de correo (mail) debe haberse iniciado.

#### *Creación de un directorio de buzón de cartas para almacenar mensajes en carpetas*

Se pueden guardar mensajes en una carpeta de directorio de buzón utilizando el submandato **set folder**.

Utilice el procedimiento siguiente para almacenar mensajes en carpetas:

1. Para comprobar si la opción **set folder** se ha habilitado en el archivo `.mailrc`, entre el siguiente submandato en el indicador de buzón:

```
set
```

El submandato **set** visualiza una lista de las opciones de correo habilitadas del archivo `.mailrc`.

Si se ha habilitado la opción **set folder**, el sistema responde con un mensaje parecido al siguiente:

```
folder /home/jorge/cartas
```

En este ejemplo, `cartas` es el directorio en que se almacenarán las carpetas de correo.

2. Si la opción **set folder** no se ha habilitado, añada una línea similar a la siguiente en el archivo `.mailrc`:

```
set folder=/home/jorge/cartas
```

En este ejemplo, `/home/jorge` es el directorio inicial de Jorge y `cartas` es el directorio en el que se almacenarán las carpetas de correo. La opción **set folder** le permite utilizar la anotación taquigráfica + (signo más) en el indicador de buzón para guardar mensajes en el directorio `cartas`.

3. Debe crear un directorio `cartas` en el directorio inicial. En el directorio inicial y desde el indicador de la línea de mandatos del sistema, escriba:

```
mkdir cartas
```

#### *Cómo guardar mensajes con cabeceras*

El submandato **s** guarda los mensajes con cabeceras.

Utilice el submandato **s** de los modos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>s 1-4 notes</b>	Guarda los mensajes 1, 2, 3 y 4 con la información de cabecera en una carpeta denominada notes del directorio actual.  El programa de correo responde con el mensaje siguiente:
	"notes" [Appended] (Añadidas) 62/1610
<b>s +admin</b>	Guarda el mensaje actual en una carpeta existente llamada admin del directorio de carpetas.  Si el directorio de carpetas se ha definido como /home/jorge/cartas en el archivo .mailrc, el sistema responde con:
	"/home/jorge/cartas/admin" [Appended] (Añadidas) 14/321
<b>s 6 +admin</b>	Guarda el mensaje 6 en una carpeta existente denominada admin del directorio de carpetas.  Si el directorio de carpetas se ha definido como /home/jorge/cartas en el archivo .mailrc, el sistema responde con:
	"/home/jorge/cartas/admin" [Appended] (Añadidas) 14/321

#### *Cómo guardar mensajes sin cabeceras*

Utilice el submandato **w** para guardar un mensaje como un archivo en lugar de guardarlo como una carpeta.

Para leer o editar un archivo guardado con el submandato **w**, debe utilizar **vi** o algún otro editor de texto. En el indicador del buzón, puede utilizar el submandato **w** de los modos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>w 6 pass</b>	Sólo guarda el texto del mensaje 6 en un archivo denominado pass del directorio actual.  Si el archivo pase todavía no existe, el sistema responde con el mensaje siguiente:
	"pase" [New file] (Archivo nuevo) 12/30
	Si el archivo pase existe, el sistema responde con el mensaje siguiente:
	"pase" [Appended] (Añadido) 12/30
<b>w 1-3 safety</b>	Sólo guarda el texto de los mensajes específicos 1, 2 y 3 en un archivo denominado safety del directorio actual.  El texto de los mensajes de este ejemplo se añadirá uno detrás de otro en un archivo. Si el archivo seguridad todavía no existe, el sistema responde con el mensaje siguiente:
	"seguridad" [New file] (Archivo nuevo) 12/30

#### *Determinación del buzón o de la carpeta actual*

Utilice el submandato **folder** para determinar el buzón o la carpeta actual.

Aunque el mandato **mail** visualiza el nombre del buzón actual cuando se inicia, puede que en algún momento no sepa en qué buzón se encuentra. En el indicador de buzón, puede utilizar el submandato **folder** mostrado en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>folder</b>	Busca el nombre del buzón o carpeta actual. Si el buzón actual es /home/lance/mbox, se visualiza lo siguiente:
	/home/lanza/mbox: 2 messages 1 deleted (2 mensajes 1 suprimido)
	Este mensaje indica que /home/lanza/mbox es el buzón actual en que se encuentra actualmente, que contiene dos mensajes y que uno de ellos se suprimirá cuando deje de utilizar este buzón.
<i>Cambio a otro buzón</i>	
	Cambiar a otro buzón es como salir de un buzón o carpeta.
	Todos los mensajes que haya marcado para suprimir desaparecerán al salir del buzón. Los mensajes que se supriman no podrán recuperarse. En el indicador de buzón, puede utilizar el submandato <b>file</b> o <b>folder</b> que se muestra en el ejemplo siguiente:
<b>Item</b>	<b>Descripción</b>
<b>folder +project</b>	Después de que se haya iniciado el programa de correo con un buzón, utilice los submandatos <b>file</b> o <b>folder</b> para cambiar a otro buzón.  Si cambia del archivo mbox a la carpeta mbox y ha suprimido todos los mensajes del archivo mbox, el programa de correo visualiza:
	/home/dee/mbox removed +proyecto: 2 messages 2 new (2 mensajes 2 nuevos)
	seguido de una lista de los mensajes de la carpeta proyecto.

### Creación y envío de correo

Puede utilizar el programa **mail** para crear, enviar, responder y reenviar mensajes a otros usuarios o para enviar archivos ASCII a otros usuarios.

Por ejemplo, un archivo ASCII puede ser un documento que haya escrito utilizando su editor favorito, o bien el archivo fuente de un programa.

Puede enviar mensajes y archivos a un usuario del sistema local, de su propia red, o a un usuario que se encuentre en otra red conectada. No es preciso que el destinatario haya iniciado la sesión en el sistema cuando usted le envíe la información. El correo se envía a la dirección de un usuario.

### Direccionamiento del correo

El correo se envía a la dirección de un usuario. La dirección, en la que figura el nombre de inicio de sesión y el nombre del sistema, controla la entrega del mensaje de correo.

En general, para enviar un mensaje a otro usuario, debe entrar el mandato **mail** y la dirección del modo siguiente:

```
mail Usuario@Dirección
```

El formato del parámetro *Dirección* depende de la ubicación del destinatario. La situación es parecida a cómo enviaría una nota a otro colega en una oficina. Para enviar una nota a Rosa, que trabaja en un pequeño departamento de seis u ocho empleados, puede escribir su nombre en un sobre y colocarlo en el sistema de correo de la oficina. Sin embargo, si Rosa está en otro departamento, es probable que tenga que proporcionar más información en el sobre:

```
Rosa
Nóminas
```

Si Rosa está en otra ubicación geográfica, es posible que necesite incluso más información para asegurarse de que le va a llegar el mensaje:

Rosa  
Nóminas  
Oficina Central

Para enviar correo electrónicamente, utilice una progresión de direccionamiento similar:

Item	Descripción
<b>mail rosa</b>	Si desea enviar correo a un usuario del sistema local, sólo necesita especificar el nombre de inicio de sesión en la dirección.
<b>mail rosa@tybalt</b>	Para enviar correo a un usuario de la red local, entre la dirección completa del sistema (nodo).
<b>mail rosa@mars.aus.dbm.co</b>	Para enviar correo a un usuario que se encuentra en otra red conectada, entre la dirección de sistema y la dirección de red completas.
<b>mail depto71</b>	Es posible enviar correo a un grupo específico de personas utilizando una lista de alias o de distribución. Para ello, debe crear dicha lista en el archivo <code>.mailrc</code> . Si necesita información sobre la creación de alias, vea el apartado “Alias y listas de distribución” en la página 37.

#### *Direccionamiento de correo a más de un usuario*

Para dirigir correo a más de un usuario al mismo tiempo, separe cada nombre de usuario con un espacio.

Por ejemplo:

```
rosa@tybalt suemc@julius dmorgan@ophelia
```

#### *Direccionamiento de correo a usuarios del sistema local*

Para enviar un mensaje a un usuario del sistema local (a alguien cuyo nombre de inicio de sesión figura en su archivo `/etc/passwd`), utilice el nombre de inicio de sesión para la dirección.

En el indicador de línea de mandatos del sistema, puede utilizar el mandato **mail** que se muestra en el ejemplo siguiente:

```
mail NombreInicioSesión
```

Item	Descripción
<b>mail rosa</b>	Si Rosa está en su sistema y tiene el nombre de inicio de sesión <code>rosa</code> , este mandato activa el programa de correo, le permite crear un mensaje e intenta enviarlo al nombre de inicio de sesión local <code>rosa</code> . Si el mensaje se entrega satisfactoriamente, no recibirá notificación alguna. Si Rosa no está en el sistema, el sistema de correo devuelve inmediatamente un mensaje de error, además del mensaje no enviado al buzón del sistema.

#### *Direccionamiento de correo a usuarios de la red*

Utilice el mandato **mail** para enviar un mensaje a los usuarios de la red. Incluya en la dirección el nombre de inicio de sesión del usuario y el nombre de sistema.

Para enviar un mensaje a través de una red local a un usuario de otro sistema, escriba lo siguiente en la línea de mandatos:

Item	Descripción
<b>mail</b> <i>NombreInicioSesión@NombreSistema</i>	<p>Por ejemplo, si Rosa está en el sistema zeus, utilice el mandato siguiente para crear un mensaje y enviárselo:</p> <pre>mail rosa@zeus</pre> <p>Este mandato activa el programa de correo, le permite crear un mensaje e intenta enviarlo al nombre de inicio de sesión <i>rosa</i> del sistema <i>zeus</i>. Si el mensaje se entrega satisfactoriamente, aparecerá el indicador del sistema sin notificación alguna. Si la dirección de correo es incorrecta, recibirá un mensaje de error.</p>

**Nota:** Para enviar un mensaje a través de una red local a un usuario de otro sistema, debe conocer el nombre de inicio de sesión y el nombre del otro sistema. Para obtener más información sobre cómo visualizar información que identifica a los usuarios, consulte el apartado “[Mandatos de red comunes](#)” en la página 6.

#### *Direccionamiento de correo a usuarios de una red diferente*

Si su red está conectada con otras redes, es posible enviar correo a los usuarios de dichas redes.

Los parámetros de direccionamiento dependerán del modo en que ambas redes se hayan direccionado entre sí y del modo en que estén conectadas. En función de la configuración de red, realice una de estas acciones:

- Si está utilizando una base de datos central de nombres y direcciones, utilice el mandato **mail** mostrado en el ejemplo siguiente:

```
mail  
NombreInicioSesión@NombreSistema
```

Si las redes utilizan una base de datos central de nombres, no se precisa información adicional para enviar correo a los usuarios de las redes conectadas. Utilice el mismo formato de direccionamiento que utiliza para los usuarios de su red local.

Este tipo de direccionamiento resulta muy adecuado cuando la naturaleza de la red permite el mantenimiento de una base de datos central de nombres.

- Si la red utiliza el direccionamiento de nombres de dominio, utilice el mandato **mail** mostrado en el ejemplo siguiente:

```
mail NombreInicioSesión@NombreSistema.NombreDominio
```

En el caso de redes con una amplia extensión y numerosas redes no relacionadas, el mantenimiento de una base de datos central de nombres no es posible. El parámetro *NombreDominio* define la red remota, en relación con la red local, dentro de la estructura definida para el grupo más amplio de redes interconectadas.

Por ejemplo, si entra el mandato siguiente:

```
mail pilar@merlin.odin.valryan1
```

el correo se envía al usuario *pilar* del sistema *merlin*, que está en una red local denominada *odin* que está conectada a una segunda red cuyo dominio se denomina *valryan1*.

#### *Direcciones de correo a través de un enlace BNU o UUCP*

Puede enviar mensajes a usuarios de otro sistema a través de un enlace BNU (Basic Networking Utilities - Programas de utilidad básicos de red) o UUCP (UNIX-to-UNIX Copy Program).

Para enviar un mensaje a un usuario de otro sistema conectado al suyo mediante el programa BNU o mediante otra versión del programa UUCP, debe conocer:

- El nombre de inicio de sesión
- El nombre del otro sistema
- La ruta física al otro sistema

La persona responsable de la conexión de su sistema con otros sistemas debe proporcionarle la información de direccionamiento para poder comunicarse con el otro sistema.

**Cuando el sistema tiene un enlace BNU o UUCP:** En el indicador de la línea de mandatos del sistema, utilice el mandato **mail** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>mail RutaUUCP!NombreInicioSesión</b>	Si el sistema local dispone de una conexión BNU o UUCP que puede servir para ponerse en contacto con el sistema remoto, utilice el formato indicado en este ejemplo para direccionar el mensaje. La variable <i>NombreInicioSesión</i> es el nombre de inicio de sesión del sistema remoto correspondiente al destinatario del mensaje. La variable <i>RutaUUCP</i> describe la ruta física que debe seguir el mensaje a través de la red UUCP. Si su sistema está conectado al sistema remoto sin que haya sistemas UUCP intermedios entre uno y otro, esta variable corresponde al nombre del sistema remoto.
<b>mailarturo!lancelot!merlin!olga</b>	Si el mensaje debe viajar a través de uno o más sistemas UUCP intermedios antes de alcanzar el sistema remoto de destino, esta variable muestra una lista de cada uno de estos sistemas intermedios. La lista empieza por el sistema más próximo y continúa hasta el más lejano, separando cada uno mediante un signo !. Siga el ejemplo que aquí se indica si el mensaje debe viajar a través de los sistemas <i>arturo</i> y <i>lancelot</i> (en este orden) antes de llegar a <i>merlin</i> .
<b>mail merlin!olga</b>	Si el sistema local dispone de un enlace UUCP con un sistema llamado <i>merlin</i> y no existe ningún otro sistema UUCP entre su sistema y <i>merlin</i> , puede enviar un mensaje a <i>olga</i> en dicho sistema.

**Cuando el enlace BNU o UUCP está en otro sistema:** En un entorno de red de área amplia o local, puede que uno de los sistemas de la red tenga una conexión BNU u otro tipo de conexión UUCP con un sistema remoto. Es posible utilizar dicha conexión para enviar un mensaje a un usuario que se encuentre en el sistema UUCP remoto. En el indicador de la línea de mandatos del sistema, utilice el mandato **mail** del modo que se muestra en el ejemplo siguiente:

#### **mail @arturo:merlin!olga**

Envía correo a *olga* en el sistema UUCP *merlin* desde el sistema de Internet *arturo*. El delimitador @ indica una dirección de Internet, mientras que el delimitador ! corresponde a una dirección UUCP y los dos puntos (:) conectan las dos direcciones. Observe que con este formato no se envía correo a ningún usuario de ningún sistema intermedio, por lo que no es necesario indicar el nombre de inicio de sesión antes del delimitador @ en la dirección del dominio.

#### **mail @arturo:odin!dpto.conta!pilar**

Envía correo a *pilar* en el sistema UUCP *dpto.conta* a través del sistema *odin* desde el sistema de Internet *arturo*.

#### **mail@odin.uucp:@dpto1.UUCP:@dpto2:juan@dpto3**

Envía correo a *juan@dpto3* a través de los enlaces UUCP *odin* y *dpto1* y, a continuación, a través del enlace de red local entre los sistemas *dpto2* y *dpto3*. El archivo /etc/sendmail.cf debe configurarse debidamente para utilizar este tipo de notación de dirección UUCP. Consulte información a su administrador del sistema.

Si habitualmente envía correo a usuarios de otras redes, la creación de alias que incluyan las direcciones de los usuarios puede ahorrarle mucho tiempo. Consulte el apartado “Alias y listas de distribución” en la página 37.

### **Inicio del editor de correo**

El programa **mail** proporciona un editor orientado a líneas para crear mensajes.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El programa de correo (mail) debe haberse iniciado.

Este editor le permite entrar cada una de las líneas del mensaje, pulsar la tecla Intro para obtener una línea nueva y escribir más texto. No puede cambiar una línea después de haber pulsado la tecla Intro. No obstante, antes de pulsar la tecla Intro, puede cambiar la información de la línea utilizando las teclas Retroceso y Supr para borrar. También es posible utilizar los submandatos del editor de correo para acceder a un editor en pantalla completa y modificar el mensaje.

Al crear correo con el editor de correo, el sistema rellena automáticamente los campos **date:** y **from:**. Tiene la opción de llenar los campos **subject:** y **cc:**. Estos campos se parecen al cuerpo de una carta comercial estándar.

El editor de correo contiene muchos submandatos de control que le permiten realizar otras operaciones con un mensaje. Cada uno de estos submandatos debe entrarse en una línea nueva y debe empezar con el carácter especial de *escape*. De forma predeterminada, el carácter de escape es una tilde (~). Puede cambiarlo por cualquier otro carácter incluyendo la opción **set escape** en el archivo **.mailrc**.

En el indicador de la línea de mandatos o el indicador del buzón del sistema, puede utilizar el mandato **mail** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>mail</b> <i>Usuario@Dirección</i>	Emita este mandato desde el indicador de la línea de mandatos. El mensaje va dirigido a <i>Usuario@Dirección</i> . El parámetro <i>Dirección</i> depende de la ubicación del destinatario.
<b>m</b> <i>Usuario@Dirección</i>	Emita este submandato desde el indicador del buzón. El mensaje va dirigido a <i>Usuario@Dirección</i> . El parámetro <i>Dirección</i> depende de la ubicación del destinatario.

El editor de correo también se activa si utiliza los submandatos **R** o **r** para responder a un mensaje. Para obtener más información sobre cómo responder a un mensaje, consulte el apartado “Envío de correo” en la página 29 y el apartado “Respuesta al correo” en la página 30.

### **Edición de mensajes**

Desde el buzón puede añadir información a un mensaje existente escribiendo los submandatos **(e)dit** o **(v)isual** en el indicador del buzón.

Desde el editor de correo no puede cambiar la información de una línea cuando ya se ha pulsado la tecla Intro y se ha pasado a la línea siguiente. Puede cambiar el contenido del mensaje antes de enviarlo si lo edita con otro editor.

Antes de editar un mensaje en otro editor, asegúrese de que las siguientes condiciones sean ciertas:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El editor alternativo debe estar definido en el archivo **.mailrc** con:

```
set EDITOR=NombreVíaAcceso
```

Esta opción define el editor que se activa con el submandato **~e**. El valor de *NombreVíaAcceso* debe ser el nombre de vía de acceso completo al programa editor que desea utilizar. Por ejemplo, la definición **set EDITOR=/usr/bin/vi** define el editor **vi** para utilizarse con el submandato **~e**.

3. Para añadir información a un mensaje del buzón, es preciso haber iniciado antes el mandato **mail** para leer el correo del buzón del sistema, de otro buzón o de otra carpeta.

4. Para iniciar otro editor mientras está creando un mensaje, debe estar situado en el indicador del editor de correo.

#### *Adición de información a un mensaje específico de buzón*

Para añadir información a un mensaje del buzón, entre el submandato **e** o el submandato **v**, seguido del número de mensaje.

En el indicador del buzón, puede utilizar los submandatos **e** o **v** del modo que se muestra en los ejemplos siguientes:

#### **Item Descripción**

- e** 13 Para añadir una nota al mensaje 13 utilizando el editor **e** (o cualquier editor que esté definido en el archivo `.mailrc`).
- v** 15 Para añadir una nota al mensaje 15 utilizando el editor **vi** (o cualquier editor que esté definido en el archivo `.mailrc`).

Si no especifica ningún número de mensaje, el mandato **mail** activa el editor utilizando el mensaje actual. Al salir del editor, volverá al indicador del buzón para continuar procesando los mensajes del buzón.

#### *Modificación del mensaje actual desde el editor de correo*

Al principio de una línea en el editor de correo, puede utilizar el submandato **~e** o **~v** del modo que se muestra en estos ejemplos.

#### **Item Descripción**

##### **m**

- ~e** Activa el editor **e** u otro editor que haya definido en el archivo `.mailrc`.
- ~v** Activa el editor **vi** u otro editor que haya definido en el archivo `.mailrc`.

Esto le permite editar el texto del mensaje actual. Al salir del otro editor, volverá al editor de correo.

#### *Visualización de las líneas de un mensaje desde el editor de correo*

Utilice el submandato **~p** para visualizar las líneas de mensaje mientras está en el editor de correo.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Para visualizar un mensaje desde el editor de correo, debe haber iniciado antes el editor de correo. Si necesita información sobre este tema, consulte el apartado “[Inicio del editor de correo](#)” en la página [24](#).

Al principio de una línea en el editor de correo, utilice el submandato **~p** del modo mostrado en el ejemplo siguiente:

#### **Item Descripción**

##### **m**

- ~p** El editor muestra el contenido del mensaje, incluida la información de cabecera. El texto se desplaza en la pantalla de arriba abajo. El final del mensaje va seguido del indicador del editor de correo (Continue) (Continúa).

Si el mensaje ocupa más de una pantalla y no ha definido el tamaño de página para el terminal mediante el mandato **stty**, el texto se desplaza por la parte superior de la pantalla hasta el final. Para ver el contenido de los mensajes extensos, utilice los submandatos del editor de correo para visualizar el mensaje con otro editor. Si necesita información sobre este tema, consulte el apartado “[Edición de mensajes](#)” en la página [24](#).

#### *Salida del editor de correo*

Para salir del editor de correo sin enviar el mensaje utilice el submandato **~q** o la secuencia de teclas de interrupción (por lo general suele ser la secuencia de teclas Alt-Pausa o Control-C).

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Para visualizar un mensaje desde el editor de correo, debe haber iniciado antes el editor de correo. Si necesita información sobre este tema, consulte el apartado “[Inicio del editor de correo](#)” en la página 24.

Si ha entrado texto, el mandato **mail** guarda el mensaje en el archivo `dead.letter`.

Al principio de una línea en el editor de correo, puede utilizar el submandato **~q** del modo mostrado en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>~q</b>	Le permite salir del editor de correo sin enviar el mensaje. El mensaje se guarda en el archivo <code>dead.letter</code> del directorio inicial, a menos que no haya entrado texto. Aparece el indicador del sistema.
<b>Control-C</b>	Para abandonar el editor utilizando una secuencia de teclas de interrupción, pulse la tecla Inter (la secuencia de teclas Control-C) o la tecla Pausa (la secuencia de teclas Alt-Pausa). Aparece el mensaje siguiente:

```
(Interrupt -- one more to kill letter)
(Interrupción -- pulse una vez más para destruir el mensaje)
```

Vuelva a pulsar la tecla Inter o Pausa.

```
(Last Interrupt -- letter saved in dead.letter)
(Última interrupción -- mensaje guardado en dead.letter)
```

El mensaje no se envía. El mensaje se guarda en el archivo `dead.letter` del directorio inicial, a menos que no haya entrado texto. Aparece el indicador del sistema.

**Nota:** Si sale del editor de correo sin enviar el mensaje, el contenido anterior del archivo `dead.letter` se sustituye por el mensaje incompleto. Para recuperar el archivo, consulte el apartado “[Opciones para añadir un archivo y un mensaje específico en un mensaje](#)” en la página 26.

### **Opciones para añadir un archivo y un mensaje específico en un mensaje**

Se deben satisfacer varios requisitos antes de añadir un archivo y un mensaje específico en un mensaje de correo.

#### **Prerrequisitos**

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Debe conocer el nombre y la dirección del destinatario del correo.
3. El editor de correo debe haberse iniciado.

#### *Inclusión de archivos en un mensaje*

Utilice el submandato **~r** para añadir archivos a un mensaje.

Al principio de una línea en el editor de correo, puede utilizar el submandato **~r** del modo que se muestra en el ejemplo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>~r</b>	Donde <code>planificación</code> es el nombre del archivo que desea incluir. En este ejemplo, <code>planificación</code> la información del archivo <code>planificación</code> se incluye al final del mensaje que se está escribiendo.

#### *Inclusión de un mensaje específico en un mensaje*

Utilice el submandato **~f** o **~m** para incluir un mensaje específico en el mensaje.

Al principio de una nueva línea en el editor de correo, puede utilizar el submandato **~f** o **~m** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>~f ListaMensajes</b>	Añade el mensaje o los mensajes indicados al final del mensaje actual, pero <i>no</i> se efectúa el sangrado del mensaje añadido. También puede utilizar este submandato para añadir mensajes de consulta cuyos márgenes sean demasiado anchos como para añadirlos con el submandato <b>~m</b> .
	<b>Nota:</b> El parámetro <i>ListaMensajes</i> es una lista de enteros que hace referencia a los números de mensaje válidos del buzón o de la carpeta que el correo está gestionando. También puede entrar simples rangos de números. Por ejemplo:
<b>~f 1-4</b>	Añade los mensajes 1, 2, 3 y 4 al final del mensaje que está escribiendo. Estos mensajes se alinean respecto al margen izquierdo (no se sangran).
<b>~m 2</b>	Añade el mensaje indicado al final del mensaje actual. El mensaje incluido se sangra un carácter de tabulación respecto al margen izquierdo normal del mensaje. En este ejemplo, el mensaje 2 se añade al mensaje actual.
<b>~m 1 3</b>	Añade el mensaje 1 y, a continuación, el mensaje 3 al final del mensaje que está escribiendo, sangrándolo con un tabulador respecto al margen izquierdo.

#### *Adición del contenido del archivo dead.letter al mensaje actual*

Utilice el submandato **~d** para añadir el contenido *dead.letter* al mensaje.

Al principio de una línea nueva en el editor de correo, puede utilizar el submandato **~d** del modo que se muestra en el ejemplo siguiente:

#### **Ite Descripción**

##### **m**

- ~d** Recupera y añade el contenido del archivo *dead.letter* al final del mensaje actual. En el indicador (Continue), siga añadiendo al mensaje o envíelo.

#### *Edición de la información de cabecera*

La cabecera de un mensaje contiene información de direccionamiento y una breve descripción del asunto. Como mínimo, debe especificar un destinatario para el mensaje.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Inicie el editor de correo y empiece a editar un mensaje. Para obtener más información, consulte el apartado [Inicio del editor de correo](#).

El resto de la información de cabecera no es necesaria. La información de la cabecera puede incluir lo siguiente:

<b>Item</b>	<b>Descripción</b>
<b>To: (A:)</b>	Contiene la dirección o direcciones de envío del mensaje.
<b>Subject: (Asunto:)</b>	Contiene un breve resumen del tema del mensaje.
<b>Cc:</b>	Contiene la dirección o direcciones para el envío de copias del mensaje. El contenido de este campo forma parte del mensaje que se envía a todos los que lo reciben.
<b>Bcc:</b>	Contiene la dirección o direcciones para el envío de copias <i>ocultas</i> del mensaje. Este campo <i>no</i> se incluye como parte del mensaje que se envía a todos los que lo reciben.

Puede personalizar el programa de correo para que solicite automáticamente la información de estos campos poniendo entradas en el archivo *.mailrc*. Para obtener más información, consulte el apartado “[Opciones de personalización del programa de correo](#)” en la página 35.

#### *Establecimiento o restablecimiento del campo Subject:*

Utilice el submandato **~s** para establecer el campo **Subject:** con un texto o una frase determinados.

El uso de este submandato sustituye el contenido anterior (de haberlo) del campo **Subject:**. Al principio de una línea nueva en el editor de correo, puede utilizar el submandato **~s** del modo que se muestra en el ejemplo siguiente:

Item	Descripción
<b>~s Salida Pesca</b>	Esto cambia el campo <b>Subject:</b> actual: Subject: Vacaciones
	Por el siguiente: Subject: Salida Pesca
	<b>Nota:</b> No puede añadir información al campo <b>Subject:</b> con este submandato. Utilice el submandato <b>~h</b> , tal como se describe en el apartado “Edición de la información de cabecera” en la página 27.

#### *Adición de usuarios a los campos To:, Cc: y Bcc:*

Utilice el submandato **~t**, **~c** o **~b** para añadir usuarios a los campos de cabecera.

Al principio de una línea nueva en el editor de correo, puede utilizar los submandatos **~t**, **~c** o **~b** del modo que se muestra en los ejemplos siguientes:

Item	Descripción
<b>~t leo@austin ana@gtwn</b>	Esto cambia el campo <b>To:</b> actual: To: marcos@austin por lo siguiente: To: marcos@austin leo@austin ana@gtwn
<b>~c leo@austin ana@gtwn</b>	Esto cambia el campo <b>Cc:</b> actual: Cc: marcos@austin amy por lo siguiente: Cc: marcos@austin amy leo@austin ana@gtwn
<b>~b leo@austin ana@gtwn</b>	Esto cambia el campo <b>Bcc:</b> actual: Bcc: marcos@austin por lo siguiente: Bcc: marcos@austin leo@austin ana@gtwn

**Nota:** No puede utilizar los submandatos **~t**, **~c** o **~b** para cambiar o suprimir el contenido de los campos **To:**, **Cc:** y **Bcc:**. Utilice el submandato **~h**, tal como se describe en el apartado “Edición de la información de cabecera” en la página 27.

#### *Reformato de mensajes en el editor de correo*

Después de escribir el mensaje y antes de enviarlo, puede reformatear el mensaje para mejorar su aspecto utilizando el programa de shell **fmt**.

Antes de volver a formatear un mensaje, asegúrese de que las siguientes condiciones sean ciertas:

1. El programa de correo (mail) debe estar instalado en el sistema.

2. El mandato **fmt** debe estar instalado en el sistema.

Al principio de una línea nueva en el editor de correo, puede utilizar el mandato **fmt** del modo que se muestra en el ejemplo siguiente:

**Item      Descripción**

- | fmt** Cambia el aspecto del mensaje acomodando la información de cada párrafo dentro de los márgenes definidos (cada párrafo debe ir separado por una línea en blanco). El submandato de conducto (**|**) conduce el mensaje a la entrada estándar del mandato y lo sustituye por la salida estándar del mismo.

**Atención:** No utilice el mandato **fmt** si el mensaje contiene mensajes incorporados o información preformatteada de los archivos externos. El mandato **fmt** reformatea la información de cabecera de los mensajes incorporados y puede cambiar el formato de la información preformatteada. En lugar de ello, utilice los submandatos **~e** o **~v** para acceder a un editor en pantalla completa y cambiar el formato del mensaje.

**Comprobación de la ortografía incorrecta en el editor de texto**

El mandato **spell** comprueba la ortografía del mensaje.

Antes de revisar la ortografía de un mensaje, asegúrese de que las siguientes condiciones sean ciertas:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Los programas para dar formato al texto deben estar instalados en el sistema.

Utilice el mandato **spell** desde el editor de correo para comprobar si la ortografía de las palabras del mensaje es correcta:

1. Grabe el mensaje en un archivo temporal. Por ejemplo, para grabar el mensaje en el archivo **checkit**, escriba:

```
~w checkit
```

2. Ejecute el mandato **spell** utilizando el archivo temporal como entrada. Escriba:

```
~, spell checkit
```

En este ejemplo, el punto de exclamación final (!) es el submandato que inicia un shell, ejecuta un mandato y le devuelve al buzón. El mandato **spell** responde con una lista de palabras que no están en la lista de palabras conocidas, seguida de un punto de exclamación final (!) para indicar que ha vuelto al programa de correo.

3. Examine la lista de palabras. Vea si necesita utilizar un editor para llevar a cabo las correcciones.
4. Escriba lo siguiente para suprimir el archivo temporal:

```
~, rm checkit
```

**Envío de correo**

Utilice este procedimiento para enviar un mensaje después de haberlo creado.

- El programa de correo (mail) debe estar instalado en el sistema.
- Debe conocer el nombre y la dirección del destinatario del correo.

1. Entre el mandato **mail** en la línea de mandatos, seguido del nombre y de la dirección del destinatario (o destinatarios) del mensaje. Por ejemplo:

```
>mail jan@brown
```

El sistema responde con:

Subject:

2. Escriba el asunto del mensaje. Por ejemplo:

Subject: Reunión Dpto

y pulse Intro. A continuación, puede escribir el cuerpo del texto.

3. Escriba el mensaje. Por ejemplo:

Esta tarde tendrá lugar una breve reunión del  
departamento  
en mi oficina. Se ruega vuestra asistencia.

4. Para enviar un mensaje que ha escrito con el editor de correo, pulse el carácter de fin de texto, que es normalmente la secuencia de teclas Control-D o un punto (.), al principio de una línea nueva del mensaje.

El sistema visualiza el campo **Cc**:

Cc:

5. Escriba los nombres y las direcciones de los usuarios que deben recibir copias del mensaje. Por ejemplo:

Cc: carmen@hobo carlos@cross

**Nota:** Si no desea enviar copias, pulse Intro sin escribir nada.

Una vez pulsada la tecla Intro, el mensaje se entregará en la dirección especificada.

**Nota:** Si entra una dirección desconocida para el sistema, o que no está definida en ninguna lista de alias o de distribución, el sistema responderá con el nombre de inicio de sesión seguido de un mensaje de error: [ID usuario]... Usuario desconocido.

#### **Respuesta al correo**

En el indicador de buzón, puede utilizar los submandatos **r** y **R** para responder al correo del modo mostrado en los ejemplos siguientes.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. El buzón del sistema debe tener correo.

Item	Descripción
<b>r</b>	Crea un mensaje nuevo dirigido al remitente del mensaje seleccionado y con copia a las personas indicadas en el campo <b>Cc</b> : (si existen). El campo <b>Subject</b> : del mensaje nuevo hace referencia al mensaje seleccionado. El valor predeterminado del submandato <b>r</b> es el mensaje actual. Este valor predeterminado puede alterarse temporalmente escribiendo el número del mensaje después de <b>r</b> .
<b>R</b>	Inicia una respuesta únicamente al remitente del mensaje. El valor predeterminado del submandato <b>R</b> es el mensaje actual.

Item	Descripción
R 4	Inicia una respuesta únicamente al remitente del mensaje. El mensaje actual se puede alterar temporalmente escribiendo el número del mensaje después de R. Este ejemplo inicia una respuesta al mensaje 4. El sistema responde con un mensaje similar al siguiente:

```
To: carmen@thor
Subject: Re: Reunión Departamento
```

A continuación, puede escribir la respuesta:

```
Acudiré sin falta.
```

Cuando haya terminado de escribir el texto, pulse el punto (.) o la secuencia de teclas Control-D para enviar el mensaje. Una vez enviada la respuesta, volverá al indicador del buzón.

#### **Creación de un mensaje nuevo desde el buzón**

En el indicador de buzón, puede utilizar el submandato **m** del modo que se muestra en el ejemplo siguiente para crear nuevos mensajes.

Item	Descripción
<b>m Dirección</b>	El parámetro <i>Dirección</i> puede ser cualquier dirección de usuario correcta. Este submandato inicia el editor de correo y le permite crear un mensaje nuevo desde el buzón. Una vez enviado el mensaje, volverá al indicador del buzón.

#### **Reenvío de correo**

Mientras lee el correo, puede que le interese reenviar una determinada nota a otro usuario.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Si reenvía un mensaje seleccionado, inicie el recurso de correo con el mandato **mail**. Tome nota del número del mensaje de correo que desea reenviar.

Esta tarea se puede llevar a cabo utilizando los submandatos **~f** y **~m**.

Si va a estar ausente de la dirección de red normal, puede hacer que se envíe el correo a otra dirección de red creando el archivo **.forward**. Consulte el apartado “Archivos .forward” en la página 32. La nueva dirección puede ser cualquier dirección de correo válida de la red o de una red conectada a la suya. Puede ser la dirección de un compañero de trabajo que se encargará de los mensajes durante su ausencia. Si elige reenviar su correo electrónico, no recibirá copia alguna del correo de entrada en su buzón. Todo el correo se reenviará directamente a la dirección o direcciones que haya especificado.

#### **Reenvío de mensajes seleccionados desde el buzón**

Utilice este procedimiento para reenviar mensajes de correo específicos del buzón.

Para reenviar mensajes de correo específicos:

1. Cree un mensaje nuevo utilizando el submandato **m** y especifique un destinatario escribiendo lo siguiente en el indicador del buzón:

```
m Usuario@Sistpral
```

donde *Usuario* hace referencia al nombre de inicio de sesión de otro usuario y *Sistpral* es el nombre del sistema del usuario. Si el usuario está en el sistema, puede omitir la parte *@Sistpral* de la dirección.

2. Escriba el nombre del asunto en el indicador **Subject:**
3. Para especificar el número del mensaje de correo que va a reenviar, escriba:

```
~f NúmeroMensaje
```

## O BIEN

```
~m NúmeroMensaje
```

*NúmeroMensaje* identifica el elemento de correo que va a reenviar.

El mandato **mail** visualiza un mensaje similar al siguiente:

```
Interpolating: 1  
(continue)
```

4. Para salir de mail, escriba un punto (.) en una línea en blanco. En el indicador **Cc:**, escriba los nombres adicionales a quienes desea reenviar el mensaje de correo.

### *Reenvío de todo el correo*

Utilice este procedimiento para reenviar todo el correo a otra persona.

Para reenviar todo el correo a otra persona:

1. Entre el mandato **cd** sin parámetros para asegurarse de que está en el directorio inicial.  
Por ejemplo, escriba lo siguiente para el nombre de inicio de sesión **marta**:

```
cd  
pwd
```

El sistema responde con:

```
/home/marta
```

2. Cree un archivo **.forward** en el directorio inicial.

Consulte el apartado “Archivos .forward” en la página 32.

**Nota:** No recibirá ningún correo hasta que suprima el archivo **.forward**.

### *Archivos .forward*

El archivo **.forward** contiene la dirección o las direcciones de red que recibirán el correo de red reenviado.

Las direcciones deben tener el formato *Usuario@Sistpral*. *Usuario* hace referencia al nombre de inicio de sesión de otro usuario y *Sistpral* es el nombre del sistema del usuario. Si el usuario está en el sistema, puede omitir la parte *@Sistpral* de la dirección. Puede utilizar el mandato **cat** para crear un archivo **.forward** del modo siguiente:

```
cat > .forward  
marcos  
juan@saturn  
[END OF FILE]
```

[END OF FILE] representa el carácter de fin de archivo que, en la mayoría de terminales, suele ser la secuencia de teclas Control-D. Debe escribirse en una línea en blanco.

El archivo **.forward** contiene las direcciones de los usuarios a los que desea reenviar su correo. El correo se reenviará a **marcos** en el sistema local y a **juan** en el sistema **saturn**.

Este archivo debe contener direcciones válidas. Si se trata de un archivo nulo (de longitud cero), el correo no se reenviará y se almacenará en el buzón.

**Nota:** No recibirá ningún correo hasta que suprima el archivo **.forward**.

### *Cancelación del correo reenviado*

Para dejar de reenviar correo, suprima el archivo **.forward** como se indica a continuación.

Utilice el mandato **rm** para eliminar el archivo **.forward** del directorio inicial:

```
rm .forward
```

## **Envío de un aviso de mensaje de ausencia por vacaciones**

Utilice este procedimiento para preparar y enviar un aviso de mensaje de ausencia por vacaciones.

El programa de correo (mail) debe estar instalado en el sistema.

1. Para inicializar el mensaje de vacaciones, escriba lo siguiente en el directorio \$HOME (de inicio de sesión):

```
vacation -I
```

Este mandato crea un archivo .vacation.dir y un archivo .vacation.pag en que se guardan los nombres de las personas que envían mensajes.

2. Modifique el archivo .forward.

Por ejemplo, carlos escribe la sentencia siguiente en el archivo .forward:

```
carlos, |"/usr/bin/vacation carlos"
```

La primera entrada carlos corresponde al nombre del usuario a quien se reenvía el correo. La segunda entrada carlos corresponde al nombre de usuario del remitente del mensaje de vacaciones. El remitente del mensaje de correo recibe un mensaje de vacaciones de carlos cada semana, independientemente de la cantidad de mensajes que se envíen a carlos desde el remitente. Si hace que se reenvíe el correo a otra persona, el mensaje de correo del remitente se reenvía a la persona definida en el archivo .forward.

Utilice el distintivo **-f** para modificar los intervalos de frecuencia a los que se envía el mensaje. Por ejemplo, carlos escribe la sentencia siguiente en el archivo .forward:

```
carlos, |"/usr/bin/vacation -f10d carlos"
```

El remitente del mensaje de correo recibe un mensaje de vacaciones de carlos cada diez días, independientemente de la cantidad de mensajes que se envíen a carlos desde el remitente.

3. Para enviar un mensaje a cada persona que le envía correo, cree el archivo \$HOME/.vacation.msg y añada el mensaje a este archivo.

A continuación se muestra un ejemplo de un mensaje de ausencia por vacaciones:

```
From: carl@odin.austin (Carlos Ruiz)
Subject: Estoy de vacaciones.
Estaré de vacaciones hasta el 1 de octubre. Si tiene algún asunto urgente,
póngase en contacto con Juan Torres <torres@zeus.valhalla>.
--carlos
```

El remitente recibe el mensaje que está en el archivo \$HOME/.vacation.msg o, si el archivo no existe, el remitente recibe el mensaje predeterminado que se encuentra en el archivo /usr/share/lib/vacation.def. Si no existe ninguno de estos archivos, no se envían respuestas automáticas al remitente del mensaje de correo y no se genera ningún mensaje de error.

Para cancelar el mensaje de ausencia por vacaciones, elimine el archivo .forward, el archivo .vacation.dir, el archivo .vacation.pag y el archivo .vacation.msg del directorio \$HOME (inicio de sesión) del modo siguiente:

```
rm .forward .vacation.dir .vacation.pag .vacation.msg
```

## **Envío y recepción de correo secreto**

Para enviar correo secreto, en el indicador de línea de mandatos del sistema, utilice el mandato **xsend** del modo mostrado en el ejemplo siguiente.

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Debe haberse configurado una contraseña utilizando el mandato **enroll**.

Item	Descripción
<b>xsend beatriz</b>	En este ejemplo, se está dirigiendo correo secreto al nombre de inicio de sesión <b>beatriz</b> . Al pulsar Intro, se utilizará un editor de una sola línea para escribir el texto del mensaje. Cuando haya terminado de escribir el mensaje, pulse la secuencia de teclas Control-D o un . (punto) para salir del editor de correo y enviar el mensaje. El mandato <b>xsend</b> cifra el mensaje antes de enviarlo.

1. Para recibir correo secreto, en el indicador de línea de mandatos del sistema, escriba:

```
mail
```

El sistema visualiza la lista de mensajes del buzón del sistema. El programa de correo secreto le envía una notificación de que ha recibido correo secreto. La línea del mensaje será similar a la siguiente:

```
Mail [5.2 UCB] Type ? para obtener ayuda.  
"/usr/spool/mail/linda": 4 messages 4 new (4 mensajes 4 nuevos)  
>N 1 roberto Mié Abr 14 15:23 4/182 "correo secreto de roberto@Zeus"
```

El texto del mensaje le indica que debe leer el correo secreto en su sistema principal utilizando el mandato **xget**.

2. En el indicador de la línea de mandatos del sistema, escriba:

```
xget
```

Se le solicitará la contraseña que se ha configurado anteriormente utilizando el mandato **enroll**. Después de escribir la contraseña, se visualizará el indicador del mandato **xget**, seguido de un listado del correo secreto. El programa de correo se utiliza para visualizar este tipo de correo. Debe entrar el submandato **q** si desea dejar los mensajes leídos y no leídos en el buzón secreto y evitar que el mandato **xget** suprima los mensajes.

### Información de ayuda para el correo

Puede obtener información de ayuda sobre cómo utilizar el programa de correo (mail) mediante el uso de los mandatos **?**, **man** o **info**.

Item	Descripción
Para obtener ayuda en el buzón	Entre <b>?</b> o <b>help</b> en el indicador de buzón.  El submandato <b>?</b> y <b>help</b> visualizan un resumen de submandatos de buzón comunes.  Puede visualizar una lista de todos los submandatos de buzón (sin resumen) entrando el submandato <b>(1)ist</b> .
Para obtener ayuda en el editor de correo	Escriba <b>~?</b> en el indicador del editor de correo.  El submandato <b>~?</b> visualiza un resumen de los submandatos del editor de correo más comunes.
Para obtener ayuda en el correo secreto	Escriba <b>?</b> en el indicador del editor de correo.  El submandato <b>?</b> visualiza un resumen de los submandatos comunes del correo secreto.

Item	Descripción
Para obtener ayuda utilizando páginas manuales	Escriba <code>man mail</code> en el indicador de la línea de mandatos del sistema.
	En este ejemplo, <code>mail</code> es el nombre del mandato que se busca. El sistema le proporcionará documentación en formato ASCII sobre el mandato <b>mail</b> . En la marca de continuación (:), pulse Intro para ver el resto del documento.
	El mandato <b>man</b> proporciona información, en formato ASCII, sobre diversos temas de consulta, tales como mandatos, subrutinas y archivos.

### Opciones de personalización del programa de correo

Se pueden personalizar los mandatos y opciones de los archivos `.mailrc` y `/usr/share/lib/Mail.rc` para adaptarlos a sus necesidades personales de correo.

Consulte el apartado “[Opciones de habilitación e inhabilitación de correo](#)” en la página 36 para obtener información sobre las opciones de correo.

Entre las características de una sesión de correo que puede personalizar se incluyen:

- **Mensajes de solicitud del asunto de un mensaje.** Al entrar el mandato **mail**, el programa le solicita que complete un campo **Subject**: . Cuando aparezca este mensaje de solicitud, puede escribir un resumen del tema del mensaje. Dicho resumen se incluirá en el inicio del mensaje cuando lo lea el destinatario. Consulte el apartado “[Mensaje de solicitud de los campos Subject: y Carbon Copy \(Cc:\)](#)” en la página 37.
- **Mensajes de solicitud para que los usuarios obtengan una copia de un mensaje.** Puede personalizar el archivo `.mailrc` para que cuando envíe un mensaje, el programa de correo le solicite los nombres de otros usuarios que deben recibir copias del mensaje. Consulte el apartado “[Mensaje de solicitud de los campos Subject: y Carbon Copy \(Cc:\)](#)” en la página 37.
- **Alias o listas de distribución.** Si envía correo en una red de dimensiones considerables o envía a menudo el mismo mensaje a una gran cantidad de personas, el hecho de tener que escribir largas direcciones para cada destinatario puede resultar una tarea pesada. Para simplificar este proceso, cree un alias o una lista de distribución en el archivo `.mailrc`. Un *alias* es un nombre que se define que se puede utilizar en lugar de una dirección de usuario individual. Una *lista de distribución* es un nombre que se define que se puede utilizar en lugar de un grupo de direcciones de usuario. Consulte el apartado “[Alias y listas de distribución](#)” en la página 37.
- **Número de líneas visualizadas al leer los mensajes.** Puede modificar el número de líneas de las cabeceras de mensaje o del texto del mensaje que se desplazan por la pantalla. Consulte el apartado “[Cambios en el número de cabeceras de mensaje o líneas de texto de mensaje visualizadas en el programa de correo](#)” en la página 38.
- **Información listada en los mensajes.** Puede desactivar las cabeceras de los mensajes como, por ejemplo, el campo `message-id` definido por la máquina. Consulte el apartado “[Visualización de información en un mensaje](#)” en la página 40.
- **Directorio de carpetas para almacenar mensajes.** Puede crear un directorio especial para almacenar mensajes. Puede utilizar el submandato acotado + (signo de suma) para designar dicho directorio al almacenar mensajes o al consultar carpetas. Consulte el apartado “[Creación de carpetas predeterminadas para almacenar mensajes](#)” en la página 41.
- **Archivo de anotaciones cronológicas para registrar los mensajes de salida.** Puede indicar al programa **mail** que registre todos los mensajes de salida en un archivo o un subdirectorio del directorio inicial. Consulte el apartado “[Creación de carpetas predeterminadas para almacenar mensajes](#)” en la página 41.
- **Editores para escribir mensajes.** Además del editor de correo, puede elegir otros dos editores para editar mensajes. Consulte el apartado “[Editores de texto para escribir mensajes](#)” en la página 42.

Para obtener más información sobre cómo personalizar el programa de correo, consulte los temas siguientes.

### Opciones de habilitación e inhabilitación de correo

Las opciones pueden ser binarias o con un valor.

Las opciones binarias son **set** o **unset**, mientras que las opciones con un valor pueden **establecerse** (set) con un valor específico.

**Nota:** El formato **unset opción** es equivalente a **set no opción**.

Utilice el mandato **pg** para ver el archivo `/usr/share/lib/Mail.rc`. El contenido del archivo `/usr/share/lib/Mail.rc` define la configuración del programa de correo. Modifique la configuración del sistema para el programa de correo creando un archivo `$HOME/.mailrc`. Cuando ejecute el mandato **mail**, los submandatos del archivo `.mailrc` alteran temporalmente los submandatos similares en el archivo `/usr/share/lib/Mail.rc`. Las opciones de `.mailrc` se pueden personalizar y son válidas cada vez que utiliza el programa de correo.

Para ejecutar mandatos de correo que están almacenados en un archivo, utilice el submandato **source**.

#### Prerrequisitos

El programa de correo (mail) debe estar instalado en el sistema.

#### Habilitación de las opciones de correo

Estos submandatos de buzón se utilizan comúnmente para modificar las características de una sesión de correo.

##### Item      Descripción

**set**      Habilita las opciones de correo.

**source**      Habilita las opciones de correo que están almacenadas en un archivo. Al leer el correo, puede emitir este submandato desde el indicador del buzón:

```
source  
NombreVía
```

donde *NombreVía* es la vía de acceso y el archivo que contiene los mandatos de correo. Los mandatos de este archivo prevalecen sobre los valores anteriores de cualquier mandato similar el tiempo que dure la sesión actual. También puede alterar las características de la sesión de correo actual escribiendo mandatos en el indicador del buzón.

Estas opciones pueden establecerse desde el buzón o especificando entradas en el archivo `.mailrc`.

#### Visualización de las opciones de correo habilitadas

Al leer el correo, entre el submandato **set** sin argumentos para listar todas las opciones `.mailrc` habilitadas.

En esta lista, también puede ver si se ha seleccionado un directorio de carpetas y si se ha configurado un archivo de anotaciones cronológicas para registrar los mensajes de salida.

Escriba lo siguiente en el indicador del buzón:

```
set
```

Se muestra un mensaje similar al siguiente:

```
ask  
metoo  
toplines 10
```

En este ejemplo, se han habilitado dos opciones binarias: **ask** y **metoo**. En la lista no figura la entrada **askcc**. Esto indica que la opción **askcc** no está habilitada. A la opción **toplines**, se le ha asignado el valor

10. Las opciones **ask**, **metoo**, **askcc** y **toplines** se describen en la sección [.mailrc File Format](#) de la publicación *Referencia de archivos*.

#### *Inhabilitación de las opciones de correo*

Estos submandatos de buzón se utilizan comúnmente para modificar las características de una sesión de correo.

<b>Item</b>	<b>Descripción</b>
<b>unset</b>	Inhabilita las opciones de correo.
<b>unalias</b>	Suprime los nombres de alias especificados.
<b>ignore</b>	Suprime los campos de cabecera de mensaje.

Estas opciones pueden establecerse desde el buzón o especificando entradas en el archivo `.mailrc`.

**Nota:** El formato **unset opción** es equivalente a **set no opción**.

#### *Mensaje de solicitud de los campos Subject: y Carbon Copy (Cc:)*

Cuando se editan los mensajes de solicitud de los campos **Subject:** y **Cc:**, se deben satisfacer los siguientes requisitos.

##### Prerrequisitos

El programa de correo (mail) debe estar instalado en el sistema.

##### *Habilitación o inhabilitación del indicador del campo Subject:*

Utilice los mandatos **set** y **unset** para habilitar e inhabilitar el campo **Subject:**.

Puede habilitar o inhabilitar el campo **Subject:** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>set ask</b>	El indicador del campo <b>Subject:</b> se habilita editando el archivo <code>.mailrc</code> , opción <b>ask</b> .
<b>unset ask</b>	El indicador del campo <b>Subject:</b> se inhabilita editando el archivo <code>.mailrc</code> , opción <b>ask</b> .

##### *Habilitación o inhabilitación del indicador del campo Carbon Copy (Cc:)*

Utilice los mandatos **set** y **unset** para habilitar e inhabilitar el campo **Cc:**.

Puede habilitar o inhabilitar el campo **Cc:** del modo que se muestra en los ejemplos siguientes:

<b>Item</b>	<b>Descripción</b>
<b>set askcc</b>	El indicador del campo de Copia ( <b>Cc:</b> ) se habilita editando el archivo <code>.mailrc</code> , opción <b>askcc</b> .
<b>unset askcc</b>	El indicador del campo de Copia ( <b>Cc:</b> ) se inhabilita editando el archivo <code>.mailrc</code> , opción <b>askcc</b> .

#### *Alias y listas de distribución*

Mediante la creación de alias y listas de distribución, puede gestionar más fácilmente los destinatarios y las direcciones que utiliza de forma habitual.

Antes de crear un alias o una lista de distribución, asegúrese de que se cumplan las siguientes condiciones:

1. El programa de correo (mail) debe estar instalado en el sistema.
2. Debe conocer el nombre y las direcciones de los usuarios que desea incluir en la lista de distribución o el alias.

Puede crear un alias o una lista de distribución de los modos siguientes:

Item	Descripción
<b>alias</b>	<p>isa isabel@gtwn</p> <p>En este ejemplo, se ha listado el alias <b>isa</b> para el usuario <b>isabel</b> en la dirección <b>gtwn</b>. Una vez añadida esta línea al archivo <b>\$HOME/.mailrc</b>, para enviar un mensaje a Isabel, escriba lo siguiente en el indicador de la línea de mandatos:</p> <pre>mail isa</pre> <p>Ahora ya puede enviar correo a Isabel utilizando el alias <b>isa</b>.</p>
<b>alias</b>	<p>dpto eva@merlin ana@anchor julio@zeus jorge carlos</p> <p>Una vez añadida esta línea al archivo <b>\$HOME/.mailrc</b>, para enviar un mensaje al departamento, escriba lo siguiente en el indicador de la línea de mandatos:</p> <pre>mail dpto</pre> <p>Ahora, el mensaje que cree y envíe se dirigirá a <b>eva</b> en el sistema <b>merlin</b>, a <b>ana</b> en el sistema <b>anchor</b>, a <b>julio</b> en el sistema <b>zeus</b> y a <b>jorge</b> y <b>carlos</b> en el sistema local.</p>

Para listar los alias y las listas de distribución, escriba lo siguiente en el indicador del buzón:

**alias**

O BIEN

```
a
```

Se visualizará un listado de alias o de listas de distribución.

#### *Cambios en el número de cabeceras de mensaje o líneas de texto de mensaje visualizadas en el programa de correo*

Si modifica el archivo **.mailrc**, puede personalizar la posibilidad de desplazarse por listas del buzón o por los mensajes reales.

Para poder realizar estos cambios, el programa de correo (mail) debe estar instalado en el sistema.

#### *Modificación del número de líneas visualizadas de la lista de mensajes*

Cada mensaje del buzón tiene una cabecera de una línea en la lista de mensajes. Si tiene más de 24 mensajes, las primeras cabeceras de la lista de mensajes desaparecerán por la parte superior de la pantalla. La opción **set screen** controla cuántas líneas de la lista se visualizan a la vez.

Para cambiar el número de líneas de la lista de mensajes que se pueden visualizar a la vez, escriba lo siguiente en el archivo **\$HOME/.mailrc**:

```
set screen=20
```

En este ejemplo, el sistema visualizará 20 cabeceras de mensaje al mismo tiempo. Utilice el submandato **h** o **z** para ver más grupos de cabeceras. También puede escribir este submandato en el indicador del buzón.

#### *Modificación del número de líneas visualizadas en un mensaje largo*

Si desea ver un mensaje que contiene más de 24 líneas, las primeras líneas de éste desaparecerán por la parte superior de la pantalla. Puede utilizar el mandato **pg** desde el correo para examinar los mensajes largos si ha incluido la opción **set crt** en el archivo **.mailrc**.

La opción **set crt** controla cuántas líneas debe contener un mensaje antes de que se inicie el mandato **pg**.

Por ejemplo, si utiliza el submandato **t** para leer un mensaje largo, sólo se visualizará una pantalla (o página). La página vendrá seguida del signo de dos puntos para indicarle que hay más páginas. Pulse la tecla Intro para visualizar la siguiente página del mensaje. Una vez visualizada la última página, aparecerá un indicador similar a éste:

```
EOF:
```

En el indicador, puede entrar cualquier submandato **pg** válido. También puede ver páginas anteriores, buscar series de caracteres en el mensaje o abandonar la lectura de éste para volver al indicador del buzón.

La opción **set crt** se entra en el archivo **.mailrc** como:

```
set crt=Líneas
```

Por ejemplo:

```
set crt=20
```

especifica que un mensaje debe tener 20 líneas para que se inicie el mandato **pg**. El mandato **pg** se inicia cuando se leen mensajes con más de 20 líneas.

*Modificación del número de líneas visualizadas en la parte de superior de un mensaje*

El submandato **top** le permite explorar un mensaje sin leerlo completamente.

Puede controlar la cantidad de líneas que se visualizan estableciendo la opción **toplines** del modo siguiente:

```
set toplines=Líneas
```

En este submandato, la variable *Líneas* corresponde al número de líneas que se visualizan con el submandato **top**, empezando por arriba e incluyendo todos los campos de cabecera.

Por ejemplo, si el usuario Arturo tiene la línea siguiente en el archivo **.mailrc**:

```
set toplines=10
```

cuando Arturo ejecute el mandato **mail** para leer los mensajes nuevos, se visualizará el texto siguiente:

```
Mail Type ? para obtener ayuda.  
"/usr/mail/amy": 2 messages 2 new> (2 mensajes 2 nuevos)  
N 1 jorge    Mie Ene 6 9:47 11/257 "Reunión Dpto"  
N 2 marcos   Mie Ene 6 12:59 17/445 "Planificador Proyecto"
```

Cuando Arturo utilice el submandato **top** para examinar los mensajes, se visualizará el siguiente mensaje parcial:

```
top 1  
Message 1:  
From jorge Mie Ene 6 9:47 CST 1988  
Received: by zeus  
        id AA00549; Mie, 6 Ene 88 9:47:46 CST  
Date: Mie, 6 Ene 88 9:47:46 CST  
From: jorge@zeus  
Message-Id: <8709111757.AA00178>  
To: arturo@zeus  
Subject: Reunión Dpto  
El viernes a la 1:30 se celebrará la reunión  
en la sala de conferencias. Hablaremos
```

El mensaje se visualizará parcialmente porque **toplines** está establecido con el valor 10. Sólo se visualizan las líneas 1 (campo **Received:**) a 10 (segunda línea del cuerpo del mensaje). La primera línea, **From george Wed Jan 6 9:47 CST 1988**, siempre está presente y no se cuenta en la opción **toplines**.

## **Visualización de información en un mensaje**

Si modifica el archivo `.mailrc`, puede controlar la información de cabecera que se visualiza en un mensaje.

Puede que parte de dicha información de cabecera ya esté desactivada. Examine el archivo `/usr/share/lib/Mail.rc` para comprobar los archivos de cabecera omitidos.

### Prerrequisitos

El programa de correo (mail) debe estar instalado en el sistema.

*Cómo impedir que se visualicen las cabeceras Date, From y To*

Cada mensaje consta de varios campos de cabecera al principio. Estos campos se visualizan al leer un mensaje. Puede utilizar el submandato **ignore** para suprimir la visualización de los campos de cabecera cuando se lee un mensaje.

El formato para el submandato **ignore** es:

```
ignore [ListaCampos]
```

La variable *ListaCampos* puede estar compuesta de uno o más nombres de campos que desea ignorar al visualizar un mensaje. Por ejemplo, si el usuario Arturo incluye la línea siguiente en su archivo `.mailrc`:

```
ignore date from to
```

y el archivo `/usr/share/lib/Mail.rc` contiene la línea:

```
ignore received message-id
```

el resultado del uso del submandato **t** será:

```
t 1
Message 1:
From jorge Mie Ene 6 9:47 CST 1988
Subject: Reunión Dpto
El viernes a la 1:30 se celebrará la reunión
en la sala de conferencias. Hablaremos de
los nuevos procedimientos para utilizar el programa de
planificación del proyecto desarrollado por nuestro departamento.
```

Los campos **Received**: **Date**: **From**: **Message-Id**: y **To**: no se visualizan. Para ver estos campos, utilice los submandatos **T**, **P** o **top**.

**Nota:** En el ejemplo, se visualiza la línea **From**. No es la misma que la del campo **From**: que se ha listado en la *ListaCampos* del submandato **ignore**.

*Listado de los campos de cabecera ignorados*

Utilice el submandato **ignore** para listar los campos de cabecera ignorados.

Para obtener una lista de los campos de cabecera que se ignoran actualmente, escriba lo siguiente en el indicador del buzón:

```
ignore
```

Se visualizará una lista de todas las cabeceras ignoradas en este momento. Por ejemplo:

```
mail-from
message-id
return-path
```

*Restablecimiento de los campos de cabecera*

Para restablecer los campos de cabecera, utilice el submandato **retain**.

Por ejemplo:

```
retain date
```

### *Listado de los campos de cabecera retenidos*

Utilice el submandato **retain** para listar los campos de cabecera retenidos.

Para ver qué campos de cabecera están retenidos actualmente, entre el submandato **retain** sin ningún parámetro de campo de cabecera.

### *Cómo impedir que se visualice el mensaje de cabecera*

El mensaje de cabecera de correo es la línea situada en la parte superior de la lista de mensajes que muestra el nombre del programa de correo cuando se emite el mandato **mail**.

Es parecido a la línea siguiente:

```
Mail [5.2 UCB] [Workstation 3.1] Type ? para obtener ayuda.
```

Para ocultar el mensaje de cabecera cuando inicie el programa de correo, añada la línea siguiente al archivo \$HOME/.mailrc:

```
set quiet
```

Otra opción que suprime el mensaje de cabecera de **mail** es:

```
set noheader
```

Si especifica esta opción en el archivo .mailrc, la lista de mensajes del buzón no se visualizará. Cuando inicie el programa **mail**, la única respuesta es el indicador del buzón. Puede obtener una lista de mensajes escribiendo el submandato (**h**eader).

### *Combinación de los mandatos delete y print*

Utilice la opción autoprint para combinar los submandatos delete y print.

Después de leer un mensaje, puede suprimirlo con el submandato **d**. Puede visualizar el mensaje siguiente mediante el submandato **p**. Combine estos submandatos escribiendo la línea siguiente en el archivo .mailrc:

```
set autoprint
```

Con la opción **set autoprint** del archivo .mailrc, el submandato **d** suprime el mensaje actual y visualiza el siguiente.

### *Creación de carpetas predeterminadas para almacenar mensajes*

Las carpetas predeterminadas le permiten almacenar mensajes.

El programa de correo (mail) debe estar instalado en el sistema.

Utilice el procedimiento siguiente si desea crear un directorio de buzón de cartas para almacenar mensajes en carpetas:

1. Para comprobar si la opción **set folder** se ha habilitado en el archivo .mailrc, escriba en el indicador del buzón:

```
set
```

Si se ha habilitado la opción **set folder**, el sistema responde con el siguiente mensaje:

```
folder /home/jorge/cartas
```

En este ejemplo, cartas es el directorio en que se almacenarán las carpetas de correo.

2. Si la opción **set folder** no se ha habilitado, cree una entrada **set folder** en el archivo .mailrc:

```
set folder=/home/george/letters
```

En este ejemplo, /home/jorge es el directorio inicial de Jorge y cartas es el directorio en el que se almacenarán las carpetas de correo. La opción **set folder** le permitirá utilizar la anotación taquigráfica de signo más (+) para guardar mensajes en el directorio cartas.

3. Si no existe ningún directorio **cartas**, deberá crearlo en el directorio inicial. Desde el directorio inicial, escriba lo siguiente en la línea de mandatos del sistema:

```
mkdir cartas
```

Utilice el procedimiento siguiente para mantener un registro de los mensajes enviados a otras personas:

1. Escriba la siguiente sentencia en el archivo **.mailrc**:

```
set record=cartas/correosal
```

2. Si no existe ningún directorio **cartas**, deberá crearlo en el directorio inicial. Desde el directorio inicial, escriba lo siguiente en la línea de mandatos del sistema:

```
mkdir cartas
```

3. Para leer copias de los mensajes enviados a otros usuarios, escriba:

```
mail -f +correosal
```

En este ejemplo, el archivo **correosal** contiene copias de los mensajes que ha enviado a otros usuarios.

#### **Editores de texto para escribir mensajes**

Utilice la opción **set EDITOR=NombreVía** para definir el editor de texto con el que escribe los mensajes.

El programa de correo (mail) debe estar instalado en el sistema.

##### **Item**

**set EDITOR= NombreVía**

##### **Descripción**

Esta opción del archivo **.mailrc** define el editor que se activa con la secuencia de teclas **~e**. El valor de **NombreVía** debe ser el nombre completo de la vía de acceso al programa editor que desea utilizar.

Para cambiar al editor e, mientras se encuentra en el programa de correo, escriba:

```
~e
```

Esta secuencia activa el editor e u otro editor que haya definido en el archivo **.mailrc**. Edite el mensaje de correo utilizando este editor.

**set VISUAL=NombreVía**

Esta opción del archivo **.mailrc** define el editor que se activa con la secuencia de teclas **~v**. El valor de **NombreVía** debe ser el nombre de vía de acceso completo al programa editor que desea utilizar. El valor predeterminado es **/usr/bin/vi**.

Para cambiar el editor vi mientras se encuentra en el programa de correo, escriba:

```
~v
```

Esta secuencia activa el editor vi u otro editor que haya definido en el archivo **.mailrc**. Edite el mensaje de correo utilizando este editor.

#### **Submandatos del mandato mail**

El mandato **mail** utiliza varios mandatos que realizan funciones diferentes.

Este tema se utiliza como referencia para el mandato **mail** y los submandatos.

#### **Mandatos para ejecutar mail**

Utilice estos mandatos de sistema para ejecutar mail.

<b>Item</b>	<b>Descripción</b>
<b>mail</b>	Visualiza el buzón del sistema.
<b>mail -f</b>	Visualiza su buzón personal ( <b>mbox</b> ).
<b>mail -f +carpeta</b>	Visualiza una carpeta de correo.
<b>mail usuario@ dirección</b>	Direcciona un mensaje a un usuario específico.

#### **Submandatos de buzón del programa de correo**

Cuando el programa de correo procesa un buzón, visualiza el indicador del mismo para indicar que está esperando entrada.

El indicador del buzón es un símbolo & que se visualiza al principio de una línea nueva. Desde este indicador puede especificar cualquiera de los submandatos del buzón.

#### **Submandatos de control de programa de correo**

Utilice estos submandatos para controlar el programa de correo (mail).

<b>Item</b>	<b>Descripción</b>
<b>q</b>	Sale del programa y aplica los submandatos del buzón especificados en esta sesión.
<b>x</b>	Sale del programa y restaura el buzón a su estado original.
<b>!</b>	Inicia un shell, ejecuta un mandato y le devuelve al buzón.
<b>cd dir</b>	Cambia a los directorios <b>dir</b> o \$HOME.

#### **Submandatos de visualización del programa de correo**

Utilice estos submandatos para controlar las visualizaciones del programa de correo (mail).

<b>Item</b>	<b>Descripción</b>
<b>t</b>	Visualiza los mensajes de <i>lista_mjes</i> o el mensaje actual.
<b>n</b>	Visualiza el siguiente mensaje.
<b>f lista_mjes</b>	Visualiza las cabeceras de los mensajes de <i>lista_mjes</i> o del mensaje actual si no se especifica <i>lista_mjes</i> .
<b>h num</b>	Visualiza las cabeceras de los grupos que contienen el mensaje <i>num</i> .
<b>top num</b>	Visualiza un mensaje parcial.
<b>set</b>	Visualiza una lista de todas las opciones de <b>.mailrc</b> habilitadas.
<b>ignore</b>	Visualiza una lista de todos los campos de cabecera ignorados.
<b>folder</b>	Visualiza el número de mensajes de la carpeta actual, junto con el nombre de la vía de acceso de la carpeta.

#### **Manejo de mensajes**

Utilice estos submandatos para editar, suprimir, volver a llamar, añadir o retener mensajes.

<b>Item</b>	<b>Descripción</b>
<b>e num</b>	Edita el mensaje <i>num</i> (el editor predeterminado es e).
<b>d lista_mjes</b>	Suprime los mensajes de <i>lista_mjes</i> o el mensaje actual.
<b>u lista_mjes</b>	Llama a los mensajes suprimidos de <i>lista_mjes</i> .
<b>s lista_mjes +archivo</b>	Añade mensajes (con cabeceras) a <i>archivo</i> .
<b>w lista_mjes +archivo</b>	Añade mensajes (sólo texto) a <i>archivo</i> .
<b>pre lista_mjes</b>	Guarda los mensajes en el buzón del sistema.

### *Submandatos de correo nuevo*

Utilice estos submandatos al crear mensajes de correo nuevos.

<b>Item</b>	<b>Descripción</b>
<b>m</b> <i>listadir</i>	Crea y envía un mensaje nuevo a las direcciones de <i>listadir</i> .
<b>r</b> <i>lista_mjes</i>	Envía una respuesta a los remitentes y destinatarios de los mensajes.
<b>R</b> <i>lista_mjes</i>	Envía una respuesta únicamente a los remitentes de los mensajes.
<b>a</b>	Visualiza una lista de los alias y sus direcciones.

### *Submandatos de editor de correo*

Cuando el editor de correo se procesa, visualiza el indicador de editor de correo para indicar que está esperando entrada.

Desde este indicador puede especificar cualquiera de los submandatos del editor de correo.

### *Submandatos de control de editor de correo*

Utilice los siguientes submandatos para controlar el editor de correo.

<b>Item</b>	<b>Descripción</b>
<b>~q</b>	Sale del editor sin guardar ni enviar el mensaje actual.
<b>~p</b>	Visualiza el contenido del almacenamiento intermedio de mensajes.
<b>~: mcmd</b>	Ejecuta un submandato de buzón ( <i>mcmd</i> ).
<b>EOT</b>	Envía el mensaje (Control-D en la mayoría de los terminales).
<b>.</b>	Envía el mensaje actual.

### *Submandatos de adiciones a la cabecera*

Utilice estos submandatos para añadir diferentes elementos de cabecera a los mensajes.

<b>Item</b>	<b>Descripción</b>
<b>~h</b>	Añade información a los campos <b>To:</b> , <b>Subject:</b> , <b>Cc:</b> y <b>Bcc:</b> .
<b>~t</b> <i>listadir</i>	Añada las direcciones de usuario de <i>listadir</i> al campo <b>To:</b> .
<b>~s</b> <i>asunto</i>	Establece el campo <b>Subject</b> en la serie especificada por <i>subject</i> .
<b>~c</b> <i>listadir</i>	Añade las direcciones de usuario de <i>listadir</i> al campo <b>Cc:</b> (copia).
<b>~b</b> <i>listadir</i>	Añade las direcciones de usuario de <i>listadir</i> al campo <b>Bcc :</b> (copia oculta).

### *Submandatos de adiciones al mensaje*

Utilice estos submandatos para añadir contenido a un mensaje.

<b>Item</b>	<b>Descripción</b>
<b>~d</b>	Añade el contenido de <i>dead.letter</i> al mensaje.
<b>~r</b> <i>nombarch</i>	Añade el contenido de <i>nombarch</i> al mensaje.
<b>~f</b> <i>listanum</i>	Añade el contenido de los números de mensaje de <i>listanum</i> .
<b>~m</b> <i>listanum</i>	Añade y sangra el contenido de los números de mensaje de <i>listanum</i> .

### *Submandatos de cambio de mensaje*

Utilice estos submandatos para editar mensajes.

<b>Item</b>	<b>Descripción</b>
<b>~e</b>	Edita el mensaje utilizando el editor e (el valor predeterminado es e).

<b>Item</b>	<b>Descripción</b>
<b>~v</b>	Edita el mensaje utilizando el editor vi (el valor predeterminado es vi).
<b>~wnombarch</b>	Graba el mensaje en <i>nombarch</i> .
<b>~! mandato</b>	Inicia un shell, ejecuta <i>mandato</i> y devuelve al editor.
<b>~  mandato</b>	Conduce el mensaje a la entrada estándar de <i>mandato</i> y lo sustituye por la salida estándar del mismo.

#### **Submandatos de correo secreto**

Cuando el programa de correo secreto procesa un buzón secreto, visualiza el indicador del mismo para indicar que está esperando entrada.

El indicador del buzón secreto es un ? (signo de interrogación) y aparece al principio de una nueva línea. Desde este indicador puede especificar cualquiera de los submandatos del buzón secreto.

#### *Submandatos de correo secreto*

Utilice los siguientes submandatos para enviar correo secreto.

<b>Item</b>	<b>Descripción</b>
<b>xsend beatriz</b>	Direcciona un mensaje a un usuario específico.
<b>xget</b>	Visualiza el buzón secreto.

#### **Tareas de buzón**

Los submandatos siguientes llevan a cabo diversas tareas de buzón.

<b>Item</b>	<b>Descripción</b>
<b>q</b>	Sale del programa, manteniendo los mensajes no leídos.
<b>n</b>	Suprime el mensaje actual y visualiza el siguiente.
<b>d</b>	Suprime el mensaje actual y visualiza el siguiente.
Tecla de retorno	Suprime el mensaje actual y visualiza el siguiente.
!	Ejecuta un mandato de shell.
<b>s</b>	Guarda el mensaje en el archivo indicado o en mbox.
<b>w</b>	Guarda el mensaje en el archivo indicado o en mbox.

#### **Tareas de gestión de correo**

El responsable de estas tareas es el gestor de correo.

1. Configure el archivo /etc/rc.tcpip para que el daemon **sendmail** se inicie en el tiempo de arranque del sistema. Consulte el apartado “[Inicio del daemon sendmail durante el arranque del sistema](#)” en la página 46.
2. Personalice el archivo de configuración /etc/mail/sendmail.cf. El archivo /etc/mail/sendmail.cf predeterminado está configurado para que se pueda entregar correo local y correo TCP/IP. Para entregar correo mediante BNU, debe personalizar el archivo /etc/mail/sendmail.cf. Consulte el [Archivo sendmail.cf](#) en la publicación *Referencia de archivos* para obtener más información.
3. Defina el alias de correo de todo el sistema y el alias de correo de todo el dominio en el archivo /etc/mail/aliases. Consulte el apartado “[Alias de correo](#)” en la página 46 para obtener más información.
4. Gestione la cola de correo. Consulte el apartado “[Cola de correo](#)” en la página 48 para obtener más información.

5. Gestione el registro de correo. Consulte el apartado “[Registro de correo](#)” en la página 53 para obtener más información.

### **Inicio del daemon sendmail durante el arranque del sistema**

Para configurar el archivo /etc/rc.tcpip de modo que el daemon **sendmail** también se inicie cuando se arranque el sistema, utilice este procedimiento.

1. Edite el archivo /etc/rc.tcpip mediante el editor de texto que prefiera.
2. Para iniciar automáticamente el daemon sendmail de MTA cuando arranque el sistema, busque la línea que empieza por start /usr/lib/sendmail.  
De forma predeterminada, esta línea no está comentada, lo que significa que no hay ningún signo de almohadilla (#) al principio de la línea. Sin embargo, si está comentada, suprima la almohadilla (#).
3. Si desea iniciar el ejecutor de colas del cliente sendmail cuando arranque el sistema, añada la siguiente línea al archivo /etc/rc.tcpip para iniciar el mandato **sendmail** como programa de envío de correo (MSP):

```
/usr/lib/sendmail -L sm-msp-queue -Ac -q 30m
```

4. Guarde el archivo /etc/rc.tcpip.

### **Alias de correo**

Los alias correlacionan nombres con listas de direcciones utilizando archivos de alias personales, de todo el sistema y de todo el dominio.

Puede definir tres tipos de alias:

<b>Item</b>	<b>Descripción</b>
<b>personal</b>	Lo definen usuarios individuales en el archivo \$HOME/.mailrc del usuario.
<b>sistema local</b>	Lo define el administrador del sistema de correo en el archivo /etc/mail/aliases. Estos alias se aplican al correo manejado por el programa <b>sendmail</b> en el sistema local. Raramente es necesario cambiar los alias de sistema local.
<b>todo el dominio</b>	De forma predeterminada, <b>sendmail</b> lee /etc/alias para resolver los alias. Para alterar temporalmente el valor predeterminado y utilizar NIS, edite o cree /etc/netsvc.conf y añada la línea:

```
aliases=nis
```

### **Archivo /etc/mail/aliases**

Aquí se describen las propiedades, el contenido y la ubicación del archivo /etc/mail/aliases.

El archivo /etc/mail/aliases consta de una serie de entradas en el formato siguiente:

```
Alias: Nombre1,  
Nombre2, ... NombreX
```

donde *Alias* puede ser cualquier serie alfanumérica que elija (sin incluir caracteres especiales, como @ o !). *Nombre1* a *NombreX* es una serie de uno o más nombres de destinatarios. La lista de nombres puede partirse en una o más líneas. Cada continuación de línea empieza con un espacio o un tabulador. Las líneas en blanco y las líneas que empiezan por # (signo de arroba) son líneas de comentario.

El archivo /etc/mail/aliases debe contener los tres alias siguientes:

<b>Item</b>	<b>Descripción</b>
<b>MAILER-DAEMON</b>	ID del usuario que debe recibir mensajes dirigidos al daemon de programa de correo (mailer). Este nombre se asigna inicialmente al usuario root:

```
MAILER-DAEMON: root
```

Item	Descripción
<b>postmaster</b>	ID del usuario responsable del funcionamiento del sistema de correo local. El alias <b>postmaster</b> define una sola dirección de buzón que es válida en cada sistema de una red. Esta dirección permite a los usuarios enviar consultas al alias <b>postmaster</b> de cualquier sistema, sin conocer la dirección correcta de cualquier usuario de dicho sistema. Este nombre se asigna inicialmente al usuario root:
<b>nobody</b>	ID que debe recibir los mensajes dirigidos a programas como <b>news</b> y <b>msgs</b> . Este nombre se asigna inicialmente a /dev/null:

```
postmaster: root
```

nobody: /dev/null

Para recibir estos mensajes, defina este alias para que sea un usuario válido.

Siempre que cambie este archivo, deberá recompilarlo en un formato de base de datos que el mandato **sendmail** pueda utilizar. Consulte el apartado “[Creación de base de datos de alias](#)” en la página 47.

#### **Creación de un alias local para el correo**

Crear alias locales para el correo permite crear grupos o listas de distribución a los que puede enviar el correo.

En este caso, se añadirán geo@medussa, mark@zeus, ctw@athena y dsf@plato al alias de correo **testers**. Cuando se haya creado el alias **testers**, se concederá a glenda@hera la propiedad del alias.

Cuando se haya añadido el alias **testers** al archivo /etc/mail/aliases, se recompilará la base de datos de alias mediante el mandato **sendmail**. Cuando se haya recompilado la base de datos, se podrá enviar un correo electrónico al alias **testers**.

#### **Cuestiones que deben tenerse en cuenta**

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

Utilice los pasos siguientes para crear un alias de correo local:

1. Abra el archivo /etc/mail/aliases mediante su editor de texto favorito.
2. En una línea en blanco, añada el nombre de alias, seguido por dos puntos y una lista de destinatarios separados por comas. Por ejemplo, la entrada siguiente define el alias **testers**:

```
testers: geo@medussa, mark@zeus, ctw@athena, dsf@plato
```

3. Cree un propietario para el alias. Si el mandato **sendmail** no consigue enviar satisfactoriamente el correo al alias, enviará un mensaje de error al propietario.

Añada una línea en /etc/mail/aliases para especificar el propietario. El formato de esta línea es **owner-groupname: owner**, donde **groupname** es el nombre del alias y **owner** es la dirección de correo electrónico del propietario. En este ejemplo, glenda@hera se convierte en el propietario del alias **testers**:

```
testers: geo@medussa, mark@zeus, ctw@athena, dsf@plato owner-testers: glenda@hera
```

4. Cuando se haya creado el alias, ejecute el mandato **sendmail -bi** para volver a compilar la base de datos de alias. Deberá ejecutar este mandato cada vez que actualice el archivo /etc/mail/aliases.

Ahora puede enviar un correo electrónico al alias **testers**.

#### **Creación de base de datos de alias**

El mandato **sendmail** no utiliza directamente las definiciones de alias en el archivo /etc/mail/aliases del sistema local. En lugar de ello, el mandato **sendmail** lee una versión de gestor de base de datos (dbm) procesada del archivo /etc/mail/aliases.

Puede compilar la base de datos de alias utilizando uno de los métodos siguientes:

- Ejecute el mandato `/usr/sbin/sendmail` utilizando el distintivo **-bi**.
- Ejecute el mandato **newaliases**. Este mandato hace que el mandato **sendmail** lea el archivo `/etc/mail/aliases` del sistema local y cree un archivo nuevo que contenga la información de base de datos de alias. Este archivo está en el formato de Berkeley más eficiente:  
`/etc/mail/aliases.db`
- Ejecute el mandato **sendmail** utilizando el distintivo **Rebuild Aliases** (Volver a crear los alias). Esto vuelve a crear la base de datos de alias automáticamente cuando ésta está anticuada. Puede ser peligroso volver a crear automáticamente en máquinas de carga muy pesada con grandes archivos de alias. Si el tiempo que se tarda para volver a crear la base de datos es mayor que el tiempo de espera (normalmente cinco minutos), existe la posibilidad de que varios procesos inicien simultáneamente el proceso de volver a crear.

**Nota:**

1. Si estos archivos no existen, el mandato **sendmail** no puede procesar el correo y genera un mensaje de error.
2. Si tiene varias bases de datos de alias especificadas, el distintivo **-bi** vuelve a crear todos los tipos de base de datos que conoce (por ejemplo, puede volver a crear bases de datos NDBM (Network Database Management) pero no bases de datos NIS).

El archivo `/etc/netsvc.conf` contiene el orden de los servicios de sistema. Para especificar el orden de servicios de los alias, añada la línea siguiente:

```
aliases=service, service
```

donde `service` puede ser `files` o `nis`. Por ejemplo:

```
aliases=files, nis
```

indica al mandato **sendmail** que intente primero el archivo de alias local y, si eso falla, que intente `nis`. Si `nis` se ha definido como servicio, debe estar en ejecución.

Para obtener más información sobre el archivo `/etc/netsvc.conf`, consulte la publicación *Referencia de archivos*.

## Cola de correo

La cola de correo es un directorio que almacena datos y controla archivos para mensajes de correo que entrega el mandato **sendmail**. De forma predeterminada, la cola de correo es `/var/spool/mqueue`.

Los mensajes de correo se pueden poner en cola por muchas razones.

Por ejemplo:

1. El mandato **sendmail** puede estar configurado para procesar la cola a intervalos determinados, en lugar de inmediatamente. Si es así, los mensajes de correo se deben almacenar temporalmente.
2. Si un sistema principal remoto no responde a una petición de conexión de correo, el sistema de correo pone en cola el mensaje y lo intenta otra vez más tarde.

### Impresión de cola de correo

Se puede imprimir el contenido de la cola utilizando el mandato **mailq** (o especificando el distintivo **-bp** con el mandato **sendmail**).

Estos mandatos producen un listado de los ID de cola, los tamaños de los mensajes, las fechas en que los mensajes han entrado en la cola y los remitentes y destinatarios.

### Archivos de cola de correo

Cada mensaje de la cola tiene varios archivos asociados a él.

Los archivos se denominan de acuerdo con los convenios siguientes:

donde *ID* es un ID de cola de mensaje exclusivo y *Tipo* es una de las letras siguientes que indican el tipo de archivo:

**Item Descripción**

**m**

- d El archivo de datos que contiene el cuerpo de mensaje sin la información de cabecera.
- q El archivo de control de cola. Este archivo contiene la información necesaria para procesar el trabajo.
- t Un archivo temporal. Este archivo es una imagen del archivo q cuando se está volviendo a crear. Se redenomina rápidamente según el archivo q.
- x Un archivo de transcripción que existe durante la vida de una sesión y muestra todo lo que sucede durante dicha sesión.

Por ejemplo, si un mensaje tiene un ID de cola de AA00269, se crean y se suprimen los archivos siguientes en el directorio de colas de correo mientras el mandato **sendmail** intenta entregar el mensaje:

Item	Descripción
dfAA00269	Archivo de datos
qfAA00269	Archivo de control
tfAA00269	Archivo temporal
xfAA00269	Archivo de transcripción

Item	Descripción
dfAA00269	Archivo de datos
qfAA00269	Archivo de control
tfAA00269	Archivo temporal
xfAA00269	Archivo de transcripción

**Archivo de control q**

El archivo de control q contiene una serie de líneas, cada una de las cuales empieza con una letra de código.

**Item Descripción**

**m**

- B** Especifica el body\_type (tipo de cuerpo). El resto de la línea es una serie de texto que define body\_type. Si falta este campo entero, body\_type es de forma predeterminada 7 bits y no se intenta ningún proceso especial. Los valores permitidos son **7BIT** y **8BITMIME**.
- C** Contiene el usuario de control. Para las direcciones de destinatario que son un archivo o un programa, **sendmail** realiza la entrega como propietario del archivo o programa. El usuario de control se establece en el propietario del archivo o del programa. En las direcciones de destinatario que se leen en un archivo **.forward** o **:include:** también se establecerá el usuario de control en el propietario del archivo. Cuando **sendmail** entregue correo a estos destinatarios, lo entregará como el usuario de control y, a continuación, se volverá a convertir en root.
- F** Contiene distintivos de sobre. Los distintivos son cualquier combinación de **w** que establece el distintivo **EF\_WARNING**, **r** que establece el distintivo **EF\_RESPONSE**, **8** que establece el distintivo **EF\_HAS8BIT** y **b** que establece el distintivo **EF\_DELETE\_BCC**. Las demás letras se ignoran en silencio.
- H** Contiene una definición de cabecera. Puede haber cualquier número de estas líneas. El orden en el que aparecen las líneas **H** determina el orden en el mensaje final. Estas líneas utilizan la misma sintaxis que las definiciones de cabecera del archivo de configuración */etc/mail/sendmail.cf*.
- I** Especifica la información de inodo y dispositivo para el archivo df; se puede utilizar para recuperar la cola de correo después de que el disco se haya quedado colgado.
- K** Especifica el tiempo (en segundos) del último intento de entrega.

**Item Descripción****m**

- M** Cuando se pone un mensaje en la cola porque se ha producido un error durante un intento de entrega, la naturaleza del error se almacena en la línea **M**.
- N** Especifica el número total de intentos de entrega.
- O** Especifica el valor del sistema de transferencia de mensajes (MTS) original de ESMTP. Sólo se utiliza para Notificaciones de estado de entrega.
- P** Contiene la prioridad del mensaje actual. La prioridad se utiliza para ordenar la cola. Los números más altos significan prioridades más bajas. La prioridad se incrementa a medida que el mensaje permanece en la cola. La prioridad inicial depende de la clase de mensaje y del tamaño del mensaje.
- Q** Contiene el destinatario original especificado por el campo ORCPT= en una transacción ESMTP. Se utiliza exclusivamente para Notificaciones de estado de entrega. Sólo se aplica a la línea **R** que sigue inmediatamente.
- R** Contiene la dirección de destinatario. Hay una línea para cada destinatario.
- S** Contiene la dirección de remitente. Sólo hay una línea de éstas.
- T** Contiene el hora de creación de mensaje utilizada para calcular cuándo se ha excedido el tiempo de espera del mensaje.
- V** Especifica el número de versión del formato de archivo de cola utilizado para permitir nuevos binarios **sendmail** a fin de leer los archivos de cola creados por versiones anteriores. De forma predeterminada toma la versión **zero** (cero). Si existe, debe ser la primera línea del archivo.
- Z** Especifica el ID de sobre original (de la transacción ESMTP). Sólo se utiliza para Notificaciones de estado de entrega.
- \$** Contiene una definición de macro. Los valores de determinadas macros (**\$r** y **\$s**) se pasan a través de la fase de ejecución de cola.

El archivo q para un mensaje enviado a amy@zeus tendrá un aspecto similar a lo siguiente:

```
P217031
T566755281
MDeferred: La conexión ha excedido el tiempo de espera durante la apertura
            del usuario con zeus
Sgeo
Ramy@zeus
H?P?return-path: <geo>
HReceived: by jorge (0.13 (NL support)/0.01)
           id AA00269; Jue, 17 Dic 87 10:01:21 CST
H?D?date: Jue, 17 Dic 87 10:01:21 CST
H?F?From: geo
Hmessage-id: <8712171601.AA00269@jorge>
HTo: amy@zeus
Hsubject: prueba
```

Donde:

Item	Descripción
P217031	Prioridad del mensaje
T566755281	Tiempo de sometimiento en segundos
MDeferred: La conexión ha excedido el tiempo de espera durante la apertura de usuario con zeus	Mensaje de estado
Sgeo	Identificador del remitente
Ramy@zeus	Identificador del destinatario

Item	Descripción
H líneas	Información de cabecera del mensaje

### Valores de tiempo en sendmail

Para establecer el tiempo de espera de mensaje y el intervalo de proceso de cola, debe utilizar un formato específico para el valor de tiempo.

El formato de un valor de tiempo es:

```
-qNúmeroUnidad
```

donde *Número* es un valor entero y *Unidad* es la letra de unidad. *Unidad* puede tener uno de los valores siguientes:

Item	Descripción
------	-------------

**m**

**s** Segundos

**m** Minutos

**h** Horas

**d** Días

**w** Semanas

Si no se especifica *Unidad*, el daemon **sendmail** utiliza minutos (**m**) como valor predeterminado. A continuación se proporciona tres ejemplos que ilustran la especificación de tiempo-valor:

```
/usr/sbin/sendmail -q15d
```

Este mandato indica al daemon **sendmail** que procese la cola cada 15 días.

```
/usr/sbin/sendmail -q15h
```

Este mandato indica al daemon **sendmail** que procese la cola cada 15 horas.

```
/usr/sbin/sendmail -q15
```

Este mandato indica al daemon **sendmail** que procese la cola cada 15 minutos.

### Colas de correo atascadas

En algunos casos, es posible que encuentre que la cola está atascada por algún motivo. Es posible forzar la ejecución de una cola utilizando el distintivo **-q** (sin ningún valor).

También puede utilizarse el distintivo **-v** (detallado) para observar lo que ocurre:

```
/usr/sbin/sendmail -q -v
```

Asimismo, pueden limitarse los trabajos a aquellos con un identificador de cola, remitente o destinatario concreto, utilizando uno de los modificadores de cola. Por ejemplo, **-qRsally** restringe la ejecución de la cola a los trabajos que tienen la serie **sally** en una de las direcciones del receptor. De forma similar, **-qSserie** limita la ejecución a receptores concretos y **-qIserie** la limita a identificadores de cola concretos.

### Establecimiento del intervalo de proceso de cola

El valor del distintivo **-q** cuando el daemon se inicia determina el intervalo al que el daemon **sendmail** procesa la cola de correo.

Normalmente el daemon **sendmail** lo inicia el archivo **/etc/rc.tcpip** en el arranque del sistema. El archivo **/etc/rc.tcpip** contiene una variable denominada intervalo de proceso de cola (QPI), la cual utiliza para especificar el valor del distintivo **-q** cuando inicia el daemon **sendmail**. De forma predeterminada, el valor de **qpi** es 30 minutos. Para especificar un intervalo de proceso de cola diferente:

1. Edite el archivo `/etc/rc.tcpip` con el editor que prefiera.
2. Busque la línea que asigna un valor a la variable `qpi`, por ejemplo:

```
qpi=30m
```

3. Cambie el valor asignado a la variable `qpi` por el valor de tiempo que prefiera.

Estos cambios entrarán en vigor en el siguiente reinicio del sistema. Si desea que los cambios entren en vigor inmediatamente, detenga y reinicie el daemon **sendmail**, especificando el nuevo valor de distintivo **-q**. Consulte el apartado “[Detención del daemon sendmail](#)” en la página 53 y el apartado “[Inicio del daemon sendmail](#)” en la página 52 para obtener más información.

### Cómo mover la cola de correo

Cuando un sistema principal queda fuera de servicio durante un largo periodo de tiempo, es posible que muchos mensajes direccionaldos a (o a través) de dicho sistema principal se almacenen en la cola de correo. Como resultado, el mandato `sendmail` emplea mucho tiempo clasificando la cola, lo que degrada gravemente el rendimiento del sistema. Si mueve la cola a una ubicación temporal y crea una cola nueva, la cola antigua se puede ejecutar posteriormente cuando el sistema principal vuelva a estar en servicio.

Para mover la cola a una ubicación temporal y crear una cola nueva:

1. Detenga el daemon **sendmail** siguiendo las instrucciones del apartado “[Detención del daemon sendmail](#)” en la página 53.
2. Mueva el directorio de colas entero entrando:

```
cd /var/spool  
mv mqueue omqueue
```

3. Reinicie el daemon **sendmail** siguiendo las instrucciones del apartado “[Inicio del daemon sendmail](#)” en la página 52.

4. Procese la cola de correo antigua entrando:

```
/usr/sbin/sendmail -oQ/var/spool/omqueue -q
```

El distintivo **-oQ** especifica un directorio de colas alternativo. El distintivo **-q** especifica que se ejecute cada trabajo de la cola. Para obtener un informe sobre el progreso de la operación, utilice el distintivo **-v**.

**Nota:** Esta operación puede durar bastante tiempo.

5. Elimine los archivos de registro y el directorio temporal cuando la cola esté vacía entrando:

```
rm /var/spool/omqueue/*  
rmdir /var/spool/omqueue
```

### Inicio del daemon sendmail

Hay dos mandatos que inician el daemon **sendmail**.

Para iniciar el daemon **sendmail**, entre uno de los mandatos siguientes:

```
startsrc -s sendmail -a "-bd -q15"  
  
/usr/lib/sendmail -bd -q15
```

Si el daemon **sendmail** ya está activo cuando entre uno de estos mandatos, verá el mandato siguiente en la pantalla:

```
El subsistema  
sendmail ya está activo. No se da soporte a múltiples instancias.
```

Si el daemon **sendmail** aún no está activo, verá un mensaje que indica que el daemon **sendmail** se ha iniciado.

### **Detención del daemon sendmail**

Para detener el daemon **sendmail**, ejecute el mandato **stopsrc -s sendmail**.

Si el daemon **sendmail** no se ha iniciado con el mandato **startsrc**:

- Busque el ID de proceso **sendmail**.
- Entre el mandato **kill pid\_sendmail** (donde *pid\_sendmail* es el ID del proceso **sendmail**).

## **Registro de correo**

El mandato **sendmail** registra la actividad del sistema de correo mediante el daemon **syslogd**.

El daemon **syslogd** debe estar configurado y en ejecución para que se produzca el registro. Específicamente, el archivo */etc/syslog.conf* debe contener la línea no comentada:

```
mail.debug          /var/spool/mqueue/log
```

Si no es así, utilice el editor que prefiera para realizar este cambio; asegúrese de que el nombre de vía de acceso es correcto. Si cambia el archivo */etc/syslog.conf* mientras se está ejecutando el daemon **syslogd**, renueve el daemon **syslogd** escribiendo el mandato siguiente en una línea de mandatos:

```
refresh -s syslogd
```

Si el archivo */var/spool/mqueue/log* no existe, debe crearlo escribiendo el siguiente mandato:

```
touch /var/spool/mqueue/log
```

Los mensajes del archivo de registro aparecen en el formato siguiente:

Cada línea del registro del sistema consta de una indicación de la hora, del nombre de la máquina que lo ha generado (para el registro de varias máquinas a través de la red de área local), de la palabra **sendmail**: y de un mensaje. La mayoría de los mensajes son una secuencia de pares *nombre=valor*.

Las dos líneas más comunes registradas cuando se procesa un mensaje son la línea **receipt** y la línea **delivery attempt**. La línea **receipt** registra la recepción de un mensaje; habrá una por mensaje. Es posible que se omitan algunos campos. Estos campos de mensaje son:

<b>Item</b>	<b>Descripción</b>
from	Especifica la dirección del remitente del sobre.
tamaño	Especifica el tamaño del mensaje en bytes.
class	Indica la clase (prioridad numérica) del mensaje.
pri	Especifica la prioridad inicial del mensaje (utilizada para la clasificación de colas).
nrcpts	Indica el número de destinatarios de sobre para este mensaje (después de los alias y del reenvío).
proto	Especifica el protocolo utilizado para recibir el mensaje, por ejemplo ESMTP o UUCP (UNIX-to-UNIX Copy Program - Programa de copia de UNIX a UNIX).
relay	Especifica la máquina de la que se ha recibido.

La línea **delivery attempt** se registra cada vez que hay un intento de entrega (por consiguiente puede haber varias por mensaje si la entrega se difiere o hay varios destinatarios). Estos campos son:

<b>Item</b>	<b>Descripción</b>
to	Contiene una lista separada por comas de los destinatarios en este programa de correo.
ctladdr	Especifica el <i>usuario de control</i> , es decir, el nombre del usuario cuyos credenciales se utilizan para la entrega.

<b>Item</b>	<b>Descripción</b>
delay	Especifica el retardo total entre la hora en que se ha recibido este mensaje y la hora en que se ha entregado.
xdelay	Especifica la cantidad de tiempo necesaria en este intento de entrega.
mailer	Especifica el nombre del programa de correo utilizado para realizar la entrega a este destinatario.
relay	Especifica el nombre del sistema principal que realmente ha aceptado (o rechazado) este destinatario.
stat	Especifica el estado de entrega.

Dado que se puede registrar una cantidad de información de un gran tamaño, el archivo de registro se organiza como una sucesión de niveles. A partir del nivel 1, el nivel más bajo, sólo se registran situaciones muy inusuales. En el nivel más alto, incluso se registran los sucesos insignificantes. Por convenio, los niveles de registro diez e inferiores contienen la información más útil. Los niveles de registro por encima de 64 están reservados para la depuración. Los niveles 11 a 64 están reservados a la información detallada.

Los tipos de actividades que el mandato **sendmail** pone en el archivo de registro se especifican mediante la opción **L** en el archivo /etc/mail/sendmail.cf.

### Gestión de registros cronológicos

Dado que continuamente se añade información al final del registro cronológico, el archivo puede llegar a tener un tamaño muy grande. Asimismo, las condiciones de error pueden producir entradas inesperadas en la cola de correo. Para evitar que la cola de correo y el archivo de registro cronológico lleguen a tener un tamaño demasiado grande, ejecute el script de shell /usr/lib/smdemon.clean.

Este script fuerza que el mandato **sendmail** procese la cola y mantiene cuatro copias progresivamente más antiguas de los archivos de registro cronológico, denominados log.0, log.1, log.2 y log.3. Cada vez que el script se ejecuta, mueve:

- log.2 a log.3
- log.1 a log.2
- log.0 a log.1
- log a log.0

La ejecución de este script permite que el registro cronológico se inicie otra vez con un nuevo archivo. Ejecute este script manualmente o a un intervalo especificado con el daemon **cron**.

### Registros cronológicos de tráfico

Utilice el distintivo **-X** del mandato **sendmail** para establecer el registro cronológico de tráfico.

Muchas implementaciones de **SMTP (Simple Mail Transfer Protocols - Protocolos simples de transferencia de correo)** no implementan totalmente el protocolo. Por ejemplo, algunos **SMTP** basados en sistemas personales no conocen las líneas de continuación en los códigos de respuesta. Puede ser muy difícil rastrearlas. Si sospecha un problema de este tipo, puede establecer el registro cronológico de tráfico utilizando el distintivo **-X**. Por ejemplo:

```
/usr/sbin/sendmail -X /tmp/traffic -bd
```

Este mandato registra todo el tráfico en el archivo /tmp/traffic.

Dado que este mandato registra muchos datos muy rápidamente, no se deberá utilizar nunca durante las operaciones normales. Después de ejecutar el mandato, fuerce la implementación de **errant** para enviar un mensaje al sistema principal. Todo el tráfico de mensajes de entrada y salida de **sendmail**, incluido el tráfico **SMTP** de entrada, se registrará en este archivo.

Utilizando **sendmail**, puede registrar un vuelco de los archivos abiertos y de la antememoria de conexión enviándole una señal **SIGUSR1**. Los resultados se registran en la prioridad de **LOG\_DEBUG**.

## Registros de estadísticas de programa de correo

El mandato **sendmail** realiza el seguimiento del volumen de correo manejado por cada uno de los programas de correo que intercambian información con él.

Esos programas de correo se definen en el archivo `/etc/mail/sendmail.cf`.

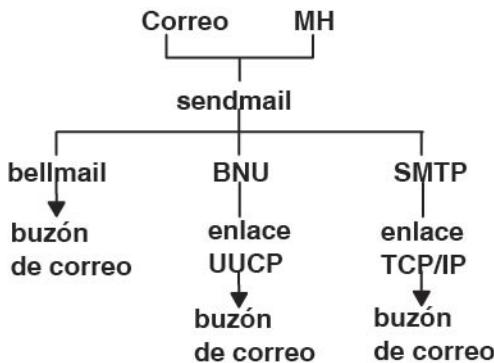


Figura 3. Programas de correo utilizados por el mandato *sendmail*

Esta ilustración es un tipo de gráfico de organización de arriba a abajo con Mail y MH en la parte superior. Las ramificaciones de éstos son bellmail, BNU y SMTP. Debajo del nivel anterior están el buzón local, el enlace UUCP y el enlace TCP/IP respectivamente. Debajo del enlace UUCP está el buzón remoto y bajo el enlace TCP/IP está el buzón remoto.

Para iniciar la acumulación de estadísticas de programa de correo, cree el archivo `/etc/mail/statistics` escribiendo lo siguiente:

```
touch /etc/mail/statistics
```

Si el mandato **sendmail** encuentra errores al intentar registrar información de estadísticas, el mandato graba un mensaje mediante la subrutina `syslog`. Estos errores no afectan a otras operaciones del mandato **sendmail**.

El mandato **sendmail** actualiza la información del archivo cada vez que procesa correo. El tamaño del archivo no aumenta, pero los números contenidos en el archivo sí lo hacen. Representan el volumen de correo desde el momento en que se ha creado o restablecido el archivo `/etc/mail/statistics`.

## Visualización de información de programa de correo

Las estadísticas mantenidas en el archivo `/etc/mail/statistics` están en un formato de base de datos que no se puede leer como archivo de texto.

Para visualizar estadísticas de programa de correo, escriba lo siguiente en un indicador de mandatos:

```
/usr/sbin/mailstats
```

Esto lee la información del archivo `/etc/mail/statistics`, la formatea y la graba en la salida estándar. Para obtener más información, consulte el mandato **/usr/sbin/mailstats**.

## API de filtro de correo sendmail

La API de filtro de correo **sendmail** (conocida como *Milter*) permite que programas de otras empresas accedan a los mensajes de correo mientras se están procesando con el fin de filtrar metainformación y contenido.

### Requisitos de filtro sendmail

Dado que los filtros utilizan hebras, los filtros deben ser seguros para las hebras. Puede configurar los filtros para asegurar la compatibilidad de éstos con las hebras.

Muchos sistemas operativos proporcionan soporte para hebras POSIX en las bibliotecas C estándares. El distintivo de compilador para enlazar con el soporte de hebras difiere en función del compilador y del

enlazador utilizados. Si no está seguro del distintivo local utilizado, consulte el Makefile del subdirectorio de creación obj.\*/libmilter apropiado.

**Nota:** Dado que los filtros utilizan hebras, es posible que sea necesario modificar los límites de proceso en el filtro. Por ejemplo, es posible que desee utilizar setrlimit para aumentar el número de descriptores de archivo abiertos si el filtro va a estar ocupado; de lo contrario, se puede rechazar el correo.

### Configuraciones de filtro sendmail

Utilice estas directrices para especificar los filtros que desea mientras configura **sendmail**.

Especifique filtros utilizando la letra de tecla X (para eXterno). En el ejemplo siguiente, se especifican tres filtros:

```
Xfilter1, S=local:/var/run/f1.sock, F=R  
Xfilter2, S=inet6:999@localhost, F=T, T=C:10m;S:1s;R:1s;E:5m  
Xfilter3, S=inet:3333@localhost
```

Puede especificar filtros en el archivo .mc utilizando la sintaxis siguiente:

```
INPUT_MAIL_FILTER(`filter1', `S=local:/var/run/f1.sock, F=R')  
INPUT_MAIL_FILTER(`filter2', `S=inet6:999@localhost, F=T, T=C:10m;S:1s;R:1s;E:5m')  
INPUT_MAIL_FILTER(`filter3', `S=inet:3333@localhost')
```

donde filter(*número*) es el número del filtro. La primera línea de la sintaxis especifica que el filtro se adjunte a un socket en el dominio UNIX en el directorio /var/run. La segunda línea especifica que el filtro utilice un socket IPv6 en el puerto 999 del sistema principal local. La tercera línea especifica que el filtro utilice un socket IPv4 en el puerto 3333 en el sistema principal local.

La F= indica cuál de los distintivos siguientes se aplica:

Item	Descripción
R	Rechaza la conexión si el filtro no está disponible.
T	Falla la conexión temporalmente si el filtro no está disponible.

Si no se especifica ninguno de los distintivos, el mensaje se pasa mediante **sendmail** como si el filtro no estuviera presente.

Mediante la especificación de un valor para T=, puede utilizar los filtros para alterar temporalmente los tiempos de espera predeterminados utilizados por **sendmail**. La ecuación T= utiliza los campos siguientes:

Item	Descripción
C	Tiempo de espera para conectarse a un filtro (si 0, utilice el tiempo de espera del sistema).
S	Tiempo de espera para enviar información de MTA a un filtro.
R	Tiempo de espera para leer respuestas del filtro.
E	Tiempo de espera global entre el envío de avisos de fin de mensaje al filtro y la espera del acuse de recibo final.

Como se indica en el ejemplo anterior, los separadores entre cada tiempo de espera es un punto y coma (;) y el separador entre cada ecuación es una coma (,).

Los valores predeterminados para los tiempos de espera son los siguientes:

```
T=C:0m;S:10s;R:10s;E:5m
```

donde s es segundos y m es minutos.

La opción **InputMailFilters** determina qué filtros se utilizan y en qué secuencia.

**Nota:** Si no se especifica la opción **InputMailFilters**, no se utilizan filtros.

La opción **InputMailFilters** se establece automáticamente de acuerdo con el orden de los mandatos INPUT\_MAIL\_FILTER en el archivo .mc. Puede restablecer este valor estableciendo un valor para confINPUT\_MAIL\_FILTERS en el archivo .mc. Por ejemplo, si la opción **InputMailFilters** se establece como:

```
InputMailFilters=filter1, filter2, filter3
```

se llamarán a los tres filtros en el mismo orden en que se han especificado.

Si se utiliza MAIL\_FILTER() en lugar de INPUT\_MAIL\_FILTER() en el archivo .mc, puede definir un filtro sin añadirlo a la lista de filtros de entrada.

### Funciones de control de la biblioteca

El filtro sendmail llama las funciones del control de biblioteca para establecer los parámetros **libmilter** antes de pasar el control al **libmilter**. Los parámetros **libmilter** se establecen llamando a la función **smfi\_main**. El filtro también llama a la función **smfi\_register** para registrar específicamente sus devoluciones de llamadas. Cada función devuelve el valor MI\_SUCCESS o MI\_FAILURE para indicar el estado de la operación. Estas funciones no se comunican con el agente de transferencia de correo (MTA), sino que alteran el estado de la biblioteca, que se comunica con el MTA dentro de la función **smfi\_main**.

Tabla 2. Funciones de control de la biblioteca	
Item	descripción
<b>smfi_opensocket</b>	La función <b>smfi_opensocket</b> crea el socket de la interfaz.
<b>smfi_register</b>	La función <b>smfi_register</b> registra un filtro.
<b>smfi_setconn</b>	La función <b>smfi_setconn</b> especifica un socket que se utilizará.
<b>smfi_settimeout</b>	La función <b>smfi_settimeout</b> establece el tiempo de espera.
<b>smfi_setbacklog</b>	La función <b>smfi_setbacklog</b> define el tamaño de cola <b>listen (2)</b> entrante.
<b>smfi_setdbg</b>	La función <b>smfi_setdbg</b> establece el nivel de depuración (rastreo) de la biblioteca de <b>milter</b> .
<b>smfi_stop</b>	La función <b>smfi_stop</b> causa un cierre ordenado.
<b>smfi_main</b>	La función <b>smfi_main</b> pasa el control a <b>libmilter</b> .

### Función **smfi\_opensocket**

#### Finalidad

La función **smfi\_opensocket** intentará crear los agentes de transferencia de correo (MTA) de socket de la interfaz que se utilizan para conectarse al filtro.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_opensocket(
    bool rmsocket
);
```

#### Descripción

La función **smfi\_opensocket** sólo se llama desde la línea principal del programa, tras llamar a la función **smfi\_setconn** y a la función **smfi\_register**, pero antes de llamar a la función **smfi\_main**. La función

**smfi\_opensocket** creará el socket especificado anteriormente llamando a la función **smfi\_setconn**, que es la interfaz entre los MTA y el filtro. La función **smfi\_opensocket** permite a la aplicación de llamada crear el socket. Si la función **smfi\_opensocket** no se llama, la función **smfi\_main** llamará a la función implícitamente.

## Argumentos

Tabla 3. Argumentos	
Item	Descripción
<i>rmsocket</i>	Un distintivo indicará si la biblioteca debe intentar eliminar cualquier socket de dominio de UNIX existente antes de intentar crear uno nuevo.

## Valores de retorno

La función **smfi\_opensocket** devuelve el valor MI\_FAILURE en los casos siguientes. De lo contrario, la función devolverá MI\_SUCCESS.

- El socket de la interfaz no se ha podido crear.
- El valor *rmsocket* es verdadero, y o bien el socket no se ha podido examinar, o bien el socket existente no se ha podido eliminar.
- La función **smfi\_setconn** o la función **smfi\_register** no se ha llamado.

## Información relacionada

[libmilter\\_smfi\\_register.dita](#)

[libmilter\\_smfi\\_setconn.dita](#)

## Función smfi\_register

### Finalidad

La función **smfi\_register** registra un conjunto de funciones de devolución de llamadas de filtro sendmail.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_register(
    smfiDesc descr)
);
```

### Descripción

La función **smfi\_register** crea un filtro sendmail utilizando la información proporcionada en el argumento **smfiDesc**. La función **smfi\_register** debe llamarse antes de la función **smfi\_main**.

**Nota:** No están permitidas varias llamadas satisfactorias a la función **smfi\_register** dentro de un único proceso. Sólo se puede registrar satisfactoriamente un único filtro sendmail. Tenga en cuenta, sin embargo, que la biblioteca no se puede comprobar si se obedece la restricción.

El campo *xxfi\_flags* debe contener los bits o los ceros o cualquiera de los siguientes valores, que describen las acciones que puede realizar el filtro sendmail.

Tabla 4. Valores	
Item	Descripción
<b>SMFIF_ADDHDRS</b>	La función <b>smfi_addheader</b> añade cabeceras.

Tabla 4. Valores (continuación)

Item	Descripción
<b>SMFIF_CHGHDRS</b>	La función <b>smfi_chgheader</b> modifica las cabeceras o bien suprime las cabeceras.
<b>SMFIF_CHGBODY</b>	La función <b>smfi_replacebody</b> sustituye el cuerpo durante el filtrado. El filtro tiene un impacto de rendimiento significativo si otros filtros realizan filtrado de cuerpo tras este filtro.
<b>SMFIF_ADDRCPT</b>	La función <b>smfi_addrcpt</b> añade destinatarios al mensaje.
<b>SMFIF_ADDRCPT_PAR</b>	La función <b>smfi_addrcpt_par</b> añade destinatarios, incluidos los argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado.
<b>SMFIF_DELRCPT</b>	La función <b>smfi_delrcpt</b> elimina destinatarios del mensaje.
<b>SMFIF_QUARANTINE</b>	La función <b>smfi_quarantine</b> pone en cuarentena un mensaje.
<b>SMFIF_CHGFROM</b>	La función <b>smfi_chgfrom</b> modifica el remitente del sobre (Mail From).
<b>SMFIF_SETSYMLIST</b>	La función <b>smfi_setsymlist</b> envía un conjunto de símbolos (macros) que son necesarios.

## Argumentos

Tabla 5. Argumentos

Item	Descripción
<i>descr</i>	<p>Un descriptor de filtros de tipo <code>smfiDesc</code> que describe las funciones de los filtros. La estructura tiene los siguientes miembros:</p> <pre> struct smfiDesc {     char      *xxfi_name;      /* filter name */     int       xxfi_version;   /* version code -- do not change */     unsigned long  xxfi_flags; /* flags */      /* connection info filter */     sfssistat (*xxfi_connect)(SMFICTX *, *, char *, _SOCK_ADDR *);     /* SMTP HELO command filter */     sfssistat (*xxfi_helo)(SMFICTX *, char *);     /* envelope sender filter */     sfssistat (*xxfi_envfrom)(SMFICTX *, *, char **);     /* envelope recipient filter */     sfssistat (*xxfi_envrcpt)(SMFICTX *, *, char **);     /* header filter */     sfssistat (*xxfi_header)(SMFICTX *, *, char *, char *);     /* end of header */     sfssistat (*xxfi_eoh)(SMFICTX *);     /* body block */     sfssistat (*xxfi_body)(SMFICTX *, unsigned char *, size_t);     /* end of message */     sfssistat (*xxfi_eom)(SMFICTX *);     /* message aborted */     sfssistat (*xxfi_abort)(SMFICTX *);     /* connection cleanup */     sfssistat (*xxfi_close)(SMFICTX *);      /* any unrecognized or unimplemented command filter */     sfssistat (*xxfi_unknown)(SMFICTX *, const char *);      /* SMTP DATA command filter */     sfssistat (*xxfi_data)(SMFICTX *);      /* negotiation callback */     sfssistat (*xxfi_negotiate)(SMFICTX *, unsigned long, unsigned long, unsigned long, unsigned long *, unsigned long *, unsigned long *, unsigned long * ); }; </pre> <p>Un valor NULL para cualquier función de devolución de llamadas indica que el filtro no procesa el tipo determinado de información, y devuelve <b>SMFIS_CONTINUE</b>.</p>

Tabla 5. Argumentos (continuación)

Item	Descripción
<code>headerf</code>	El nombre de la cabecera es una serie terminada en nulo que no es NULL.
<code>headerv</code>	El valor de la cabecera que se añadirá puede ser una serie terminada en nulo no NULL o una serie vacía.

### Valores de retorno

La función **smfi\_register** devuelve el valor MI\_FAILURE en los casos siguientes. De lo contrario, la función devolverá MI\_SUCCESS.

- Ha fallado la asignación de memoria.
- Versión incompatible o valor de distintivos ilegal.

### Información relacionada

[libmilter\\_smfi\\_addheader.dita](#)

[libmilter\\_smfi\\_chgheader.dita](#)

[libmilter\\_smfi\\_replacebody.dita](#)

[libmilter\\_smfi\\_addrcpt.dita](#)

[libmilter\\_smfi\\_addrcpt\\_par.dita](#)

[libmilter\\_smfi\\_delrcpt.dita](#)

[libmilter\\_smfi\\_quarantine.dita](#)

[libmilter\\_smfi\\_chgfrom.dita](#)

[libmilter\\_smfi\\_setsymlist.dita](#)

### Función **smfi\_setconn**

#### Finalidad

La función **smfi\_setconn** establece el socket por el que este filtro se puede comunicar con el mandato **sendmail**.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setconn(
    char *oconn;
);
```

#### Descripción

La función **smfi\_setconn** debe llamarse antes de llamar a la función **smfi\_main**.

Los filtros no deben ejecutarse como raíz al comunicarse sobre UNIX o sockets de dominio local.

Los permisos para UNIX o los sockets locales deben establecerse en 0600 (permiso de lectura o escritura únicamente para el propietario o el grupo de sockets) o 0660 (permiso de lectura/escritura para el propietario de los sockets y el grupo). Estos permisos son útiles si se utiliza la opción **sendmail RunAsUser**.

Los permisos para un UNIX o un socket de dominio local están determinados por el **umask**, que se deben establecer en 007 o 077. Para sistemas operativos como Solaris que no utilizan permisos del socket, colóquelo en un directorio protegido.

## Argumentos

Tabla 6. Argumentos	
Item	Descripción
<i>oconn</i>	<p>La dirección del socket de comunicación deseado. La dirección debe ser una serie terminada en NULL en el formato <b>proto:address</b>:</p> <div style="background-color: #f0f0f0; padding: 10px;"><p>* {unix local}:/path /to/file -- A named pipe. * inet:port @{hostname ip-address} -- An IPV4 socket. * inet6:port @{hostname ip-address} -- An IPV6 socket.</p></div>

## Valores de retorno

La función **smfi\_setconn** no falla, si es una dirección no válida. Sin embargo, la función **smfi\_setconn** fallará a la hora de establecer el socket si no hay memoria. El fallo se detecta únicamente en la función **smfi\_main**.

## Información relacionada

[libmilter\\_smfi\\_main.dita](#)

## Función smfi\_settimeout

### Finalidad

La función **smfi\_settimeout** establece el valor de tiempo de espera de E/S de los filtros.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_settimeout(
    int otimeout
);
```

### Descripción

La función **smfi\_settimeout** se llama únicamente desde la función **smfi\_main**. La función **smfi\_settimeout** establece la duración (en segundos) para que el parámetro **libmilter** espere una comunicación del agente de transferencia de correo (MTA) (lectura o escritura) antes de la temporización de espera.

**Nota:** Si la función **smfi\_settimeout** no se llama, la duración del tiempo de espera predeterminado es de 7210 segundos.

## Argumentos

Tabla 7. Argumentos	
Item	Descripción
<i>timeout</i>	La duración en segundos para que el parámetro <b>libmilter</b> espere un MTA antes de la temporización de espera. El valor <i>timeout</i> no debe ser mayor de cero. Si el valor <i>timeout</i> es cero, el parámetro <b>libmilter</b> no espera un MTA.

## Valores de retorno

La función **smfi\_settimeout** siempre devuelve el valor MI\_SUCCESS.

## Información relacionada

[smfi\\_main](#)

[Función smfi\\_setbacklog](#)

## Finalidad

La función **smfi\_setbacklog** establece el valor de retraso **listen(2)** del filtro.

## Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setbacklog(
    int obacklog
);
```

## Descripción

La función **smfi\_setbacklog** se llama únicamente antes de llamar a la función **smfi\_main**. La función **smfi\_setbacklog** establece el retraso de socket entrante, que utiliza el valor de retraso **listen(2)**. Si la función **smfi\_setbacklog** no se llama, se utilizará el sistema operativo predeterminado.

## Argumentos

Tabla 8. Argumentos	
Item	Descripción
<i>obacklog</i>	El número de conexiones entrantes permitidas en la cola de escucha.

## Valores de retorno

La función **smfi\_setbacklog** devuelve el valor MI\_FAILURE si el argumento *obacklog* se establece en menos o es igual a null.

## Información relacionada

[libmilter\\_smfi\\_main.dita](#)

[Función smfi\\_setdbg](#)

## Finalidad

La función **smfi\_setdbg** establece el nivel de depuración (rastreo) de la biblioteca **milter**.

## Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setdbg(
    int level;
);
```

## Descripción

La función **smfi\_setdbg** establece el nivel de depuración interno de la biblioteca **milter** a un nuevo nivel, para que los detalles del código se puedan rastrear. Un nivel de cero devuelve la depuración. Cuanto mayor (más positivo) sea el nivel, más detallada será la depuración. Seis es el valor actual, más alto y útil.

## Argumentos

Tabla 9. Argumentos	
Item	Descripción
<i>nivel</i>	El nuevo nivel de depuración.

## Valores de retorno

La función **smfi\_setdbg** devuelve el valor MI\_SUCCESS de forma predeterminada.

## Función **smfi\_stop**

### Finalidad

La función **smfi\_stop** desactiva el **milter**. Las conexiones no se aceptan después de esta llamada.

## Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_stop(void);
);
```

## Descripción

La función **smfi\_stop** se llama desde las Funciones de devolución de llamada o desde las rutinas de manejo de errores en cualquier momento. La rutina **smfi\_stop** no permite nuevas conexiones. Sin embargo, la función no espera que las conexiones existentes (hebras) finalicen. Esta función hace que la función **smfi\_main** vuelva al programa llamante, que puede salir o reanudar el sistema.

## Argumentos

Tabla 10. Argumentos	
Item	Descripción
<i>void</i>	Este argumento no toma ningún valor.

## Valores de retorno

La función **smfi\_stop** devuelve el valor SMFI\_CONTINUE en los casos siguientes:

- Una rutina interna causa que la biblioteca **milter** se detenga.
- Una rutina causa que la biblioteca **milter** se detenga.
- El proceso que se inició no se puede detener.

## Ejemplo

```
int ret;
SMFICTX *ctx;
...
ret = smfi_addheader(ctx, "Content-Type",
"multipart/mixed;\n\tboundary=\"foobar\"");
```

## Información relacionada

[Funciones de devolución de llamada](#)

### Función **smfi\_main**

#### Finalidad

La función **smfi\_main** pasa el control al bucle de sucesos **libmilter**.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_main(
```

#### Descripción

La función **smfi\_main** se llama una vez que la inicialización del filtro esté completa.

#### Valores de retorno

La función **smfi\_main** devuelve el valor **MI\_FAILURE** si la conexión no se ha podido establecer. De lo contrario, la función devolverá **MI\_SUCCESS**.

El fallo se produce por diferentes motivos, y los motivos para el fallo se registran. Por ejemplo, pasar una dirección no válida dentro de la función **smfi\_setconn** hace que la función falle.

## Información relacionada

[libmilter\\_smfi\\_setconn.dita](#)

### Funciones del acceso de datos

Las funciones del acceso de datos se llaman desde dentro de las funciones de devolución de llamada que se definen dentro de los filtros, para acceder a la información sobre el mensaje o la conexión actual.

Tabla 11. Funciones del acceso de datos	
Item	Descripción
<b>smfi_getsymal</b>	La función <b>smfi_getsymal</b> devuelve el valor de un símbolo.
<b>smfi_getpriv</b>	La función <b>smfi_getpriv</b> capta el puntero de datos privados.
<b>smfi_setpriv</b>	La función <b>smfi_setpriv</b> establece el puntero de datos privados.
<b>smfi_setreply</b>	La función <b>smfi_setreply</b> establece el código de respuesta específico que se utilizará.
<b>smfi_setmlreply</b>	La función <b>smfi_setmlreply</b> establece la respuesta de varias líneas específica que se utilizará.

## Función `smfi_getsymval`

### Finalidad

La función `smfi_getsymval` capta el valor de una macro `sendmail`.

### Sintaxis

```
#include <libmilter/mfapi.h>
char* smfi_getsymval(
    SMFICTX *ctx,
    char *headerf,
    char *symname
);
```

### Descripción

La función `smfi_getsymval` se llama desde cualquiera de las funciones `xxfi_* callback` para añadir una cabecera al mensaje. La definición de macro depende de la función que se llame.

De forma predeterminada, son válidas las siguientes macros:

Tabla 12. Descripción	
Item	Descripción
<code>xxfi_connect</code>	<code>daemon_name, if_name, if_addr, j, _</code>
<code>xxfi_hello</code>	<code>tls_version, cipher, cipher_bits, cert_subject, cert_issuer</code>
<code>xxfi_envfrom</code>	<code>i, auth_type, auth_authen, auth_ssf, auth_author, mail_mailer, mail_host, mail_addr</code>
<code>xxfi_envrcpt</code>	<code>rcpt_mailer, rcpt_host, rcpt_addr</code>
<code>xxfi_data</code>	Ninguno
<code>xxfi_eoh</code>	Ninguno
<code>xxfi_eom</code>	<code>msg_id</code>

Todas las macros siguen estando activas desde el punto de vista de que se reciben hasta el final de la conexión para las funciones `xxfi_connect`, `xxfi_hello`.

Todas las macros siguen activas hasta el final del mensaje para la función `xxfi_envfrom` y la función `xxfi_eom`.

Todas las macros siguen activas para cada destinatario de la función `xxfi_envrcpt`.

La lista de macros se puede cambiar utilizando las opciones `confMILTER_MACROS_*` de `sendmail.mc`. El ámbito de tales macros se determina cuando se establezcan mediante el mandato `sendmail`. Para obtener descripciones de los valores de las macros, consulte *Guía de funcionamiento e instalación de sendmail*.

### Argumentos

Tabla 13. Argumentos	
Item	Descripción
<code>ctx</code>	La estructura de contexto opaca se mantiene en el parámetro <code>libmilter</code> .

Tabla 13. Argumentos (continuación)

Item	Descripción
symname	El nombre de una macro <b>sendmail</b> . Las macros de letra única pueden estar opcionalmente entre llaves ("{" y "}"), los nombres de macros más largos deben estar entre llaves, como en un archivo <b>sendmail.cf</b> .

### Valores de retorno

La función **smfi\_getsymval** devuelve el valor de la macro dada como una serie terminada en nulo. De lo contrario, la función **smfi\_getsymval** devuelve NULL si la macro no está definida.

### Información relacionada

[libmilter\\_xxfi\\_connect.dita](#)

[libmilter\\_xxfi\\_helo.dita](#)

[libmilter\\_xxfi\\_envfrom.dita](#)

[libmilter\\_xxfi\\_envrcpt.dita](#)

[libmilter\\_xxfi\\_data.dita](#)

[libmilter\\_xxfi\\_eoh.dita](#)

[libmilter\\_xxfi\\_eom.dita](#)

### Función smfi\_getpriv

#### Finalidad

La función **smfi\_getpriv** capta el puntero de datos específicos de la conexión para esta conexión.

#### Sintaxis

```
#include <libmilter/mfapi.h>
void* smfi_getpriv(
    SMFICTX *ctx
);
```

#### Descripción

La función **smfi\_getpriv** se puede llamar en cualquiera de las funciones **xxfi\_\* callback**.

#### Argumentos

Tabla 14. Argumentos

Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

### Valores de retorno

La función **smfi\_getpriv** que se almacena devuelve el puntero de datos privados almacenado mediante una llamada antes de la función **smfi\_setpriv**. De lo contrario, la función **smfi\_setpriv** devuelve NULL si el valor no se establece.

## Información relacionada

[libmilter\\_smfi\\_setpriv.dita](#)

### Función **smfi\_setpriv**

#### Finalidad

La función **smfi\_setpriv** establece el puntero de datos privados para esta conexión.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setpriv
SMFICTX *ctx,
void *privatedata
();
```

#### Descripción

La función **smfi\_setpriv** se llama desde cualquiera de las funciones **xxfi\_\* callback** para establecer el puntero de datos privados para el ctx.

**Nota:** Hay un puntero de datos privados por conexión; varias llamadas a la función **smfi\_setpriv** con distintos valores causan que los valores anteriores se pierdan. Antes de que finalice un filtro, éste debe liberar los datos privados y establecer el puntero en NULL.

#### Argumentos

Tabla 15. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
privatedata	Los puntos del argumento para los datos privados. Este valor se devuelve mediante llamadas posteriores a la función <b>smfi_getpriv</b> utilizando ctx.

#### Valores de retorno

La función **smfi\_setpriv** devuelve el valor MI\_FAILURE si ctx es un contexto no válido. De lo contrario, la función devolverá MI\_SUCCESS.

## Información relacionada

[libmilter\\_smfi\\_setpriv.dita#smfi\\_setpriv](#)

### Función **smfi\_setreply**

#### Finalidad

La función **smfi\_setreply** establece el código de respuesta al error de protocolo simple de transferencia de correo (SMTP) predeterminado y acepta únicamente códigos de respuesta 4XX y 5XX.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setreply
SFICTX *ctx,
char *rcode,
```

```

char *xcode,
char *message
);

```

## Descripción

La función **smfi\_setreply** se llama desde cualquiera de las funciones de **xxfi\_callback**, a excepción de la función **xxfi\_connect**. La función **smfi\_setreply** establece el código de respuesta de error SMTP para la conexión. Este código se utiliza para las siguientes respuestas de error que vienen de acciones emprendidas por este filtro.

Los valores pasados a la función **smfi\_setreply** no se comprueban para el cumplimiento de los estándares.

El argumento *message* debe contener únicamente caracteres imprimibles. Otros caracteres pueden llevar a un comportamiento no definido. Por ejemplo, los caracteres como CR o LF dan lugar a que falle la llamada, los caracteres únicos '%' dan lugar a que el texto se ignore.

**Nota:** Si es necesaria una serie '%' en el parámetro, utilice '%%' como para printf(3).

Para obtener más detalles sobre los códigos de respuesta y sus significados, consulte [RFC 821](#) o [2821](#) y [RFC 1893](#) o [2034](#).

Si el argumento *rcode* se establece como 4XX pero el valor SMFI\_REJECT se utiliza para el mensaje, la respuesta personalizada no se utilizará.

Si el argumento *rcode* se establece como 5XX pero el valor SMFI\_TEMPFAIL se utiliza para el mensaje, la respuesta personalizada no se utilizará.

**Nota:** En los dos casos anteriores, se devuelve un error para el parámetro **milter**. El parámetro **Libmilter** ignora el código de respuesta anterior.

Si el parámetro **milter** devuelve el valor SMFI\_TEMPFAIL y establece el código de respuesta en 421, el servidor SMTP terminará la sesión SMTP con un código de error 421.

## Argumentos

Tabla 16. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>rcode</i>	El código de respuesta SMTP de tres dígitos ( <a href="#">RFC 821</a> o <a href="#">2821</a> ) es una serie terminada en nulo. <i>rcode</i> no puede ser NULL, y debe ser un código de respuesta 4XX o 5XX válido.
<i>xcode</i>	El código de respuesta ampliado ( <a href="#">RFC 1893</a> o <a href="#">2034</a> ). Si <i>xcode</i> es NULL, no se utilizará ningún código ampliado. De lo contrario, <i>xcode</i> debe ajustarse a <a href="#">RFC 1893</a> o <a href="#">2034</a> .
<i>message</i>	La parte del texto de la respuesta de SMTP. Si el mensaje es NULL, se utilizará un mensaje vacío.

## Valores de retorno

La función **smfi\_setreply** devuelve el valor MI\_FAILURE en los casos siguientes. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento *rcode* o *xcode* no es válido.
- Se ha producido un fallo de asignación de memoria.

## Información relacionada

[libmilter\\_xxfi\\_connect.dita](#)

### Función smfi\_setmlreply

#### Finalidad

La función **smfi\_setmlreply** establece el código de respuesta al error de protocolo simple de transferencia de correo predeterminado (SMTP) en una respuesta de varias líneas. La función **smfi\_setmlreply** sólo acepta respuestas 4XX y 5XX.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setmlreply(
    SMFICTX *ctx,
    char *rcode,
    char *xcode,
    ...
);
```

#### Descripción

La función **smfi\_setmlreply** se llama desde cualquiera de las funciones **xxfi\_callback**, a excepción de la función **xxfi\_connect**. La función **smfi\_setmlreply** proporciona un código de respuesta de error SMTP para las conexiones mencionadas debajo de *xcode*. La lista de argumentos debe terminar en nulo. Este código se utiliza para las siguientes respuestas de error que vienen de acciones emprendidas por este filtro.

Los valores pasados a la función **smfi\_setmlreply** no se comprueban para el cumplimiento de los estándares.

El parámetro *message* debe contener sólo caracteres imprimibles; otros caracteres pueden llevar a un comportamiento no definido. Por ejemplo, los caracteres como CR o LF dan lugar a que falle la llamada, los caracteres únicos '%' dan lugar a que el texto se ignore.

**Nota:** Si es necesaria una serie '%' en el parámetro *message*, utilice la serie '%%' de forma similar a como se utiliza la serie **printf(3)**.

Para obtener los códigos de respuesta y sus significados, consulte [RFC 821](#) o [2821](#) y [RFC 1893](#) o [2034](#).

Si el *rcode* se establece como 4XX pero el valor **SMFI\_REJECT** se utiliza para el mensaje, no se utilizará la respuesta personalizada.

Si el *rcode* se establece como 5XX pero se utiliza el valor **SMFI\_TEMPFAIL** para el mensaje, no se utilizará la respuesta personalizada.

**Nota:** En los dos casos anteriores, se devuelve un error al parámetro **milter**, y el parámetro **Libmilter** ignorará el error.

Si el parámetro **milter** devuelve el valor **SMFI\_TEMPFAIL** y establece el código de respuesta en 421, el servidor SMTP terminará la sesión SMTP con un código de error 421.

#### Argumentos

Tabla 17. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

Tabla 17. Argumentos (continuación)

Item	Descripción
rcode	El código de respuesta SMTP de tres dígitos ( <a href="#">RFC 821</a> o <a href="#">2821</a> ), como una serie terminada en nulo. El argumento <i>rcode</i> no puede ser NULL, y debe ser un código de respuesta 4XX o 5XX válido.
xcode	El código de respuesta ampliado ( <a href="#">RFC 1893</a> o <a href="#">2034</a> ). Si <i>xcode</i> es NULL, no se utilizará ningún código ampliado. De lo contrario, <i>xcode</i> debe ajustarse a <a href="#">RFC 1893</a> o a <a href="#">2034</a>
...	El resto de los argumentos son líneas únicas de texto, hasta 32 argumentos, que se utilizan como parte de texto de la respuesta de SMTP. La lista debe estar terminada en nulo.

### Valores de retorno

La función **smfi\_setmlreply** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento *rcode* o *xcode* no es válido.
- Se ha producido un fallo de asignación de memoria.
- La línea de texto contiene un retorno de carro o un salto de línea.
- La longitud de cada línea de texto es mayor de MAXREPLYLEN (980).
- Las respuestas de texto superan las 32 líneas.

### Ejemplo

```
ret = smfi_setmlreply(ctx, "550", "5.7.0",
"Spammer access rejected",
"Please see our policy at:",
"http://www.example.com/spampolicy.html",
NULL);
```

El ejemplo anterior da el siguiente resultado:

```
550-5.7.0 Spammer access rejected
550-5.7.0 Please see our policy at:
550 5.7.0 http://www.example.com/spampolicy.html
```

### Información relacionada

[libmilter\\_xxfi\\_connect.dita](#)

### Funciones de modificación del mensaje

Las funciones de modificación del mensaje cambian los atributos y el contenido del mensaje. Las funciones se llaman únicamente mediante la función **xxfi\_eom**. Las funciones de modificación de mensajes pueden invocar comunicación adicional con el agente de transferencia de correo (MTA). Estas funciones devuelven el valor MI\_SUCCESS o MI\_FAILURE para indicar el estado de la operación.

**Nota:** Los datos del mensaje (remitentes, destinatarios, cabeceras y fragmentos del cuerpo) que se pasan a las funciones de modificación del mensaje en los parámetros se copian y no necesitan guardarse (la memoria asignada puede liberarse).

Para llamar a una función de modificación de mensaje, el filtro debe establecer el distintivo adecuado en la descripción que se pasa a la función **smfi\_register**. Si el distintivo no está establecido, MTA tratará a la llamada a la función como un fallo del filtro, y finalizará la conexión.

**Nota:** El estado devuelto por la función indica si el filtro del mensaje se envió satisfactoriamente al MTA. El estado no indica si el MTA ha realizado la operación solicitada. Por ejemplo, la función **smfi\_header**, cuando se llama con un nombre de cabecera ilegal, devuelve el distintivo MI\_SUCCESS aunque el MTA pueda rechazar más tarde añadir la cabecera ilegal.

Tabla 18. funciones de Mod		
Item	Descripción	función
<b>smfi_addheader</b>	La función <b>smfi_addheader</b> añade una cabecera al mensaje.	<b>SMFIF_ADDHDRS</b>
<b>smfi_chgheader</b>	La función <b>smfi_chgheader</b> modifica o suprime una cabecera.	<b>SMFIF_CHGHDRS</b>
<b>smfi_insheader</b>	La función <b>smfi_insheader</b> inserta una cabecera en el mensaje.	<b>SMFIF_ADDHDRS</b>
<b>smfi_chgfrom</b>	La función <b>smfi_chgfrom</b> modifica la dirección del remitente del sobre.	<b>SMFIF_CHGFROM</b>
<b>smfi_addrcpt</b>	La función <b>smfi_addrcpt</b> añade un destinatario al sobre.	<b>SMFIF_ADDRCPT</b>
<b>smfi_addrcpt_par</b>	La función <b>smfi_addrcpt_par</b> añade un destinatario, incluido el parámetro del protocolo simple de transferencia de correo (ESMTP) ampliado al sobre.	<b>SMFIF_ADDRCPT_PAR</b>
<b>smfi_delrcpt</b>	La función <b>smfi_delrcpt</b> suprime un destinatario del sobre.	<b>SMFIF_DELRCPT</b>
<b>smfi_replacebody</b>	La función <b>smfi_replacebody</b> sustituye el cuerpo del mensaje.	<b>SMFIF_CHGBODY</b>

### Función **smfi\_addheader**

#### Finalidad

La función **smfi\_addheader** añade una cabecera al mensaje actual.

#### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_addheader(
    SMFICTX *ctx,
    char *headerf,
    char *headerv
);
```

#### Descripción

La función **smfi\_addheader** se llama desde la función **xxfi\_eom** para añadir una cabecera al mensaje.

La función **smfi\_addheader** no modifica las cabeceras existentes de un mensaje.

Para modificar el valor actual de una cabecera, utilice la función **smfi\_chgheader**.

Un filtro que llama a la función **smfi\_addheader** debe establecer el distintivo **SMFIF\_ADDHDRS** en el argumento **smfiDesc\_str**. El filtro pasará entonces el valor a la función **smfi\_register**.

La función **smfi\_addheader** requiere que se especifique el orden del filtro. Puede visualizar las modificaciones en la cabecera utilizando los filtros que se crearon anteriormente.

El nombre o el valor de la cabecera no se comprueba para el cumplimiento de los estándares. Sin embargo, cada línea de la cabecera debe tener menos de 998 caracteres. Si necesita nombres de cabeceras más largos, utilice una cabecera de varias líneas. Si debe crear una cabecera de varias líneas, inserte un salto de línea (ASCII 0x0a, o \n en el lenguaje de programación C) seguido por un carácter de espacio en blanco como un espacio (ASCII 0x20) o un tabulador (ASCII 0x09 o \t en el lenguaje de programación C). El salto de línea no puede estar precedido por un retorno de carro (ASCII 0x0d). El agente de transferencia de correo (MTA) lo añade automáticamente. La responsabilidad de los escritores de filtros debe asegurar que no se viole ningún estándar.

El MTA añade un espacio inicial a un valor de cabecera añadido, a menos que se establezca el distintivo **SMFIP\_HDR\_LEADSPC**, en cuyo caso el parámetro **milter** debe incluir cualquier espacio inicial deseado.

## Argumentos

Tabla 19. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>headerf</i>	El nombre de la cabecera es una serie terminada en nulo que no es NULL.
<i>headerv</i>	El valor de la cabecera que se añadirá puede ser una serie terminada en nulo no NULL o una serie vacía.

## Valores de retorno

La función **smfi\_addheader** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento *headerf* o *headerv* es NULL.
- La adición de cabeceras en el estado de conexión actual no es válido.
- Ha fallado la asignación de memoria.
- Se ha producido un error de red.
- El distintivo **SMFIF\_ADDHDRS** no se ha establecido cuando se ha llamado la función **smfi\_register**.

## Ejemplo

```
int ret;
SMFICTX *ctx;
...
ret = smfi_addheader(ctx, "Content-Type",
"multipart/mixed;\n\tboundary=\"foobar\"");
```

## Información relacionada

[libmilter\\_xxfi\\_eom.dita](#)

[libmilter\\_smfi\\_chgheader.dita](#)

[libmilter\\_smfi\\_register.dita](#)

## Función **smfi\_chgheader**

### Finalidad

La función **smfi\_chgheader** modifica o suprime una cabecera de mensaje.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_chgheader(
    SMFICTX *ctx,
    char *headerf,
    mi_int32 hridx,
    char *headerv
);
```

### Descripción

La función **smfi\_chgheader** se llama desde la función **xxfi\_eom** para modificar un valor headers para el mensaje actual.

La función **smfi\_chgheader** se puede utilizar para añadir nuevas cabeceras. Sin embargo, es eficiente y más seguro utilizar la función **smfi\_addheader**.

Un filtro que llama la función **smfi\_chgheader** debe establecer el distintivo **SMFIF\_CHGHDRS** en el argumento **smfiDesc\_str**. El filtro pasará entonces el valor a la función **smfi\_register**.

La función **smfi\_chgheader** requiere que se especifique el orden del filtro. Puede visualizar las modificaciones en la cabecera utilizando los filtros que se crearon anteriormente.

El nombre o el valor de la cabecera no se comprueba para el cumplimiento de los estándares. Sin embargo, cada línea de la cabecera debe tener menos de 998 caracteres. Si necesita nombres de cabeceras más largos, utilice una cabecera de varias líneas. Si debe crear una cabecera de varias líneas, inserte un salto de línea (ASCII 0x0a, o \n en el lenguaje de programación C) seguido por un carácter de espacio en blanco como un espacio (ASCII 0x20) o un tabulador (ASCII 0x09 o \t en el lenguaje de programación C). El salto de línea no puede estar precedido por un retorno de carro (ASCII 0x0d), un agente de transferencia de correo (MTA) lo añade automáticamente. La responsabilidad de los escritores de filtros debe asegurar que no se viole ningún estándar.

El MTA añade un espacio inicial a un valor de cabecera añadido, a menos que se establezca el distintivo **SMFIP\_HDR\_LEADSPC**, en cuyo caso el parámetro **milter** debe incluir los espacios iniciales deseados.

### Argumentos

Tabla 20. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>headerf</i>	El nombre de la cabecera es una serie terminada en nulo que no es NULL.
<i>hridx</i>	El valor de índice de cabecera (basado en uno). Un valor de <i>hridx</i> de 1 modifica la primera aparición de una cabecera denominada <i>headerf</i> . Si <i>hridx</i> es mayor que el número de veces que aparece <i>headerf</i> , se añadirá una nueva copia de <i>headerf</i> .
<i>headerv</i>	El valor de la cabecera que se añadirá puede ser una serie terminada en nulo no NULL o una serie vacía.

## Valores de retorno

La función **smfi\_chgheader** devuelve el valor MI\_FAILURE en los casos siguientes. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento *headerf* es NULL.
- La modificación de las cabeceras en el estado de conexión actual no es válido.
- Ha fallado la asignación de memoria.
- Se ha producido un error de red.
- El distintivo **SMFIF\_CHGHDRS** no se ha establecido cuando se ha llamado la función **smfi\_register**.

## Ejemplo

```
int ret;
SMFICTX *ctx;
...
ret = smfi_chgheader(ctx, "Content-Type", 1,
"multipart/mixed;\n\tboundary=\"foobar\"");
```

## Información relacionada

[libmilter\\_xxfi\\_eom.dita](#)

[libmilter\\_smfi\\_addheader.dita](#)

## Función **smfi\_insheader**

### Finalidad

La función **smfi\_insheader** antepone una cabecera al mensaje actual.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_insheader(
SMFICTX ,
int hdridx,
char *headerf,
char *headerv
);
```

### Descripción

La función **smfi\_insheader** se llama desde la función **xxfi\_eom**, para anteponer una cabecera al mensaje actual.

La función **smfi\_insheader** no modifica las cabeceras existentes de un mensaje.

Para cambiar el valor actual de una cabecera, utilice la función **smfi\_chgheader**.

Un filtro que llama la función **smfi\_insheader** debe establecer el distintivo **SMFIF\_ADDHDRS** en el argumento *smfiDesc\_str*, que se pasa en la función **smfi\_register**.

La función **smfi\_insheader** requiere que se especifique el orden del filtro. Puede visualizar las modificaciones en la cabecera utilizando los filtros que se crearon anteriormente.

Un filtro recibe cabeceras que se envían mediante el cliente del protocolo simple de transferencia de correo (SMTP) y también las cabeceras modificadas por los filtros anteriores. Las cabeceras insertadas por el mandato **sendmail** y las cabeceras insertadas por él mismo no se reciben. La posición para insertar la cabecera depende de las cabeceras existentes en el mensaje entrante y también de las cabeceras configuradas que se añadirán mediante el mandato **sendmail**.

Por ejemplo, el mandato **sendmail** siempre añade un **Received: header** a comienzo de la cabecera. Al establecer el valor *hdridx* en 0, la cabecera se inserta antes del parámetro **Received: header**. Sin embargo, los filtros quedarán corruptos cuando reciban la cabecera añadida, pero no el **Received: header**, haciendo difícil insertar una cabecera en una posición fija.

Si el valor *hdridx* es mayor que el número de cabeceras del mensaje, la cabecera se agregaría.

El nombre o el valor de la cabecera no se comprueba para el cumplimiento de los estándares. Sin embargo, cada línea de la cabecera debe tener menos de 998 caracteres. Si necesita nombres de cabeceras más largos, utilice una cabecera de varias líneas. Si debe crear una cabecera de varias líneas, inserte un salto de línea (ASCII 0x0a, o \n en el lenguaje de programación C) seguido por un carácter de espacio en blanco como un espacio (ASCII 0x20) o un tabulador (ASCII 0x09 o \t en el lenguaje de programación C). El salto de línea no puede estar precedido por un retorno de carro (ASCII 0x0d). El agente de transferencia de correo (MTA) añade el retorno de carro automáticamente. La responsabilidad de los escritores de filtros debe asegurar que no se viole ningún estándar.

El MTA añade un espacio inicial a un valor de cabecera insertado, a menos que se establezca el distintivo **SMFIP\_HDR\_LEADSPC**, en cuyo caso el parámetro **milter** debe incluir cualquier espacio inicial deseado.

## Argumentos

Tabla 21. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>headerf</i>	El nombre de la cabecera es una serie terminada en nulo que no es NULL.
<i>headerv</i>	El valor de la cabecera que se añadirá puede ser una serie terminada en nulo no NULL o una serie vacía.

## Valores de retorno

La función **smfi\_insheader** devuelve el valor MI\_FAILURE en los casos siguientes, de lo contrario la función devuelve MI\_SUCCESS.

- El argumento *headerf* o *headerv* es NULL.
- La adición de cabeceras en el estado de conexión actual no es válido.
- Ha fallado la asignación de memoria.
- Se ha producido un error de red.
- El distintivo **SMFIF\_ADDHDRS** no se ha establecido cuando se ha llamado a la función **smfi\_register**.

## Ejemplo

```
int ret;
SMFICTX *ctx;
...
ret = smfi_insheader( ctx, 0, "First", "See me?");
```

## Información relacionada

[libmilter\\_xxfi\\_eom.dita](#)

[libmilter\\_smfi\\_register.dita](#)

[libmilter\\_smfi\\_chgheader.dita](#)

## Función `smfi_chgfrom`

### Finalidad

La función **smfi\_chgfrom** modifica el remitente del sobre (MAIL From) para el mensaje actual.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_chgfrom(
    SMFICTX *ctx,
    const char *mail,
    char *args
);
```

### Descripción

La función **smfi\_chgfrom** se llama desde la función **xxfi\_eom**, para modificar el remitente del sobre y el MAIL From del mensaje actual.

Un filtro que llama a la función **smfi\_chgfrom** debe establecer el distintivo **SMFIF\_CHGFROM** en el argumento `smfiDesc_str`. El filtro pasará entonces el valor a la función **smfi\_register**.

Todos los argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado se pueden establecer mediante la llamada. Pero el establecimiento de valores para algunos de los argumentos como SIZE y BODY está causando problemas. Por lo tanto, debe tenerse especial cuidado al establecer los argumentos. No hay comentarios del agente de transferencia de correo (MTA) para el parámetro **milter** sobre si la llamada es satisfactoria.

### Argumentos

Tabla 22. Argumentos	
Item	Descripción
<code>ctx</code>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<code>mail</code>	La nueva dirección del remitente.
<code>args</code>	Argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado.

### Valores de retorno

La función **smfi\_chgfrom** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento `mail` es NULL.
- El cambio del remitente en el estado de la conexión actual no es válido.
- Se ha producido un error de red.
- El distintivo **SMFIF\_CHGFROM** no se ha establecido cuando se ha llamado la función **smfi\_register**.

### Información relacionada

[libmilter\\_xxfi\\_eom.dita](#)

[libmilter\\_smfi\\_register.dita](#)

## [Función smfi\\_addrcpt](#)

### **Finalidad**

La función **smfi\_addrcpt** añade un destinatario para el mensaje actual.

### **Sintaxis**

```
#include <libmilter/mfapi.h>
int smfi_addrcpt(
    SMFICTX *ctx,
    char *rcpt
);
```

### **Descripción**

La función **smfi\_addrcpt** se llama únicamente desde la función **xxfi\_eom**, para añadir un destinatario al sobre del mensaje.

**Nota:** El filtro que llama a la función **smfi\_addrcpt** debe establecer el distintivo **SMFIF\_ADDRCPT** en la estructura **smfiDesc\_str** que se pasa a la función **smfi\_register**.

### **Argumentos**

Tabla 23. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
rcpt	La nueva dirección de los destinatarios.

### **Valores de retorno**

La función **smfi\_addrcpt** devuelve el valor **MI\_FAILURE** en los siguientes casos. De lo contrario, la función devolverá **MI\_SUCCESS**.

- El argumento *rcpt* es NULL.
- La adición de destinatarios en el estado de conexión actual no es válido.
- Se ha producido un error de red.
- El distintivo **SMFIF\_ADDRCPT** no se ha establecido cuando se ha llamado a la función **smfi\_register**.

### **Información relacionada**

[libmilter\\_xxfi\\_eom.dita](#)

[libmilter\\_smfi\\_register.dita](#)

## [Función smfi\\_addrcpt\\_par](#)

### **Finalidad**

La función **smfi\_addrcpt\_par** añade un destinatario para el mensaje actual, incluidos los argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado.

### **Sintaxis**

```
#include <libmilter/mfapi.h>
int smfi_addrcpt_par(
    SMFICTX *ctx,
    char *rcpt,
```

```
char *args  
);
```

## Descripción

La función **smfi\_addrcpt\_par** se llama desde la función **xxfi\_eom**, para añadir un destinatario al sobre del mensaje.

## Argumentos

Tabla 24. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>rcpt</i>	La nueva dirección de los destinatarios.
<i>args</i>	Los nuevos parámetros ESMTP de los destinatarios.

## Valores de retorno

La función **smfi\_addrcpt** devuelve el valor **MI\_FAILURE** en los casos siguientes. De lo contrario, la función devolverá **MI\_SUCCESS**.

- El argumento *rcpt* es NULL.
- La adición de destinatarios en el estado de conexión actual no es válido.
- Se ha producido un error de red.
- El distintivo **SMFIF\_ADDRCPT\_PAR** no se ha establecido cuando se ha llamado la función **smfi\_register**.

## Información relacionada

[libmilter\\_smfi\\_addrcpt.dita](#)

[libmilter\\_smfi\\_register.dita](#)

## Función **smfi\_delrcpt**

### Finalidad

La función **smfi\_delrcpt** suprime el destinatario desde el sobre del mensaje actual.

### Sintaxis

```
#include <libmilter/mfapi.h>  
int smfi_delrcpt(  
    SMFICTX *ctx;  
    char *rcpt;  
>;
```

## Descripción

La función **smfi\_delrcpt** se llama desde la función de devolución de llamada **xxfi\_eom** para eliminar el destinatario llamado desde el sobre de mensajes actual.

**Nota:** Las direcciones que se eliminarán deben coincidir exactamente. Por ejemplo, una dirección y su forma ampliada no coinciden.

## Argumentos

Tabla 25. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>rcpt</i>	La dirección del destinatario que se eliminará, una serie terminada en nulo y no NULL.

## Valores de retorno

La función **smfi\_delrcpt** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- El argumento *rcpt* es NULL.
- La supresión de los destinatarios en el estado de conexión actual no es válido.
- Se ha producido un error de red.
- El distintivo SMFIF\_DELRcpt no se ha establecido cuando se ha llamado la función **smfi\_register**.

## Información relacionada

[smfi\\_register](#)

[xxfi\\_eom](#)

## Función smfi\_replacebody

### Finalidad

La función **smfi\_replacebody** sustituye el cuerpo del mensaje.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_replacebody(
    SMFICTX *ctx,
    unsigned char *bodyp,
    int bodylen
);
```

### Descripción

La función **smfi\_replacebody** sustituye el cuerpo del mensaje actual. Si la función se llama más de una vez, las llamadas posteriores resultan en que se adjunten datos al nuevo cuerpo. La función puede llamarse más de una vez.

Debido a que el cuerpo del mensaje es demasiado grande, el establecimiento del distintivo SMFIF\_CHGBODY puede afectar de forma significativa al rendimiento del filtro.

Si un filtro establece el distintivo SMFIF\_CHGBODY, pero no llama a la función **smfi\_replacebody**, el cuerpo original seguirá sin cambiarse.

El orden del filtro es importante para la función **smfi\_replacebody**. Los nuevos contenidos del cuerpo se crean mediante filtros antiguos en los nuevos archivos de filtros.

## Argumentos

Tabla 26. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>bodyp</i>	Un puntero al comienzo de los nuevos datos del cuerpo, que no tienen que estar terminados en nulo. Si el <i>bodyp</i> es NULL, se tratará como de longitud == 0. Los datos del cuerpo deben estar en formato CR o LF.
<i>bodylen</i>	El número de bytes de los datos apuntados por <i>bodyp</i> .

## Valores de retorno

La función **smfi\_replacebody** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- *bodyp* == NULL and *bodylen* > 0
- El cambio del cuerpo en el estado de conexión actual no es válido.
- Se ha producido un error de red.
- El distintivo SMFIF\_CHGBODY no se ha establecido cuando se ha llamado a la función **smfi\_register**.

## Información relacionada

[smfi\\_register](#)

## Funciones de manejo de mensajes

Las funciones de manejo de mensajes proporcionan instrucciones de caso de manejo especiales para el parámetro **milter** o el agente de transferencia de correo (MTA), sin alterar el contenido ni el estado del mensaje. Las Funciones de manejo de mensajes se pueden llamar únicamente en la función **xxfi\_eom**. La función **xxfi\_eom** puede invocar la comunicación adicional con el MTA y devolver el valor MI\_SUCCESS o MI\_FAILURE para indicar el estado de la operación.

**Nota:** El estado devuelto por la función indica si el mensaje de los filtros se envió satisfactoriamente al MTA. El estado no indica si el MTA ha realizado la operación solicitada.

Tabla 27. función de manejo de mensajes	
Item	Descripción
<b>smfi_progress</b>	La función <b>smfi_progress</b> informa de la operación en curso.
<b>smfi_quarantine</b>	La función <b>smfi_quarantine</b> pone en cuarentena un mensaje.

## Función **smfi\_progress**

### Finalidad

La función **smfi\_progress** informa del progreso de la operación.

## Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_progress(
    SMFICTX *ctx;
);
```

## Descripción

La función **smfi\_progress** se llama desde la función de devolución de llamada **xxfi\_eom** para notificar al agente de transferencia de correo (MTA) de que el filtro sigue funcionando en un mensaje. Esta función hace que MTA reinicie sus tiempos de espera.

## Argumentos

Tabla 28. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

## Valores de retorno

La función **smfi\_progress** devuelve el valor MI\_FAILURE si hay un error de red. De lo contrario, la función devolverá MI\_SUCCESS.

## Información relacionada

[xxfi\\_eom](#)

[\*\*Función smfi\\_quarantine\*\*](#)

## Finalidad

La función **smfi\_quarantine** pone en cuarentena el mensaje.

## Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_quarantine(
    SMFICTX *ctx;
    char *reason;
);
```

## Descripción

La función **smfi\_quarantine** se llama desde la función de devolución de llamada **xxfi\_eom** para poner en cuarentena un mensaje utilizando un motivo determinado.

## Argumentos

Tabla 29. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
reason	El motivo de la cuarentena, una serie terminada en nulo, no NULL y no vacía.

## Valores de retorno

La función **smfi\_quarantine** devuelve el valor MI\_FAILURE en los siguientes casos. De lo contrario, la función devolverá MI\_SUCCESS.

- El *reason* es NULL o vacío.
- Se ha producido un error de red.
- El distintivo SMFIF\_QUARANTINE no se ha establecido cuando se ha llamado a la función **smfi\_register**.

## Información relacionada

[smfi\\_register](#)

[xxfi\\_eom](#)

## Funciones de devolución de llamada

El filtro sendmail debe implementar una o varias de las funciones de devolución de llamada, que se registran mediante la función **smfi\_register**.

Tabla 30. funciones de devolución de llamada	
Item	Descripción
<b>xxfi_connect</b>	La función <b>xxfi_connect</b> se llama una vez al comienzo de cada conexión SMTP. La función devuelve el valor SMFIS_CONTINUE.
<b>xxfi_hello</b>	La función <b>xxfi_hello</b> se llama siempre que el cliente envía un mandato HELO/EHLO.
<b>xxfi_envfrom</b>	La función <b>xxfi_envfrom</b> se llama al comienzo de un mensaje.
<b>xxfi_envrcpt</b>	La función <b>xxfi_envrcpt</b> se llama para cada destinatario.
<b>xxfi_data</b>	La función <b>xxfi_data</b> maneja el mandato DATA.
<b>xxfi_unknown</b>	La función <b>xxfi_unknown</b> maneja mandatos de protocolo de transferencia de correo sencillos desconocidos (SMTP).
<b>xxfi_header</b>	La función <b>xxfi_header</b> maneja una cabecera de mensaje.
<b>xxfi_eoh</b>	La función <b>xxfi_eoh</b> maneja las cabeceras de mensajes.
<b>xxfi_body</b>	La función <b>xxfi_body</b> maneja un fragmento de un cuerpo de mensajes.
<b>xxfi_eom</b>	La función <b>xxfi_eom</b> maneja el final del mensaje.
<b>xxfi_abort</b>	La función <b>xxfi_abort</b> maneja los mensajes que terminaron anormalmente.
<b>xxfi_close</b>	La función <b>xxfi_close</b> se llama para cerrar la conexión actual.
<b>xxfi_negotiate</b>	La función <b>xxfi_negotiate</b> se llama al comienzo de la conexión SMTP.

Las funciones de devolución de llamada deben devolver un valor apropiado. Si las funciones de devolución de llamada devuelven cualquier otro valor que el valor definido, constituirá un error, y el mandato **sendmail** finalizará la conexión con el filtro.

El parámetro **Milter** distingue entre rutinas **orientadas al destinatario**, **orientadas al mensaje** y **orientadas a la conexión**:

- Las funciones de devolución de llamada **orientadas al destinatario** afectan al proceso de un único destinatario del mensaje.
- Las funciones de devolución de llamada **orientadas al mensaje** afectan a un único mensaje.
- Las funciones de devolución de llamada **orientadas a la conexión** afectan a toda la conexión (durante la cual se pueden enviar varios mensajes a varios conjuntos de destinatarios).
- La función **xxfi\_envrcpt** está orientada al destinatario. Las funciones **xxfi\_connect**, **xxfi\_hello** y **xxfi\_close** están orientadas a la conexión. El resto de las funciones de devolución de llamada están orientadas al mensaje.

*Tabla 31. Funciones de devolución de llamada*

Item	Descripción
SMFIS_CONTINUE	Continúe procesando la conexión, el mensaje o el destinatario actual.
SMFIS_REJECT	<ul style="list-style-type: none"> <li>• Para una rutina <b>orientada a la conexión</b>, rechace esta conexión; llame a <b>xxfi_close</b>.</li> <li>• Para una rutina <b>orientada al mensaje</b> (a excepción de la función <b>xxfi_eom</b> o la función <b>xxfi_abort</b>), rechace este mensaje.</li> <li>• Para una rutina <b>orientada al destinatario</b>, rechace el destinatario actual (pero continúe procesando el mensaje actual).</li> </ul>
SMFIS_DISCARD	<ul style="list-style-type: none"> <li>• Para una rutina <b>orientada al mensaje</b> u <b>orientada al destinatario</b>, acepte este mensaje, pero descártelo.</li> <li>• SMFIS_DISCARD no debe devolverse mediante una rutina <b>orientada a la conexión</b>.</li> </ul>
SMFIS_ACCEPT	<ul style="list-style-type: none"> <li>• Para una rutina <b>orientada a la conexión</b>, acepte esta conexión sin ningún proceso de filtrado adicional; llame a la función <b>xxfi_close</b>.</li> <li>• Para una rutina <b>orientada al mensaje</b> o <b>al destinatario</b>, acepte este mensaje sin ningún filtrado adicional.</li> </ul>

Tabla 31. Funciones de devolución de llamada (continuación)

Item	Descripción
SMFIS_TEMPFAIL	<p>Devuelve un fallo temporal, es decir, el mandato de protocolo de transferencia de correo simple correspondiente (SMTP) devuelve el código de estado 4xx.</p> <ul style="list-style-type: none"> <li>Para una rutina <b>orientada al mensaje</b> (a excepción de la función <code>xxfi_envfrom</code>), apruebe este mensaje.</li> <li>Para una rutina <b>orientada a la conexión</b>, apruebe esta conexión; llame a la función <code>xxfi_close</code>.</li> <li>Para una rutina <b>orientada al destinatario</b>, apruebe sólo el destinatario actual; continúe procesando el mensaje.</li> </ul>
SMFIS_SKIP	<p>Omita devoluciones de llamadas posteriores del mismo tipo en esta transacción. Actualmente, este valor de retorno sólo se permite en la función <code>xxfi_body</code>. El valor de retorno se puede utilizar si un parámetro <b>milter</b> ha recibido suficientes fragmentos del cuerpo para tomar una decisión. Pero si el valor de retorno aún desea invocar las funciones de modificación del mensaje que sólo están permitidas llamarse desde la función <code>xxfi_eom</code>.</p> <p><b>Nota:</b> El parámetro <b>milter</b> debe negociar este comportamiento con el agente de transferencia de correo (MTA). El parámetro <b>milter</b> comprobará si la acción de protocolo SMFIP_SKIP está disponible. Si la acción de protocolo SMFIP_SKIP está disponible, el parámetro <b>milter</b> debe solicitarla.</p>

Tabla 31. Funciones de devolución de llamada (continuación)

Item	Descripción
SMFIS_NOREPLY	<ul style="list-style-type: none"> <li>• No envíe una respuesta al MTA. El parámetro <b>milter</b> debe negociar este comportamiento con el MTA. El parámetro <b>milter</b> debe comprobar si la acción de protocolo adecuada SMFIP_NR_* está disponible. Si la acción de protocolo SMFIP_NR_* está disponible, el parámetro <b>milter</b> debe solicitarla.</li> <li>• Si establece la acción de protocolo SMFIP_NR_* para una devolución de llamada, dicha devolución de llamada debe siempre responderse con SMFIS_NOREPLY. La utilización de cualquier otro código de respuesta es una violación de la interfaz de programación de la aplicación (API). Si en algunos casos su devolución de llamada puede devolver otro valor (debido a algunas reducciones de recursos), no debe establecer SMFIP_NR_* y debe utilizar SMFIS_CONTINUE como el código de retorno predeterminado. De forma alternativa, puede intentar retrasar informar del problema en una devolución de llamada posterior para la que SMFIP_NR_* no está establecido.</li> </ul>

### Función de devolución de llamada **xxfi\_connect**

#### Finalidad

La función de devolución de llamada **xxfi\_connect** proporciona la información de conexión.

#### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_connect)(
    SMFICTX    *ctx,
    char       *hostname,
    _SOCK_ADDR *hostaddr);
```

#### Descripción

La función de devolución de llamada **xxfi\_connect** se llama una vez al comienzo de cada conexión del protocolo simple de transferencia de correo (SMTP) y devuelve el distintivo SMFIS\_CONTINUE.

**Nota:** Si un filtro anterior rechaza la conexión en la rutina de función de devolución de llamada **xxfi\_connect**, la función de devolución de llamada **xxfi\_connect** del filtro no se llamará.

#### Argumentos

Tabla 32. Argumentos

Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el <b>libmilter</b> .

Tabla 32. Argumentos (continuación)

Item	Descripción
hostname	El nombre de sistema principal del remitente del mensaje, como determina una búsqueda inversa en la dirección del sistema principal. Si la búsqueda inversa falla o si ninguna de las direcciones IP de los nombres de host resueltos coincide con el original dirección IP, el nombre de host contendrá el mensaje del remitente dirección IP, que se ha especificado entre corchetes (por ejemplo, '[a.b.c.d]'). Si la conexión del protocolo simple de transferencia de correo (SMTP) se realiza mediante stdin, el valor es localhost.
hostaddr	La dirección de sistema principal, como se determina mediante la llamada <b>getpeername(2)</b> en el socket SMTP. El valor es NULL si el tipo no está soportado en la versión actual o si la conexión SMTP se realiza mediante <b>stdin</b> .

### Función de devolución de llamada **xxfi\_hello**

#### Finalidad

La función de devolución de llamada **xxfi\_hello** maneja el mandato **HELO** o **EHLO**.

#### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_hello)(
    SMFICTX *ctx,
    char *helohost
);
```

#### Descripción

La función de devolución de llamada **xxfi\_hello** se llama siempre que el cliente envíe un mandato **HELO** o **EHLO** y devuelva el distintivo SMFIS\_CONTINUE. La devolución de llamada puede llamarse por lo tanto varias veces o incluso no llamarse. Se pueden imponer algunas restricciones mediante la configuración del agente de transferencia de correo (MTA).

#### Argumentos

Tabla 33. Argumentos

Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
helohost	El valor pasado al mandato <b>HELO</b> o <b>EHLO</b> , debe ser el nombre de dominio del sistema principal de envío

### Función de devolución de llamada **xxfi\_envfrom**

#### Finalidad

La función de devolución de llamada **xxfi\_envfrom** maneja el mandato **MAIL** (remitente del sobre).

## Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_envfrom)(
    SMFICTX *ctx,
    char **argv
);
```

## Descripción

La función de devolución de llamada **xxfi\_envfrom** se llama cuando el cliente utiliza el mandato **DATA** y devuelve el distintivo SMFIS\_CONTINUE.

**Nota:** Para obtener más detalles sobre las respuestas de ESMTP, consulte [RFC 1869](#).

## Argumentos

Tabla 34. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
argv	Los argumentos del mandato SMTP terminado en nulo; argv[0] está garantizada como la dirección del remitente. Los argumentos posteriores son los argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado.

## Valores de retorno

Tabla 35. Valores de retorno	
Item	Descripción
SMFIS_TEMPFAIL	El remitente y el mensaje se rechazan con un error temporal; un nuevo remitente (y un nuevo mensaje) se pueden especificar más tarde y la función de devolución de llamada <b>xxfi_abort</b> no se llamará.
SMFIS_REJECT	El remitente y el mensaje se rechazan; se pueden especificar un nuevo remitente y mensaje y la función de devolución de llamada <b>xxfi_abort</b> no se llamará.
SMFIS_DISCARD	El mensaje se acepta y se descarta, y la función de devolución de llamada <b>xxfi_abort</b> no se llama.
SMFIS_ACCEPT	El mensaje se acepta y la función de devolución de llamada <b>xxfi_abort</b> no se llama.

## Información relacionada

[xxfi\\_abort](#)

[Función de devolución de llamada xxfi\\_envrcpt](#)

## Finalidad

La función de devolución de llamada **xxfi\_envrcpt** maneja el mandato **RCPT** de sobre.

## Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_envrcpt)(
    SMFICTX *ctx,
    char **argv
);
```

## Descripción

La función de devolución de llamada **xxfi\_envrcpt** se llama una vez por destinatario, y una o más veces por mensaje inmediatamente después de la función de devolución de llamada **xxfi\_envfrom** y devuelve el distintivo SMFIS\_CONTINUE.

**Nota:** Para obtener más detalles sobre las respuestas del protocolo simple de transferencia de correo (ESMTP) ampliado, consulte [RFC 1869](#).

## Argumentos

Tabla 36. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
argv	Los argumentos del mandato SMTP terminado en nulo; argv [0] está garantizado como la dirección del destinatario. Los argumentos posteriores son los argumentos del protocolo simple de transferencia de correo (ESMTP) ampliado.

## Valores de retorno

Tabla 37. Valores de retorno	
Item	Descripción
SMFIS_TEMPFAIL	El destinatario ha fallado de forma temporal; se puede enviar a los destinatarios posteriores y no se ha llamado a la función de devolución de llamada <b>xxfi_abort</b> .
SMFIS_REJECT	El destinatario se ha rechazado; se puede enviar a los destinatarios posteriores y no se ha llamado a la función de devolución de llamada <b>xxfi_abort</b> .
SMFIS_DISCARD	El mensaje se acepta o se descarta, y se llama a la función de devolución de llamada <b>xxfi_abort</b> .
SMFIS_ACCEPT	El destinatario se acepta y la función de devolución de llamada <b>xxfi_abort</b> no se llama.

## Información relacionada

[xxfi\\_envfrom](#)

[xxfi\\_abort](#)

## *Función de devolución de llamada **xxfi\_data***

### **Finalidad**

La función de devolución de llamada **xxfi\_data** maneja el mandato **DATA**.

### **Sintaxis**

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_data)(
    SMFICTX *ctx
);
```

### **Descripción**

La función de devolución de llamada **xxfi\_data** se llama cuando el cliente utiliza el mandato **DATA** y devuelve el distintivo **SMFIS\_CONTINUE**.

**Nota:** Para obtener más detalles sobre las respuestas de ESMTP, consulte [RFC 1869](#).

### **Argumentos**

Tabla 38. Argumentos	
Item	Descripción
<code>ctx</code>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

### **Valores de retorno**

Tabla 39. Valores de retorno	
Item	Descripción
<code>SMFIS_TEMPFAIL</code>	El mensaje se rechaza con un error temporal.
<code>SMFIS_REJECT</code>	El mensaje se rechaza.
<code>SMFIS_DISCARD</code>	El mensaje se acepta y descarta.
<code>SMFIS_ACCEPT</code>	El mensaje se acepta.

## *Función de devolución de llamada **xxfi\_unknown***

### **Finalidad**

La función de devolución de llamada **xxfi\_unknown** maneja mandatos de protocolo simple de transferencia de correo (SMTP) desconocido y no implementado.

### **Sintaxis**

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_unknown)(
    SMFICTX *ctx,
    const char *arg
);
```

### **Descripción**

La función de devolución de llamada **xxfi\_unknown** se llama cuando el cliente utiliza un mandato SMTP que es desconocido o que no está implementado por el agente de transferencia de correo (MTA) y que devuelve el distintivo **SMFIS\_CONTINUE**.

**Nota:** El servidor siempre rechaza el mandato SMTP. Sólo es posible devolver un código de error distinto.

## Argumentos

Tabla 40. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
arg	El mandato SMTP, incluidos todos los argumentos.

## Valores de retorno

Tabla 41. Valores de retorno	
Item	Descripción
SMFIS_TEMPFAIL	El mandato se rechaza con un error temporal.
SMFIS_REJECT	El mandato se rechaza.

## Función de devolución de llamada **xxfi\_header**

### Finalidad

La función de devolución de llamada **xxfi\_header** maneja la cabecera del mensaje.

### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_header)(
    SMFICTX *ctx,
    char *headerf,
    char *headeru
);
```

### Descripción

La función de devolución de llamada **xxfi\_header** se llama una vez para cada cabecera de mensaje y devuelve el distintivo SMFIS\_CONTINUE.

#### Nota:

- Comenzando con sendmail 8.14, los espacios tras los dos puntos de un campo de cabecera se reservan si se solicitan utilizando el distintivo SMFIP\_HDR\_LEADSPC. Por ejemplo, la siguiente cabecera:

```
From: sender <f@example.com>
To: user <t@example.com>
Subject: no
```

se enviaría a un parámetro **milter** como sigue:

```
"From", "sender <f@example.com>"
"To", "user <t@example.com>"
"Subject", "no"
```

mientras que anteriormente (o sin el distintivo SMFIP\_HDR\_LEADSPC) era como sigue:

```
"From", "sender <f@example.com>"
"To", "user <t@example.com>"
"Subject", "no"
```

- El filtro antiguo realiza cambios o adiciones en la cabecera a los nuevos filtros.

- Para obtener más detalles sobre el formato de la cabecera, consulte [RFC 822](#) y [RFC 2822](#).

## Argumentos

Tabla 42. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>headerf</i>	El nombre del campo de la cabecera.
<i>headerv</i>	El valor del campo de la cabecera. El contenido de la cabecera puede incluir un espacio en blanco doblado, es decir, varias líneas con el siguiente espacio en blanco donde las líneas están separadas por LF (ni CR ni LF). Se elimina el terminador de línea de cola (CR o LF).

## Información relacionada

[RFC 2822](#)

[RFC 822](#)

## Función de devolución de llamada `xxfi_eoh`

### Finalidad

La función de devolución de llamada **xxfi\_eoh** maneja el final de las cabeceras de mensajes.

### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_eoh)(
    SMFICTX *ctx
);
```

### Descripción

La función de devolución de llamada **xxfi\_eoh** se llama una vez que todas las cabeceras se hayan enviado y procesado, y devuelve el distintivo SMFIS\_CONTINUE.

## Argumentos

Tabla 43. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

## Función de devolución de llamada `xxfi_body`

### Finalidad

La función de devolución de llamada **xxfi\_body** maneja una parte de un cuerpo de mensajes.

### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_body)(
    SMFICTX *ctx,
```

```

    unsigned char *bodyp,
    size_t len
);

```

## Descripción

La función de devolución de llamada **xxfi\_body** no se llama o se llama muchas veces entre la función de devolución de llamada **xxfi\_eoh** y **xxfi\_eom** y devuelve el distintivo SMFIS\_CONTINUE.

### Nota:

- Los puntos **bodyp** para una secuencia de bytes. No es una serie C (una secuencia de caracteres que se termina mediante '\0'). Por lo tanto, no utilice las funciones de series de C normales como **strlen(3)** en este bloque de bytes. La secuencia de bytes debe contener caracteres de '\0' dentro del bloque. Por lo tanto, aunque se añada un '\0' de cola, las funciones de serie C no seguirán funcionando como se espera.
- Dado que los cuerpos de los mensajes pueden ser grandes, la definición de la función de devolución de llamada **xxfi\_body** puede afectar de forma significativa al rendimiento del filtro.
- Los fines de línea se representan como recibidos desde SMTP (normalmente CR/LF).
- Los filtros antiguos realizan cambios del cuerpo en los nuevos filtros.
- Los cuerpos de los mensajes se pueden enviar en varios fragmentos con una llamada a la función de devolución de llamada **xxfi\_body** por fragmento.
- Esta función devuelve el distintivo SMFIS\_SKIP si un parámetro milter ha recibido los suficientes fragmentos del cuerpo para tomar una decisión, pero aún desea invocar las funciones de modificación del mensaje que sólo permiten llamarse desde la función de devolución de llamada **xxfi\_eom**.
- El parámetro milter debe negociar este comportamiento con el agente de transferencia de correo (MTA), es decir, debe comprobar si el distintivo de acción del protocolo SMFIP\_SKIP está disponible y, si es así, el parámetro **milter** debe solicitarlo.

## Argumentos

Tabla 44. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>bodyp</i>	El puntero al comienzo de este bloque de los datos del cuerpo. <i>bodyp</i> no es válido fuera de esta llamada en la función de devolución de llamada <b><u>xxfi_body</u></b> .
<i>len</i>	La cantidad de datos apuntados por <i>bodyp</i> .

## Información relacionada

[xxfi\\_eoh](#)

[xxfi\\_eom](#)

[\*\*Función de devolución de llamada xxfi\\_eom\*\*](#)

## Finalidad

La función de devolución de llamada **xxfi\_eom** maneja el final del mensaje.

## Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_eom)(
    SMFICTX ctx
);
```

## Descripción

La función de devolución de llamada **xxfi\_eom** se llama una vez después de todas las llamadas a la función de devolución de llamada **xxfi\_body** para un mensaje determinado y devuelve el distintivo **SMFIS\_CONTINUE**.

**Nota:** Es necesario un filtro para realizar todas sus modificaciones a las cabeceras, el cuerpo y el sobre del mensaje en la función de devolución de llamada **xxfi\_eom**. Las modificaciones se realizan mediante las rutinas **smfi\_\***.

## Argumentos

Tabla 45. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

## Información relacionada

[xxfi\\_body](#)

### Función de devolución de llamada **xxfi\_abort**

## Finalidad

La función de devolución de llamada **xxfi\_abort** maneja los mensajes actuales que están terminando anormalmente.

## Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_abort)(
    SMFICTX ctx
);
```

## Descripción

La función de devolución de llamada **xxfi\_abort** se llama en cualquier momento durante el proceso de mensajes (es decir, entre alguna rutina orientada a mensajes y la función de devolución de llamada **xxfi\_eom**) y devuelve el distintivo **SMFIS\_CONTINUE**.

### Nota:

- La función de devolución de llamada **xxfi\_abort** debe reclamar cualquier recurso asignado en una base por mensaje, y debe ser tolerante sobre llamarse entre cualquier devolución de llamadas orientadas a mensajes.
- Las llamadas a la función de devolución de llamada **xxfi\_abort** y **xxfi\_eom** son mutuamente excluyentes.
- La función de devolución de llamada **xxfi\_abort** no es responsable de reclamar datos específicos de la conexión, ya que la función de devolución de llamada **xxfi\_close** siempre se llama cuando se cierra una conexión.

- Dado que el mensaje actual ya está terminando anormalmente, el valor de retorno se ignora actualmente.
- La función de devolución de llamada **xxfi\_abort** sólo se llama si el mensaje termina anormalmente fuera del control del filtro y el filtro no ha completado el proceso orientado a mensajes. Por ejemplo, si un filtro ya ha devuelto el distintivo SMFIS\_ACCEPT, SMFIS\_REJECT o SMFIS\_DISCARD desde una rutina orientada a mensajes. La función de devolución de llamada **xxfi\_abort** no se llamará aunque el mensaje termine anormalmente más tarde fuera de control.

## Argumentos

Tabla 46. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el <b>libmilter</b> .

## Información relacionada

[xxfi\\_close](#)

[xxfi\\_eom](#)

### Función de devolución de llamada **xxfi\_close**

#### Finalidad

La función de devolución de llamada **xxfi\_close** cerrará la conexión actual.

#### Sintaxis

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_close)(
    SMFICTX *ctx
);
```

#### Descripción

La función de devolución de llamada **xxfi\_close** siempre se llama una vez al final de cada conexión y devuelve el distintivo SMFIS\_CONTINUE.

La función de devolución de llamada **xxfi\_close** puede llamarse fuera de secuencia, es decir, antes incluso de que se llame la función de devolución de llamada **xxfi\_connect**. Una vez que establezca una conexión el agente de transferencia de correo (MTA) con el filtro, si el MTA decide que se descarte el tráfico de esta conexión (por ejemplo, mediante un resultado access\_db), no se pasarán datos al filtro desde el MTA hasta que el cliente se cierre. En tal momento, se llamará la función de devolución de llamada **xxfi\_close**. Puede ser, por lo tanto, la única devolución de llamada utilizada para una conexión determinada, y debe anticipar esta posibilidad al controlar manualmente el código de función de devolución de llamada **xxfi\_close**. En concreto, es incorrecto suponer que el puntero de contexto privado será un valor distinto a NULL en esta devolución de llamada.

La función de devolución de llamada **xxfi\_close** se llama en cerrado aunque la transacción de correo anterior terminara anormalmente.

La función de devolución de llamada **xxfi\_close** es responsable de liberar cualquier recurso asignado en una base por conexión.

Dado que la conexión ya se está cerrando, el valor de retorno se ignora actualmente.

## Argumentos

Tabla 47. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .

## Información relacionada

[xxfi\\_connect](#)

[\*\*Función de devolución de llamada xxfi\\_negotiate\*\*](#)

## Finalidad

La función de devolución de llamada **xxfi\_negotiate** maneja la negociación.

## Sintaxis

```
#include <libmilter/mfapi.h>
#include <libmilter/mfdef.h>
sfsistat (*xxfi_negotiate) (
    SMFICTX      *ctx,
    unsigned long f0,
    unsigned long f1,
    unsigned long f2,
    unsigned long f3,
    unsigned long *pf0,
    unsigned long *pf1,
    unsigned long *pf2,
    unsigned long *pf3);
```

## Descripción

La función de devolución de llamada **xxfi\_negotiate** se llama al comienzo de cada conexión del protocolo simple de transferencia de correo (SMTP) y devuelve el distintivo SMFIS\_ALL\_OPTS.

Con esta función, un parámetro **milter** podría determinar de forma dinámica y solicitar operaciones y acciones durante el arranque. En versiones anteriores, las acciones (f0) estaban fijadas en el campo de distintivos de la estructura **smfiDesc** y los campos del protocolo (f1) se derivaban implícitamente comprobando si estaba definida una devolución de llamada. Debido a las extensiones de la nueva versión de **milter**, tal selección estática no funcionaría si un parámetro **milter** requiere nuevas acciones que no estén disponibles cuando se hable a un agente de transferencia de correo (MTA) más antiguo. Así pues, en la negociación, una devolución de llamada puede determinar qué operaciones están disponibles y determinar de forma dinámica aquellas funciones de devolución de llamada que necesita y que se ofrecen. Si algunas operaciones no están disponibles, el parámetro **milter** puede volver a un modo más antiguo o detener la sesión y pedir al usuario que actualice.

## Pasos del protocolo

```
(f1, *pf1)
```

:

- SMFIP\_RCPT\_REJ: Al establecer este trozo, un parámetro **milter** puede solicitar que el MTA también envíe mandatos RCPT que se hayan rechazado porque el usuario es desconocido (o por motivos similares), pero no dichas funciones que se han rechazado por errores de sintaxis. Si un **milter** solicita este paso de protocolo, debe comprobar la macro **{rcpt\_mailer}**: si se configura como error, el MTA puede rechazar el destinatario. Normalmente, las macros **{rcpt\_host}** y **{rcpt\_addr}** pueden contener un código de estado ampliado y un texto de error en tal caso.
- SMFIP\_SKIP indica que el MTA comprende el código de retorno SMFIS\_SKIP.

- SMFIP\_NR\_\* indica que el MTA comprende el código de retorno SMFIS\_NOREPLY. Hay distintivos para varias etapas del protocolo:
  - SMFIP\_NR\_CONN: “Función de devolución de llamada `xxfi_connect`” en la página 86
  - SMFIP\_NR\_HELO: “Función de devolución de llamada `xxfi_helo`” en la página 87
  - SMFIP\_NR\_MAIL: “Función de devolución de llamada `xxfi_envfrom`” en la página 87
  - SMFIP\_NR\_RCPT: “Función de devolución de llamada `xxfi_envrcpt`” en la página 88
  - SMFIP\_NR\_DATA: “Función de devolución de llamada `xxfi_data`” en la página 90
  - SMFIP\_NR\_UNKN: “Función de devolución de llamada `xxfi_unknown`” en la página 90
  - SMFIP\_NR\_EOH: “Función de devolución de llamada `xxfi_eoh`” en la página 92
  - SMFIP\_NR\_BODY: “Función de devolución de llamada `xxfi_body`” en la página 92
  - SMFIP\_NR\_HDR: “Función de devolución de llamada `xxfi_header`” en la página 91
- El distintivo SMFIP\_HDR\_LEADSPC indica que el MTA puede enviar valores de cabecera con el espacio inicial intacto. Si se solicita este paso de protocolo, el MTA no añadiría un espacio inicial a las cabeceras cuando se añaden, ser insertan o se cambian.
- Se puede indicar al MTA que no envíe información sobre varias etapas de SMTP, estos distintivos comienzan con: SMFIP\_NO\*.
  - SMFIP\_NOCONNECT: “Función de devolución de llamada `xxfi_connect`” en la página 86
  - SMFIP\_NOHELO: “Función de devolución de llamada `xxfi_header`” en la página 91
  - SMFIP\_NOMAIL: “Función de devolución de llamada `xxfi_envfrom`” en la página 87
  - SMFIP\_NORCPT: “Función de devolución de llamada `xxfi_envrcpt`” en la página 88
  - SMFIP\_NOBODY: “Función de devolución de llamada `xxfi_body`” en la página 92
  - SMFIP\_NOHDRS: “Función de devolución de llamada `xxfi_header`” en la página 91
  - SMFIP\_NOEOH: “Función de devolución de llamada `xxfi_eoh`” en la página 92
  - SMFIP\_NOUNKNOWN: “Función de devolución de llamada `xxfi_unknown`” en la página 90
  - SMFIP\_NODATA: “Función de devolución de llamada `xxfi_data`” en la página 90

Para cada una de estas **`xxfi_*` callbacks** que un parámetro `milter` no utiliza, el distintivo correspondiente debe establecerse en

\*pf1.

Las acciones disponibles

(f0, \*pf0)

se describen en (**`xxfi_flags`**).

Si un `milter` devuelve el distintivo SMFIS\_CONTINUE, el `milter` establece las acciones deseadas y los pasos del protocolo mediante los parámetros (salida) pf0 y pf1 (que se corresponden con f0 y f1, respectivamente). Los parámetros (salida) pf2 y pf3 deberían establecerse en 0 para su compatibilidad con futuras versiones.

## Argumentos

Tabla 48. Argumentos	
Item	Descripción
ctx	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
f0	Las acciones ofrecidas por el MTA.
f1	Los pasos del protocolo ofrecidos por el MTA.

Tabla 48. Argumentos (continuación)

Item	Descripción
f2	Para futuras extensiones.
f3	Para futuras extensiones.
pf0	Las acciones solicitadas por el <b>milter</b>
pf1	Los pasos del protocolo solicitados por el <b>milter</b> .
pf2	Para futuras extensiones.
pf3	Para futuras extensiones.

### Valores de retorno

Tabla 49. Valores de retorno

Item	Descripción
SMFIS_ALL_OPTS	Si un <b>milter</b> sólo desea inspeccionar las acciones y los pasos del protocolo disponibles, puede devolver el distintivo SMFIS_ALL_OPTS y el MTA hará todas las acciones y los pasos del protocolo disponibles para el <b>milter</b> . En este caso, no se debe asignar ningún valor a los parámetros de salida pf0 - pf3, puesto que se ignorarán.
SMFIS_REJECT	El arranque de <b>milter</b> fallará y puede que no se ponga en contacto de nuevo (para la conexión actual).
SMFIS_CONTINUE	Continúe el proceso. En este caso, el parámetro <b>milter</b> debe establecer todos los parámetros de salida pf0 - pf3. Consulte lo siguiente para obtener una explicación sobre cómo establecer dichos parámetros de salida.

### Funciones varias y constantes

Las funciones varias y constantes captan la información de la versión de los parámetros **libmilter**.

Tabla 50. Funciones constantes

Item	Descripción
<b>smfi_version</b>	La función <b>smfi_version</b> capta la información de la versión del parámetro <b>libmilter</b> (tiempo de ejecución).
<b>smfi_setsymlist</b>	La <b>smfi_setsymlist</b> establece la lista de macros que el parámetro <b>libmilter</b> desea recibir desde el agente de transferencia de correo (MTA) para una etapa del protocolo.

Tabla 51. Funciones constantes

Item	Descripción
<b>SMFI_VERSION</b>	La <b>SMFI_VERSION</b> obtiene la versión de tiempo de ejecución del parámetro <b>libmilter</b> .

## Función **smfi\_version**

### Finalidad

La función **smfi\_version** proporciona la información de la versión **libmilter** (tiempo de ejecución).

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_version(
    unsigned int *pmajor,
    unsigned int *pminor,
    unsigned int *ppl
);
```

### Descripción

La función de devolución de llamadas **smfi\_version** puede llamarse en cualquier momento.

La versión de tiempo de compilación de la biblioteca **libmilter** está disponible en la macro **SMFI\_VERSION**. Para extraer la versión mayor y menor, así como el nivel de parche actual desde esta macro, se pueden utilizar las macros **SM\_LM\_VRS\_MAJOR(v)**, **SM\_LM\_VRS\_MINOR(v)** y **SM\_LM\_VRS\_PLVL(v)**. Un parámetro **milter** puede comprobar la macro **SMFI\_VERSION** para determinar qué funciones utilizar (en el tiempo de la compilación mediante las sentencias del preprocesador C). Al utilizar esta macro y la función **smfi\_version**, un parámetro **milter** puede determinar en el tiempo de ejecución si se ha enlazado (dinámicamente) en la versión de **libmilter** esperada. Tal función debe comparar sólo la versión mayor y menor, no el nivel de parche, es decir, la biblioteca **libmilter** será compatible a pesar de los distintos niveles de parches.

### Argumentos

Tabla 52. Argumentos	
Item	Descripción
<i>pmajor</i>	Un puntero para una variable int no firmada para almacenar el número de versión mayor.
<i>pminor</i>	Un puntero para una variable int no firmada para almacenar el número de versión menor.
<i>ppl</i>	Un puntero para una variable int no firmada para almacenar el número de nivel de parche.

### Valores de retorno

La función **smfi\_version** devuelve el valor **MI\_SUCCESS**.

## Función **smfi\_setsymlist**

### Finalidad

La función **smfi\_setsymlist** establece la lista de macros que el parámetro **milter** quiere recibir desde el agente de transferencia de correo (MTA) para una fase del protocolo.

### Sintaxis

```
#include <libmilter/mfapi.h>
int smfi_setsymlist(
    SMFICTX      *ctx,
    int          stage,
    char        *macros
);
```

## Descripción

La función de devolución de llamada **smfi\_setsymlist** debe llamarse durante la función **xxfi\_negotiate**, y esta función se puede utilizar para sobrescribir la lista de macros que el parámetro **milter** desea recibir desde el agente de transferencia de correo (MTA).

**Nota:** Hay un límite interno en el número de macros que se puede establecer (actualmente 5). Sin embargo, este límite no se fuerza mediante el parámetro **milter**, y sólo se fuerza mediante el MTA, pero una posible violación de esta restricción no se comunicará al parámetro **milter**.

## Argumentos

Tabla 53. Argumentos	
Item	Descripción
<i>ctx</i>	La estructura de contexto opaca se mantiene en el parámetro <b>libmilter</b> .
<i>stage</i>	La etapa del protocolo durante la que la lista de la macro debe utilizarse. Consulte el archivo <code>include/libmilter/mfapi.h</code> para ver los valores legales, y busque las macros C con el prefijo <code>SMFIM_</code> . Las etapas de protocolo disponibles son al menos la conexión inicial, HELO o EHLO, MAIL, RCPT, DATA, el final de la cabecera y el final de un mensaje.
<i>macros</i>	La lista de macros (separada por un espacio). Por ejemplo: " <code>{rcpt_mailer} {rcpt_host}</code> ".

## Valores de retorno

La función **smfi\_setsymlist** devuelve el valor `MI_FAILURE` en los siguientes casos. De lo contrario, la función devolverá `MI_SUCCESS`.

- No hay suficiente espacio libre para realizar una copia de la lista de macros.
- Las *macros* son NULL o vacías.
- La *stage* no es una etapa de protocolo válida.
- La lista de macros para una etapa se ha establecido anteriormente.

## Información relacionada

[xxfi\\_negotiate](#)

## Distintivos de depuración para sendmail

Hay un gran número de distintivos de depuración incorporados en el mandato **sendmail**.

Cada distintivo de depuración tiene un número y nivel, donde los niveles más altos imprimen más información. El convenio consiste en que los niveles de más de nueve imprimen tanta información que sólo se utilizan para depurar un parte determinada de código. Los distintivos de depuración se establecen utilizando el distintivo **-d** como se muestra en el ejemplo siguiente:

```
debug-flag:      -d debug-list
debug-list:      debug-flag[.debug-flag]* 
debug-flag:      debug-range[.debug-level]
debug-range:     integer|integer-integer
debug-level:    integer

-d12           Establecer distintivo 12 en el nivel 1
-d12.3         Establecer distintivo 12 en el nivel 3
```

-d3-17	Establecer distintivos 3 a 17 en el nivel 1
-d3-17.4	Establecer distintivos 3 a 17 en el nivel 4

Los distintivos de depuración disponibles son:

- | <b>Item</b>  | <b>Descripción</b>                                  |
|--------------|---|
| <b>-d0</b>   | Depuración general.                                 |
| <b>-d1</b>   | Mostrar información de envío.                       |
| <b>-d2</b>   | Finalizar con <i>finis()</i> .                      |
| <b>-d3</b>   | Imprimir el promedio de carga.                      |
| <b>-d4</b>   | Suficiente espacio de disco.                        |
| <b>-d5</b>   | Mostrar sucesos.                                    |
| <b>-d6</b>   | Mostrar correo anómalo.                             |
| <b>-d7</b>   | Nombre de archivo de cola.                          |
| <b>-d8</b>   | Resolución de nombres DNS.                          |
| <b>-d9</b>   | Rastrear consultas de RFC1413.                      |
| <b>-d9.1</b> | Convertir nombres de sistema principal en canónico. |
| <b>-d10</b>  | Mostrar entrega de destinatario.                    |
| <b>-d11</b>  | Rastrear entrega.                                   |
| <b>-d12</b>  | Mostrar correlación de sistema principal relativo.  |
| <b>-d13</b>  | Mostrar entrega.                                    |
| <b>-d14</b>  | Mostrar comas de campo de cabecera.                 |
| <b>-d15</b>  | Mostrar actividad de petición de obtención de red.  |
| <b>-d16</b>  | Conexiones de salida.                               |
| <b>-d17</b>  | Listar sistemas principales MX.                     |

**Nota:** Ahora hay casi 200 distintivos de depuración definidos en **sendmail**.

## Internet Message Access Protocol y Post Office Protocol

AIX proporciona dos implementaciones del servidor de protocolos de correo basados en Internet para acceder al correo de forma remota.

- **Post Office Protocol (POP o POP3DS)**
- **Internet Message Access Protocol (IMAP o IMAPDS)**

Cada tipo de servidor almacena los mensajes electrónicos y proporciona acceso a los mismos. Si se utilizan estos protocolos de acceso a correo en un servidor, se elimina la necesidad de que el sistema siempre deba estar activo y en ejecución para recibir correo.

El servidor **POP** o **POP3DS** proporciona un sistema de correo fuera de línea, en el que un cliente, utilizando software de cliente **POP** o **POP3DS**, puede acceder de forma remota a un servidor de correo para recuperar los mensajes de correo. El cliente puede descargar los mensajes de correo y suprimirlos del servidor de forma inmediata o descargar los mensajes y dejar que permanezcan en el servidor **POP** o **POP3DS**. Una vez el correo se ha descargado a la máquina cliente, todo el proceso del correo se realiza de forma local en la máquina del cliente. El servidor **POP** permite a los usuarios acceder al buzón de uno en uno. La versión **POP3DS** utiliza las bibliotecas OpenSSL, que requieren certificados de seguridad.

El servidor **IMAP** o **IMAPDS** proporciona un superconjunto de las funciones de **POP** pero tiene una interfaz distinta. El servidor **IMAP** o **IMAPDS** proporciona un servicio fuera de línea, un servicio en línea y un servicio desconectado. El protocolo está diseñado para permitir la manipulación de los buzones

remotos como si fueran locales. Por ejemplo, los clientes pueden realizar búsquedas y marcar mensajes con distintivos de estado como, por ejemplo, **suprimido** o **contestado**. Además, los mensajes pueden permanecer en la base de datos del servidor hasta que se eliminan de forma explícita. El servidor **IMAP** también permite el acceso interactivo simultáneo de varios clientes a las buzones de los usuarios. La versión **IMAPDS** utiliza las bibliotecas OpenSSL, que requieren certificados de seguridad.

Cada tipo de servidor se utiliza para acceder al correo exclusivamente. Estos servidores se basan en **SMTP (Simple Mail Transfer Protocol)** para el envío del correo.

Cada protocolo es un protocolo abierto, basado en los estándares descritos en los RFC. Los servidores **IMAP** se basan en RFC 2060 y 2061 y los servidores **POP** se basan en RFC 1939. Ambos están orientados a la conexión mediante zócalos TCP. El servidor **IMAP** está a la escucha en el puerto 143 y el servidor **IMAPDS** está a la escucha en el puerto 993. El servidor **POP** está a la escucha en el puerto 110 y el servidor **POP3DS** está a la escucha en el puerto 995. El daemon **inetd** gestiona todos los servidores.

**Requisito:** Para utilizar las versiones de OpenSSL, debe instalarse OpenSSL. OpenSSL está disponible en el CD *AIX Toolbox for Linux Applications*.

### Configuración de los servidores IMAP y POP

Utilice este procedimiento para configurar los servidores **IMAP** y **POP**.

Para realizar esta tarea, se requiere autorización root.

1. Descomente las entradas de configuración **imapd** o **imapds** y **pop3d** o **pop3ds** del archivo /etc/inetd.conf.

A continuación se proporcionan ejemplos de las entradas de configuración:

```
#imap2 stream tcp    nowait  root    /usr/sbin/imapd imapd
#pop3 stream tcp    nowait  root    /usr/sbin/pop3d pop3d
#imaps stream tcp    nowait  root    /usr/sbin/imapds imapds
#pop3s stream tcp    nowait  root    /usr/sbin/pop3ds pop3ds
```

2. Establezca los archivos de configuración para el servidor **imapds** en el archivo /etc/imapd.cf y para el servidor **pop3ds** en el archivo /etc/pop3d.cf.

De forma predeterminada, los protocolos de conformidad de conexión de seguridad menos seguros (Secure Sockets Layer versión 2 (SSLv2) y SSLv3) están habilitados para los servidores **imapds** y **pop3ds**. No obstante, puede inhabilitar SSLv2 y SSLv3, actualizando los archivos de configuración según se muestra en el ejemplo siguiente. También puede habilitar o inhabilitar cualquier cifrado, especificando la cadena de caracteres **SSL\_CIPHER\_LIST** en el archivo de configuración. Esta opción sobrescribe la serie de cifrados predeterminados codificados en las aplicaciones.

#### Archivo de configuración para el servidor **imapds** (/etc/imapd.cf):

```
=====
#
# Ejemplo de archivo de configuración del servidor IMAP
#
=====
#
# Quite la marca de comentario de la línea que se encuentra bajo
# Inhabilitar SSL v2 para el servidor imap.
#
#   Inhabilitar SSL V2    --> SSL_OP_NO_SSLv2      YES
#   Permitir SSL V2     --> SSL_OP_NO_SSLv2      NO
#
#
#SSL_OP_NO_SSLv2      SÍ <----- quite la marca de
# comentario de esta línea para inhabilitar sslv2
#
# Quite la marca de comentario de la línea que se encuentra bajo
# Inhabilitar SSL v3 para el servidor imap.
#
#   Inhabilitar SSL V3    --> SSL_OP_NO_SSLv3      YES
#   Permitir SSL V3     --> SSL_OP_NO_SSLv3      NO
#
#
#SSL_OP_NO_SSLv3      SÍ <----- quite la marca de
# comentario de esta línea para inhabilitar sslv3
=====
```

```

# Quite la marca de comentario de la linea que se encuentra más
# abajo para utilizar la lista de cifrado proporcionada
# para el servidor imap. La lógica del analizador espera la cadena
# de cifrado dentro de " ".
#
#
#SSL_CIPHER_LIST "ALL:!LOW" <--- quite la marca de comentario de
# esta linea para la serie de cifrados personalizada (habilitar/inhabilitado)
#=====

```

### Archivo de configuración para el servidor pop3ds (/etc/pop3d.cf):

```

#=====
#
# Ejemplo de archivo de configuración del servidor POP3
#
#=====
#
# Quite la marca de comentario de la linea que se encuentra bajo
# Inhabilitar SSL v2 para el servidor pop3d.
#
#   Inhabilitar SSL V2    --> SSL_OP_NO_SSLv2      YES
#   Permitir SSL V2     --> SSL_OP_NO_SSLv2      NO
#
#
#SSL_OP_NO_SSLv2      Sí <----- quite la marca de
# comentario de esta linea para inhabilitar sslv2
#=====
#
# Quite la marca de comentario de la linea que se encuentra bajo
# Inhabilitar SSL v3 para el servidor pop3d.
#
#   Inhabilitar SSL V3    --> SSL_OP_NO_SSLv3      YES
#   Permitir SSL V3     --> SSL_OP_NO_SSLv3      NO
#
#
#SSL_OP_NO_SSLv3      Sí <----- quite la marca de
# comentario de esta linea para inhabilitar sslv3
#=====
#
# Quite la marca de comentario de la linea que se encuentra más
# abajo para utilizar la lista de cifrado proporcionada
# para el servidor pop3d. La lógica del analizador espera la cadena
# de cifrado dentro de " ".
#
#
#SSL_CIPHER_LIST "ALL:!LOW" <--- quite la marca de comentario
# de esta linea para la serie de cifrados personalizada (habilitar/inhabilitado)
#=====

```

- Renueve el daemon **inetd** ejecutando el mandato siguiente:

```
refresh -s inetd
```

### Ejecución de pruebas de configuración

Ejecute unas cuentas pruebas para verificar que los servidores estén listos para funcionar.

- En primer lugar, verifique que los servidores estén a la escucha en sus puertos.

Para ello, escriba los mandatos siguientes en la solicitud de mandatos, pulsando la tecla Intro después de cada mandato:

```
netstat -a | grep imap
netstat -a | grep pop
```

A continuación se muestra la salida de los mandatos **netstat**:

tcp	0	0	.*.imap2	.*.*	LISTEN
tcp	0	0	.*.imaps	.*.*	LISTEN
tcp	0	0	.*.pop3	.*.*	LISTEN
tcp	0	0	.*.pop3s	.*.*	LISTEN

- Si no recibe una salida similar, vuelva a comprobar las entradas del archivo /etc/inetd.conf y ejecute de nuevo el mandato **refresh -s inetd**.
- Para probar la configuración del servidor imapd, utilice Telnet para acceder al servidor imap2, puerto 143 (para IMAPDS, Telnet puerto 993).

Cuando se conecte utilizando Telnet, obtendrá la solicitud de imapd. Entonces puede ejecutar los mandatos de IMAP Versión 4 tal como se define en RFC 1730. Para ejecutar un mandato, escriba un punto (.), seguido de un espacio, entonces una señal, un nombre de mandato y los parámetros que desee. La señal se utiliza para secuenciar el nombre del mandato. Por ejemplo:

```
. señal NombreMandato parámetros
```

Al conectar con el servidor imapd mediante Telnet, se ejecuta echo en las contraseñas.

En el ejemplo siguiente de Telnet, debe proporcionar su propia contraseña donde *contraseña\_ID* se indica en el mandato **login**.

**Consejo:** Para IMAPDS, el mandato y la salida varía ligeramente.

```
telnet e-xbelize 143
Intentando...
Conectado a e-xbelize.austin.ibm.com.
El carácter de escape es '^].
* OK servidor e-xbelize.austin.ibm.com IMAP4 preparado
. 1 login id contraseña_ID
. OK
. 2 examine /usr/spool/mail/root
* FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
* OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen \*)]
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 823888143]
. OK [READ-ONLY] Examen completado
. 3 logout
* BYE Servidor terminando conexión
. OK Fin de sesión completado
Conexión cerrada.
```

4. Para probar la configuración del servidor pop3d, utilice Telnet para acceder al puerto POP3, 110 (para POP3DS, Telnet puerto 995).

Cuando se conecte utilizando Telnet, obtendrá la solicitud de pop3d. Puede escribir los mandatos POP definidos en RFC 1725. Para ejecutar uno de los mandatos, escriba un punto (.), seguido de un espacio y entonces el nombre de un mandato. Por ejemplo:

```
. NombreMandato
```

Al conectar con el servidor pop3d mediante Telnet, se ejecuta echo en las contraseñas.

En el ejemplo siguiente de Telnet, debe proporcionar su propia contraseña donde *contraseña\_ID* se indica en el mandato **pass**.

**Consejo:** Para POP3DS, el mandato y la salida varía ligeramente.

```
telnet e-xbelize 110
Intentando...
Conectado a e-xbelize.austin.ibm.com.
El carácter de escape es '^].
+OK Servidor e-xbelize.austin.ibm.com POP3 preparado
user id
+OK El nombre es un buzón de correo válido
pass id_contraseña
+OK Eliminación de correo bloqueada y preparada
list
+OK Sigue el listado de exploración
.
stat
+OK 0 0
quit
+OK
Conexión cerrada.
```

#### Registro cronológico con el recurso SYSLOG

El software de servidor **IMAP** (e **IMAPDS**) y **POP** (y **POP3DS**) envía mensajes de registro cronológico al recurso **SYSLOG**.

1. Para configurar el sistema para el registro cronológico **IMAP** y **POP** mediante el recurso **SYSLOG**, debe ser el usuario root. Edite el archivo `/etc/syslog.conf` y añada una entrada para `*.debug` del modo siguiente:

```
*.debug /usr/adm/imapd.log
```

2. El archivo `usr/adm/imapd.log` debe existir antes de que el daemon **syslogd** lea el archivo de configuración `/etc/syslog.conf`. Para crear este archivo, escriba lo siguiente en un indicador de línea de mandatos y pulse Intro:

```
touch /usr/adm/imapd.log
```

3. Renueve el daemon **syslogd** para leer el archivo de configuración otra vez. Escriba lo siguiente en un indicador de la línea de mandatos y pulse Intro:

```
refresh -s syslogd
```

## Mandatos de gestión de correo

Aquí se resumen los mandatos de gestión de correo.

Item	Descripción
<b>bugfiler</b>	Almacena informes de errores en directorios de correo específicos.
<b>comsat</b>	Notifica a los usuarios que hay correo de entrada (daemon).
<b>mailq</b>	Imprime el contenido de la cola de correo.
<b>mailstats</b>	Visualiza estadísticas acerca del tráfico de correo.
<b>newaliases</b>	Crea una copia nueva de la base de datos de alias desde el archivo <code>/etc/mail/aliases</code> .
<b>rmail</b>	Maneja el correo remoto recibido mediante el mandato <b>uucp</b> de los Programas de utilidad básicos de red (BNU).
<b>sendbug</b>	Envía por correo un informe de depuración de sistema a una dirección específica.
<b>sendmail</b>	Direcciona el correo para la entrega local o de red.
<b>smdemon.cleanu</b>	Limpia la cola <b>sendmail</b> para el mantenimiento periódico.

## Archivos y directorios de correo

Los archivos y directorios de correo se pueden organizar por función.

Item	Descripción
<code>/usr/share/lib/Mail.rc</code>	Establece valores predeterminados de sistema local para todos los usuarios del programa de correo. Archivo de texto que puede modificar para establecer las características predeterminadas del mandato <b>mail</b> .
<code>\$HOME/.mailrc</code>	Permite al usuario cambiar los valores predeterminados de sistema local para el recurso de correo.
<code>\$HOME/mbox</code>	Almacena el correo procesado para el usuario individual.

<b>Item</b>	<b>Descripción</b>
/usr/bin/Mail,/usr/bin/mail o /usr/bin/mailx	Especifica tres nombres enlazados al mismo programa. El programa de correo (mail) es <i>una</i> de las interfaces de usuario al sistema de correo.
/var/spool/mail	Especifica el directorio de eliminación de correo predeterminado. De forma predeterminada, todo el correo se entrega al archivo /var/spool/mail/ <i>NombreUsuario</i> .
/usr/bin/bellmail	Realiza la entrega de correo local.
/usr/bin/rmail	Ejecuta la interfaz de correo remoto para BNU.
/var/spool/clientmqueue	Contiene el archivo de registro y los archivos temporales asociados con los mensajes de salida generados localmente en la cola de correo.
/var/spool/mqueue	Contiene el archivo de registro y los archivos temporales asociados con los mensajes en la cola de correo.

<b>Item</b>	<b>Descripción</b>
/usr/sbin/sendmail	Mando <b>sendmail</b> .
/usr/ucb/mailq	Enlaza a /usr/sbin/sendmail. La utilización de mailq equivale a la utilización del mandato /usr/sbin/sendmail -bp.
/usr/ucb/newaliases	Enlaza al archivo /usr/sbin/sendmail. La utilización de newaliases equivale a la utilización del mandato /usr/sbin/sendmail -bi.
/etc/netsvc.conf	Especifica el orden de determinados servicios de resolución de nombres.
/usr/sbin/mailstats	Formatea e imprime las estadísticas de <b>sendmail</b> tal como se encuentran en el archivo /etc/sendmail.st, si existe. El archivo /etc/sendmail.st es el valor predeterminado, pero puede especificar un archivo alternativo.
/etc/mail/aliases	Describe una versión de texto del archivo de alias para el mandato <b>sendmail</b> . Puede editar este archivo para crear, modificar o suprimir alias para el sistema.
/etc/aliasesDB	Describe un directorio que contiene los archivos de base de datos de alias, DB.dir y DB.pag, que se crean desde el archivo /etc/mail/aliases al ejecutar el mandato <b>sendmail -bi</b> .
/etc/mail/sendmail.cf	Contiene la información de configuración de <b>sendmail</b> en formato de texto. Edite el archivo para cambiar esta información.
/usr/lib/sm demon.cleanu	Especifica un archivo de shell que ejecuta la cola de correo y mantiene los archivos de registro de <b>sendmail</b> en el directorio /var/spool/mqueue.
/etc/mail/statistics	Recopila estadísticas acerca del tráfico de correo. Este archivo no aumenta de tamaño. Utilice el mandato /usr/sbin/mailstats para visualizar el contenido de este archivo. Suprima este archivo si no desea recopilar esta información.

Item	Descripción
/var/spool/clientmqueue	Describe un directorio que contiene los archivos temporales, que contiene el correo electrónico de salida generado localmente, en la cola de correo. Los archivos temporales incluyen, por ejemplo, los correos electrónicos del sistema.
/var/spool/mqueue	Describe un directorio que contiene los archivos temporales asociados con cada mensaje de la cola. El directorio puede contener el archivo de registro.
/var/spool/cron/crontabs	Describe un directorio que contiene archivos que el daemon <b>cron</b> lee para determinar qué trabajos se deben iniciar. El archivo root contiene una línea para iniciar el script de shell smdemon.cleanup.

## Mandatos de IMAP y POP

Para IMAP y POP se utilizan los mandatos de correo **imapd** y **pop3d**.

Item	Descripción
/usr/sbin/ <b>imapd</b>	Proceso de servidor IMAP (Internet Message Access Protocol).
/usr/sbin/ <b>pop3d</b>	Proceso servidor POP3 (Post Office Protocol Versión 3).

## Protocolo de control de transmisiones/Protocolo Internet (Transmission Control Protocol/Internet Protocol)

---

Cuando los sistemas se comunican entre sí, existen ciertas normas o *protocolos*, que les permiten transmitir y recibir datos de una forma ordenada. En todo el mundo, uno de los conjuntos de protocolos utilizados más habitualmente es **TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet)**. (Sin embargo, en gran parte de Europa se utiliza el protocolo **X.25**.) Algunas funciones comunes para utilizar **TCP/IP** son el correo electrónico, la transferencia de archivos de sistema a sistema y el inicio de sesión remoto.

El mandato de usuario **mail**, los mandatos de usuario de Manejo de mensajes (MH) y el mandato de servidor **sendmail** pueden utilizar **TCP/IP** para enviar y recibir correo entre sistemas y los Programas de utilidad básicos de red (BNU) pueden utilizar **TCP/IP** para enviar y recibir archivos y mandatos entre sistemas.

**TCP/IP** es un conjunto de protocolos que especifican estándares de comunicaciones entre sistemas y detallan los convenios para el direccionamiento y la interconexión de redes. Su uso en Internet está ampliamente extendido y, por consiguiente, es la herramienta preferida de centros de investigación, escuelas, universidades, organismos oficiales y empresas para comunicarse entre sí.

**TCP/IP** permite las comunicaciones entre varios sistemas (llamados sistemas principales) conectados en una red. A su vez, cada red puede estar conectada a otra para comunicarse con los sistemas principales de dicha red. Aunque existen muchos tipos de tecnologías de red, muchas de las cuales utilizan el transporte en modalidad continua y por conmutación de paquetes, **TCP/IP** ofrece una ventaja importante: la independencia de hardware.

Dado que los protocolos de Internet definen la unidad de transmisión y especifican cómo enviarla, **TCP/IP** puede ocultar los detalles del hardware de red, permitiendo que muchos tipos de tecnologías de red se conecten e intercambien información. Las direcciones de Internet hacen posible que todas las máquinas de la red se comuniquen entre sí. **TCP/IP** también proporciona estándares para muchos de los servicios de comunicaciones que los usuarios necesitan.

**TCP/IP** proporciona recursos que convierten el sistema en un sistema principal de Internet, que se puede conectar a una red y comunicar con otros sistemas principales de Internet. **TCP/IP** incluye mandatos y recursos que permiten:

- Transferir archivos entre sistemas

- Iniciar sesiones en sistemas remotos
- Ejecutar mandatos en sistemas remotos
- Imprimir archivos en sistemas remotos
- Enviar correo electrónico a usuarios remotos
- Conversar de forma interactiva con usuarios remotos
- Gestionar una red

**Nota:** **TCP/IP** proporciona la posibilidad de gestión de red básica. El **SNMP (Protocolo simple de gestión de red)** proporciona más mandatos y funciones de gestión de red.

## Terminología de TCP/IP

Puede que le resulte útil familiarizarse con los siguientes términos de Internet tal como se utilizan en relación con TCP/IP.

Item	Descripción
<b>cliente</b>	Sistema o proceso que accede a los datos, servicios o recursos de otro sistema o proceso de la red.
<b>sistema principal</b>	Sistema conectado a una red Internet, y que puede comunicarse con otros sistemas principales de Internet. El <i>sistema principal local</i> de un usuario individual es el sistema en el que trabaja el usuario. Un <i>sistema principal externo</i> es cualquier otro nombre de sistema principal de la red. Desde el punto de vista de la red de comunicaciones, tanto el origen como el destino de los paquetes son sistemas principales. Un sistema principal puede ser un cliente, un servidor, o ambas cosas. En una red Internet, el sistema principal está identificado mediante su nombre y dirección de Internet.
<b>red</b>	Combinación de dos o más sistemas principales y los enlaces de conexión entre dichos sistemas. Una <i>red física</i> es el hardware que configura la red. Una <i>red lógica</i> es la base abstracta que subyace en toda una red física (o varias), o en una parte. La red Internet es un ejemplo de red lógica. El programa de interfaz maneja la conversión de operaciones de la red lógica en operaciones de la red física.
<b>paquete</b>	Bloque de datos y de información de control que conforman una transacción entre un sistema principal y su red. Los paquetes son el medio de intercambio que utilizan los procesos para enviar y recibir datos a través de las redes Internet. Un paquete se envía desde un <i>origen</i> a un <i>destino</i> .
<b>puerto</b>	Punto de conexión lógico de un proceso. Los datos se transmiten entre los procesos a través de puertos (o <i>sockets</i> ). Cada puerto proporciona colas para el envío y la recepción de datos. En una red de programas de interfaz, cada puerto dispone de un <i>número de puerto</i> de Internet basado en el uso del puerto. Un puerto determinado se identifica mediante una <i>dirección de socket</i> , que es la combinación de un número de puerto y una dirección de sistema principal de Internet.
<b>proceso</b>	Programa en ejecución. Un proceso es el elemento activo de un sistema. Los terminales, archivos y demás dispositivos de E/S se comunican entre sí a través de procesos. De este modo, las comunicaciones de red son <i>comunicaciones entre procesos</i> .
<b>protocolo</b>	Conjunto de normas para el manejo de las comunicaciones a nivel físico o lógico. Los protocolos suelen utilizar otros protocolos para ofrecer determinados servicios. Por ejemplo, un <i>protocolo a nivel de conexión</i> utiliza un <i>protocolo a nivel de transporte</i> para transferir paquetes que mantienen una conexión entre dos sistemas principales.
<b>servidor</b>	Sistema o proceso que facilita datos, servicios o recursos a los que pueden acceder otros sistemas o procesos de la red.

## Planificación de la red TCP/IP

Puesto que **TCP/IP** es una herramienta de gestión de redes tan flexible, puede personalizarlo para que se ajuste a las necesidades específicas de la organización. Tenga en cuenta los puntos principales de este

tema al planificar la red. Los detalles de estos puntos se describen en otros temas. Esta lista sólo está destinada a presentarle estos puntos.

1. Decida qué tipo de hardware de red desea utilizar: Red en anillo, Ethernet Versión 2, IEEE 802.3, FFDI (Fiber Distributed Data Interface), SOC (Serial Optical Channel) o SLIP (Serial Line Interface Protocol).
2. Planifique el diseño físico de la red.

Considere qué funciones atenderá cada máquina de sistema principal. Por ejemplo, debe decidir qué máquina o máquinas servirán de pasarelas antes de cablear la red.

3. Decida si se ajusta mejor a sus necesidades una organización de red *plana* o de red *jerárquica*.

Si la red es bastante pequeña, de un solo sitio, y consta de una red física, probablemente se ajustará mejor a sus necesidades una red plana. Si la red es muy grande o compleja con varios sitios o varias redes físicas, es posible que una red jerárquica sea una organización de red más eficiente.

4. Si la red se va a conectar a otras redes, debe planificar cómo se deben preparar y configurar las pasarelas.

Las cuestiones a tener en cuenta son las siguientes:

- a. Decida qué máquina o máquinas servirán de pasarelas.
  - b. Decida si necesita utilizar el direccionamiento estático o dinámico o una combinación de ambos. Si elige el direccionamiento dinámico, decida qué daemons de direccionamiento utilizará cada pasarela teniendo en cuenta los tipos de protocolos de comunicaciones a los que necesita dar soporte.
5. Decida un esquema de direccionamiento.

Si la red no va a formar parte de un sistema de comunicación entre redes, elija el esquema de direccionamiento que mejor se ajuste a sus necesidades. Si desea que la red esté conectada a un sistema de comunicación entre redes mayor, por ejemplo Internet, tendrá que obtener un conjunto de direcciones oficial del proveedor de servicios de internet (ISP).

6. Determine si el subsistema necesita dividirse en subredes. Si es así, decida cómo asignará máscaras de subred.
7. Determine un esquema de denominación. Cada máquina de la red necesita el nombre de sistema principal exclusivo.
8. Decida si la red necesita un servidor de nombres para la resolución de nombres o si la utilización del archivo /etc/hosts será suficiente.

Si elige utilizar servidores de nombres, tenga en cuenta el tipo de servidores de nombres que necesita y cuántos necesita para atender la red de forma eficiente.

9. Decida los tipos de servicios que desea que la red proporcione a los usuarios remotos; por ejemplo servicios de correo, servicios de impresión, compartimiento de archivos, inicio de sesión remoto, ejecución de mandatos remota y otros.

## Instalación de TCP/IP

El software necesario para configurar la red TCP/IP se instala durante el proceso de instalación del sistema operativo base. No es necesario instalar ningún paquete específico adicional para la red TCP/IP.

Para obtener información sobre cómo instalar el **sistema operativo base**, consulte [Instalación y migración](#).

## Configuración de TCP/IP

Cuando haya instalado el sistema operativo base de AIX en el sistema, estará preparado para empezar a configurar la red TCP/IP.

Muchas tareas de configuración de **TCP/IP** se pueden realizar de más de una forma:

- Utilizar System Management Interface Tool (SMIT)
- Editar un formato de archivo
- Emitir un mandato en el indicador de shell.

Por ejemplo, el script de shell `rc.net` realiza la configuración de sistema principal mínima necesaria para **TCP/IP** durante el proceso de arranque de sistema (el programa gestor de configuración ejecuta el script `rc.net` durante la segunda fase de arranque). Al utilizar SMIT para realizar la configuración de sistema principal, el archivo `rc.net` se configura de forma automática.

De forma alternativa, puede configurar el archivo `/etc/rc.bsdnet` utilizando un editor de texto estándar. Con este método, puede especificar los mandatos de configuración **TCP/IP** tradicionales de UNIX, como **ifconfig**, **hostname** y **route**. Si utiliza el método de edición de archivo, debe entrar la vía de acceso rápida `smit configtcp` y, a continuación, seleccionar **Configuración rc estilo BSD**. Consulte [List of TCP/IP Programming References](#) en la publicación *Communications Programming Concepts* para obtener información sobre los archivos y los formatos de archivo **TCP/IP**.

Hay unas cuantas tareas, por ejemplo configurar un servidor de nombres, que no se pueden realizar utilizando SMIT.

Utilice este procedimiento como guía para configurar la red. Asegúrese de haber leído y comprendido el material apropiado.

Antes de empezar este procedimiento, asegúrese de que se cumplan los siguientes requisitos previos:

1. El hardware de red está instalado y cableado. Para obtener más información sobre cómo instalar y cablear el hardware, consulte [“Tarjetas adaptadoras de red de área local TCP/IP” en la página 170](#).
2. El software **TCP/IP** está instalado. Para obtener más información sobre cómo instalar el software **TCP/IP**, consulte la publicación *Installation and migration*.

Después de arrancar la red y de que ésta se ejecute correctamente, es posible que encuentre útil consultar esta lista de comprobación para realizar la depuración.

Para configurar la red **TCP/IP**, utilice los pasos siguientes:

1. Lea [“Protocolos TCP/IP” en la página 128](#) para conocer la organización básica de **TCP/IP**.

Debe comprender:

- la naturaleza de capas de **TCP/IP** (es decir, diferentes protocolos residen en capas diferentes)
- cómo fluyen los datos a través de las capas

2. Configure mínimamente cada máquina de sistema principal de la red.

Esto significa añadir un adaptador de red, asignar una dirección IP y asignar un nombre de sistema principal a cada sistema principal, así como definir una ruta predeterminada a la red. Para obtener información básica sobre estas tareas, consulte [“Interfaces de red TCP/IP” en la página 173](#), [“Direccionamiento TCP/IP” en la página 179](#) y [“Denominación de los sistemas principales de la red” en la página 186](#).

**Nota:** Cada máquina de la red necesita esta configuración básica tanto si va a ser un sistema principal de usuario final, un servidor de archivos, una pasarela o un servidor de nombres.

3. Configure e inicie el daemon **inetd** en cada máquina de sistema principal de la red. Lea el apartado [“Daemons TCP/IP” en la página 431](#) y, a continuación, siga las instrucciones del apartado [“Configuración del daemon inetd” en la página 431](#).

4. Configure cada máquina de sistema principal para realizar la resolución de nombres local o para utilizar un servidor de nombres.

Si está configurando una red de nombres de dominio jerárquica, configure como mínimo un sistema principal para que funcione como servidor de nombres. Lea y siga las instrucciones del apartado [“Resolución de nombres” en la página 189](#).

5. Si la red se va a comunicar con redes remotas, configure como mínimo un sistema principal para que funcione como pasarela.

La pasarela puede utilizar rutas estáticas o un daemon de direccionamiento para realizar el direccionamiento entre redes. Lea y siga las instrucciones del apartado [“Direccionamiento TCP/IP” en la página 433](#).

6. Decida qué servicios utilizará cada máquina de sistema principal de la red.

De forma predeterminada, están disponibles todos los servicios. Siga las instrucciones del apartado “[Servicios de red de cliente](#)” en la página 432 si desea que un servicio determinado no esté disponible.

7. Decida qué sistemas principales de la red serán servidores y qué servicios proporcionará un servidor determinado.  
Siga las instrucciones del apartado “[Servicios de red de servidor](#)” en la página 433 para iniciar los daemons de servidor que desea ejecutar.
8. Configure los servidores de impresión remotos que va a necesitar.  
Consulte el apartado [Printing administration](#) para obtener más información.
9. **Opcional:** Si lo desea, configure un sistema principal para utilizarlo o para que sirva de servidor horario maestro para la red.  
Para obtener más información, consulte el daemon [timed](#).

### Configuración de sistema principal

Cada máquina de sistema principal de la red se debe configurar para que funcione de acuerdo con las necesidades de los usuarios finales y de la red en conjunto.

Para cada sistema principal de la red, debe configurar la interfaz de red, establecer la dirección de Internet y establecer el nombre de sistema principal. También debe configurar rutas estáticas a pasarelas o a otros sistemas principales, especificar los daemons que se deben iniciar de forma predeterminada y configurar el archivo `/etc/hosts` para la resolución de nombres (o configurar el sistema principal para que utilice un servidor de nombres para la resolución de nombres).

### Configuración de sistema principal como servidor

Si la máquina de sistema principal va a tener una función específica como servir de pasarela, de servidor de archivos o de servidor de nombres, debe realizar las tareas de configuración necesarias después de que se haya completado la configuración básica.

Por ejemplo, si la red está organizada jerárquicamente y desea utilizar el protocolo de **Nombres de dominio** para resolver nombres en direcciones Internet, necesitará configurar como mínimo un servidor de nombres para proporcionar esta función para la red.

Recuerde, un sistema principal de servidor no tiene que ser una máquina dedicada, también se puede utilizar para otras tareas. Si la función de servidor de nombres para la red es claramente pequeña, la máquina también se puede utilizar como estación de trabajo o como servidor de archivos para la red.

**Nota:** Si el sistema tiene instalado NIS, estos servicios también puede proporcionar resolución de nombres.

### Configuración de pasarela

Si la red va a comunicarse con otras redes, necesitará configurar como mínimo un sistema principal pasarela.

Debe tener en cuenta qué protocolos de comunicaciones desea soportar y, a continuación, utilizar cualquier daemon de direccionamiento (el daemon **routed** o **gated**) que soporte esos protocolos.

### Mandatos de configuración y gestión de TCP/IP

Puede utilizar diversos mandatos para configurar y gestionar una red **TCP/IP**. Estos mandatos se describen en esta tabla.

Item	Descripción
<b>arp</b>	Visualiza o cambia la dirección de Internet en tablas de conversión de direcciones de hardware utilizadas por el protocolo de <b>resolución de direcciones</b> .
<b>finger</b>	Devuelve información sobre los usuarios de un sistema principal especificado.

Item	Descripción
<b>host</b>	Muestra la dirección de Internet de un sistema principal especificado o el nombre de nombre de sistema principal de una dirección de Internet especificada.
<b>hostname</b>	Muestra o establece el nombre y la dirección de Internet del sistema principal local.
<b>ifconfig</b>	Configura interfaces de red y sus características.
<b>netstat</b>	Muestra direcciones locales y externas, tablas de direccionamiento, estadísticas de hardware y un resumen de paquetes transferidos.
<b>no</b>	Establece o muestra opciones de kernel de red actuales.
<b>ping</b>	Determina si un sistema principal es alcanzable.
<b>route</b>	Permite manipular manualmente las tablas de direccionamiento.
<b>ruptime</b>	Muestra información de estado sobre los sistemas principales que están conectados a redes físicas locales y están ejecutando el servidor <b>rwhod</b> .
<b>rwho</b>	Muestra información de estado para los usuarios sobre los sistemas principales que están conectados a redes físicas locales y están ejecutando el servidor <b>rwhod</b> .
<b>setclock</b>	Lee el servicio el tiempo de red y establece la hora y fecha del sistema principal local como corresponde.
<b>timedc</b>	Devuelve información acerca del daemon <b>timed</b> .
<b>trpt</b>	Informa sobre el rastreo de protocolo en sockets TCP.
<b>whois</b>	Proporciona el servicio de directorio de nombres e Internet.

## Autentificación y los rcmds seguros

Estos mandatos se han mejorado para proporcionar métodos de autentificación adicionales a los utilizados hoy en día.

Los rcmds seguros son **rlogin**, **rcp**, **rsh**, **telnet** y **ftp**. De forma predeterminada, estos mandatos utilizan el método de autenticación *Standard AIX*. Los dos métodos adicionales son Kerberos V.5 y Kerberos V.4.

Al utilizar el método de autentificación Kerberos V.5, el cliente obtiene el ticket de Kerberos V.5 del servidor de seguridad DCE o del servidor Native Kerberos. El ticket es una parte de las credenciales DCE o Native actuales del usuario cifradas para el servidor **TCP/IP** con el que desean conectarse. El daemon del servidor **TCP/IP** descifra el ticket. Esto permite al servidor **TCP/IP** identificar al usuario de forma absoluta. Si el principal DCE o Native descrito en el ticket tiene permiso para acceder a la cuenta del usuario del sistema operativo, la conexión prosigue.

**Nota:** A partir de DCE versión 2.2, el servidor de seguridad DCE puede devolver tickets de Kerberos V.5. El rcmds seguro en el sistema operativo AIX utiliza la biblioteca Kerberos V.5 y la biblioteca GSSAPI proporcionada por NAS (Network Authentication Service) versión 1.3.

Además de autenticar el cliente, Kerberos V.5 reenvía las credenciales del usuario actual al servidor **TCP/IP**. Si dichas credenciales están marcadas como que se pueden remitir, el cliente las envía al servidor como TGT (Ticket Granting Ticket) de Kerberos. En el lado del servidor **TCP/IP**, si uno se comunica con un servidor de seguridad DCE, el daemon actualiza el TGT para convertirlo en las credenciales DCE completas utilizando el mandato **k5dcecreds**.

El mandato **ftp** utiliza un método de autentificación distinto al de los restantes mandatos. Utiliza el mecanismo de seguridad GSSAPI para pasar la autentificación entre el mandato **ftp** y el daemon **ftpd**.

Mediante la utilización de los submandatos **clear/safe/private**, el cliente **ftp** soporta el cifrado de datos.

Entre clientes y servidores del sistema operativo, se ha mejorado **ftp** para permitir transferencias de múltiples bytes para las conexiones de datos cifrados. Los estándares sólo definen transferencias de un solo byte para las conexiones de datos cifrados. Cuando esté conectado a máquinas de otras empresas y esté utilizando el cifrado de datos, **ftp** seguirá el límite de transferencia de un solo byte.

**Nota:** Los mandatos de seguridad rcmds **rlogin**, **rsh** y **telnet**, junto con los métodos de autenticación **klogin** y **kshell** de Kerberos V.5, permiten tres intentos antes de que la conexión al host remoto se cierre.

### **Configuración del sistema para los rcmds seguros**

Para todos los rcmds seguros, existe un mecanismo de configuración a nivel de sistema para determinar qué métodos de autenticación están permitidos para cada sistema. La configuración controla las conexiones de entrada y de salida.

La configuración de autenticación consta de una biblioteca, `libauthm.a`, y de dos mandatos, **lsauthent** y **chauthent**, que proporcionan acceso a la línea de mandatos a las dos rutinas de la biblioteca: `get_auth_methods` y `set_auth_methods`.

El sistema soporta tres métodos de autenticación distintos: Kerberos V.5, Kerberos V.4 y *Standard AIX*. El método de autenticación define el método que se utiliza para autenticar un usuario en una red.

- Kerberos V.5 es el método más común y constituye la base de Distributed Computing Environment (DCE). El sistema operativo actualiza los tickets de entrada de Kerberos V.5 a credenciales DCE completas o utiliza tickets de entrada de Native Kerberos V.5.
- Sólo utilizan Kerberos V.4 dos de los rcmds seguros: **rsh** y **rcp**. Se proporciona para dar soporte a la compatibilidad con una versión anterior en sistemas SP y es funcional sólo en uno. Un ticket de Kerberos V.4 no se actualiza para credenciales DCE.
- El término, *Método de autenticación estándar de AIX*, hace referencia al método de autenticación utilizado por el sistema operativo AIX.

Cuando se configura más de un método de autenticación, se produce una implantación replegada. Si el primer método no se puede conectar, el cliente intentará autenticarse utilizando el siguiente método de autenticación configurado.

Los métodos de autenticación se pueden configurar en cualquier orden. La única excepción es que *Standard AIX* debe ser el método de autenticación final configurado porque no hay ninguna opción de repliegue de ella. Si *Standard AIX* no es un método de autenticación configurado, la autenticación de contraseña no se intentará, y se rechazará cualquier intento de conexión que utilice este método.

Es posible configurar el sistema sin ningún método de autenticación. En este caso, el sistema rechaza todas las conexiones desde y hasta cualquier terminal que utiliza rcmds seguro. Además, puesto que Kerberos V.4 sólo se soporta con los mandatos **rsh** y **rcp**, un sistema que está configurado para utilizar sólo Kerberos V.4 no permite conexiones que utilizan **telnet**, **ftp** o **rlogin**.

### **Información relacionada**

[subrutina get\\_auth\\_method](#)

[subrutina set\\_auth\\_method](#)

[lsauthent, mandato](#)

[chauthent, mandato](#)

### **Validación de usuario de Kerberos V.5 para los rcmds seguros**

Cuando se utiliza el método de autenticación de Kerberos V.5, el cliente de **TCP/IP** obtiene un ticket de servicio cifrado para el servidor **TCP/IP**. Cuando el servidor descifra el ticket, tiene un método seguro para identificar al usuario (por el principal DCE o Native).

No obstante, sigue teniendo que determinar si este principal DCE o Native tiene permiso para acceder a la cuenta local. La correlación del principal DCE o Native con la cuenta del sistema operativo local se maneja mediante una biblioteca compartida, `libvaliduser.a`, que tiene una única subrutina, `kvalid_user`. Si

se prefiere un método de correlación distinto, el administrador del sistema operativo debe proporcionar una alternativa a la biblioteca `libvaliduser.a`.

### Configuración de DCE para los rcmds seguros

Para utilizar los rcmds seguros, deben existir dos principales DCE para cada interfaz de red a la que se puedan conectar.

Se trata de:

```
host/NombreInterfazCompleto
ftp/NombreInterfazCompleto
```

donde *NombreInterfazCompleto* es el nombre de interfaz y el nombre de dominio para el *NombreSistpral.NombreDominio* primario.

### Configuración nativa para los rcmds seguros

Para utilizar los rcmds seguros, deben existir dos principios para cada interfaz de red a la que se pueden conectar.

Se trata de:

```
host/
NombreInterfazCompleto@NombreRegión
ftp/NombreInterfazCompleto@NombreRegión
```

donde *NombreInterfazCompleto* es el nombre de interfaz y el nombre de dominio para el *NombreSistpral.NombreDominio* principal. *NombreRegión* es el nombre de la región Native Kerberos V.

## Personalización de TCP/IP

Para personalizar **TCP/IP**, cree un archivo `.netrc`.

El archivo `.netrc` especifica información de inicio de sesión automática para los mandatos **ftp** y **rexec**. También puede escribir macros **ftp** nuevas, que se definen en el archivo `$HOME/.netrc`. Para personalizar secuencias o funciones de teclas, cree y edite el archivo `$HOME/.3270keys`. Además, el archivo `.k5login` especifica a qué principales de DCE de qué células se les permite el acceso a la cuenta del usuario.

### Creación del archivo `.netrc`

Estos pasos describen cómo crear y editar el archivo `$HOME/.netrc`:

1. Debe tener una copia del archivo `/usr/samples/tcpip/netrc`.
2. El mandato **securetcpip** no debe estar ejecutándose en el sistema.

Para crear el archivo `.netrc`:

1. Copie el archivo `/usr/samples/tcpip/netrc` en el directorio `$HOME` escribiendo el mandato siguiente:

```
cp /usr/samples/tcpip/netrc $HOME
```

2. Edite el archivo `$HOME/netrc` para proporcionar las variables *NombreSistPral*, *NombreInicioSesión* y *Contraseña* apropiadas. Por ejemplo:

```
machine host1.austin.century.com login fred password bluebonnet
```

3. Para establecer los permisos en el archivo `$HOME/netrc` en 600 utilizando el mandato **chmod** en el indicador de línea de mandatos (\$), escriba:

```
chmod 600 $HOME/netrc
```

4. Cambie el nombre del archivo `$HOME/netrc` por `$HOME/.netrc`. El punto (.) inicial hace que el archivo se oculte.

```
mv $HOME/.netrc $HOME/.netrc
```

El archivo \$HOME/.netrc puede contener múltiples definiciones de inicio de sesión y hasta 16 macros por definición de inicio de sesión.

### Escritura de macros ftp

Estos pasos siguientes describen cómo crear una macro **ftp**.

Debe haber creado el archivo \$HOME/.netrc.

Para escribir una macro **ftp**:

1. Edite el archivo \$HOME/.netrc para incluir las instrucciones siguientes:

```
macdef init  
put planificación
```

Asegúrese de insertar una línea en blanco al final de la macro **ftp**. La línea en blanco termina la macro **ftp**. En el ejemplo anterior, el submandato **macdef** define la macro del submandato **init**. La línea siguiente es el mandato que la macro especifica, en este caso **put planificación**, donde **planificación** es el nombre de un archivo.

2. Después de crear la macro **ftp**, escriba lo siguiente en el indicador de línea de mandatos:

```
ftp nombresistpral
```

Donde *nombresistpral* es el nombre del sistema principal al que se está conectando.

**ftp** busca en el archivo \$HOME/.netrc una definición de inicio de sesión que coincida con el nombre de sistema principal y utiliza esa definición de inicio de sesión para conectarle.

3. Despues de iniciar la sesión, escriba lo siguiente en el indicador de la línea de mandatos:

```
ftp init
```

En este ejemplo, **ftp** explora la macro llamada **init** y ejecuta el mandato o mandatos que especifica la macro.

Una macro **ftp** está asociada con la entrada de inicio de sesión inmediatamente anterior a la misma. Las macros **ftp** no son globales en el archivo \$HOME/.netrc. La macro **init** se ejecutará automáticamente tras el inicio de sesión. Se pueden ejecutar otras macros desde el indicador de **ftp** (**ftp>**) escribiendo lo siguiente:

```
$getit
```

En este ejemplo, \$ ejecuta la macro **ftp getit**.

### Modificación de la asignación de un grupo de teclas

Al personalizar **TCP/IP**, puede utilizar este procedimiento para cambiar las secuencias y las funciones de tecla.

1. Debe tener conocimientos suficientes sobre el uso del editor **vi**.
2. El editor vi debe estar instalado en el sistema.

Los pasos siguientes describen cómo crear y editar el archivo \$HOME/.3270keys para personalizar las funciones o secuencias de teclas:

1. Copie el archivo /etc/3270.keys en el directorio \$HOME y cámbiele el nombre por .3270keys utilizando el mandato siguiente:

```
cp /etc/3270.keys $HOME/.3270keys
```

2. Cambie las sentencias de enlace del archivo \$HOME/.3270keys para modificar la asignación de un grupo de teclas efectuando los pasos siguientes:

- a) Inicie el editor vi en un archivo nuevo y entre en la modalidad de inserción.

b) Pulse la secuencia de teclas Control-V y, a continuación, la tecla que desea correlacionar.

Se visualizará un valor para la tecla pulsada.

c) Coloque el valor visualizado en la línea apropiada de la columna Sequence del archivo \$HOME/.3270keys.

Por ejemplo, después de haber invocado el editor vi y de haber entrado en la modalidad de inserción, pulse Control-V y, a continuación, Alt-Insert. Esta operación visualizará [ [141q. El primer símbolo [ se sustituye por \e en la columna Sequence, de forma que la línea configurada tiene el aspecto siguiente:

```
3270 Function Sequence Key  
bind pa1      "\e[141q" #a_insert
```

#### **.k5login, archivo**

El archivo .k5login se utiliza cuando se emplea la autentificación Kerberos V.5 para los rcmds de seguridad. Este archivo especifica qué principales DCE de qué células tienen permitido acceder al perfil del usuario.

El archivo se encuentra en \$HOME/.k5login. Debe pertenecer al usuario local y el propietario debe tener el permiso read (lectura) sobre este archivo. El valor de permiso mínimo para este archivo es 400.

El archivo .k5login contiene una lista de los pares de principal DCE/célula que tienen permitido el acceso al perfil. Los pares de principal/célula se conservan en formato Kerberos (en oposición al formato DCE). Por ejemplo, si el archivo contiene

```
UsuarioA@Célula1
```

el principal DCE UsuarioA de la célula DCE Célula1 puede acceder al perfil.

Si el principal DCE es igual que el nombre de perfil del usuario y si no hay ningún archivo \$HOME/.k5login para el perfil del usuario, el principal DCE obtendrá acceso al perfil (a condición que esté configurada la autentificación de Kerberos V.5).

Para obtener más información sobre la autentificación Kerberos V.5, consulte el apartado “[Autentificación y los rcmds seguros](#)” en la página 112.

## **Métodos para comunicarse con otros sistemas y usuarios**

Existen varios métodos para comunicarse con otros sistemas y usuarios. Dos de estos métodos se exponen a continuación. El primero consiste en conectar un sistema principal local con un sistema principal remoto. El segundo método se basa en la conversación con un usuario remoto.

### **Conexiones de sistema principal local a un sistema principal remoto**

Estos mandatos de conexión de sistema principal **TCP/IP** son para el inicio de sesión remoto y la ejecución de mandatos.

Existen varias razones por las que puede necesitar acceder a un sistema que no sea el suyo. Por ejemplo, quizás el administrador del sistema necesite reasignar los permisos para un determinado archivo con el que ha estado trabajando o bien precise el acceso a un archivo personal de la estación de trabajo de otra persona. Incluso puede conectarse a su propio sistema desde la estación de sistema de cualquier otra persona. Las funciones de inicio de sesión remoto, por ejemplo los mandatos **rlogin**, **rexec** y **telnet**, permiten al sistema principal local funcionar como un sistema principal de terminal de entrada/salida. Las pulsaciones de tecla se envían al sistema principal remoto y los resultados se visualizan en el monitor local. Al finalizar la sesión remota, todas las funciones vuelven al sistema principal local.

**TCP/IP** contiene los siguientes mandatos para el inicio de sesión remoto y la ejecución de mandatos:

Item	Descripción
<b>rexec</b>	<p>El mandato <b>rexec</b> hace que sea posible ejecutar mandatos de forma interactiva en diferentes sistemas principales externos cuando el usuario inicia la sesión en un sistema principal remoto con el mandato <b>rlogin</b>. Si su red precisa seguridad adicional, el gestor del sistema se encarga de inhabilitar este mandato. Al emitir el mandato <b>rexec</b>, el sistema principal local busca en el archivo <code>\$HOME/.netrc</code> del sistema principal remoto el nombre de usuario y una contraseña del sistema principal local. Si los encuentra, el mandato cuya ejecución ha solicitado que se realice en el sistema principal local se ejecutará. De lo contrario, se le solicitará que proporcione un nombre de inicio de sesión y una contraseña para dar vía libre a la petición.</p>
<b>rlogin</b>	<p>El mandato <b>rlogin</b> permite iniciar la sesión en sistemas principales externos similares. A diferencia de <b>telnet</b>, que se puede utilizar con diferentes sistemas principales remotos, sólo se puede utilizar el mandato <b>rlogin</b> en sistemas principales UNIX. Si su red precisa seguridad adicional, el gestor del sistema se encarga de inhabilitar este mandato.</p> <p>El mandato <b>rlogin</b> es similar al mandato <b>telnet</b> en que ambos permiten que un sistema principal local se conecte a un sistema principal remoto. La única diferencia es que el mandato <b>rlogin</b> se considera un mandato no autorizado y puede inhabilitarse si el sistema necesita seguridad adicional.</p> <p>El mandato <b>rlogin</b> no es un mandato autorizado porque el archivo <code>\$HOME/.rhosts</code>, que es propiedad del usuario local, y el archivo <code>/etc/hosts.equiv</code>, que es propiedad del gestor de sistemas, mantienen un listado de los sistemas principales remotos que tienen acceso a sistema principal local. Por consiguiente, si deja el terminal encendido mientras está desatendido, un usuario no autorizado podría examinar los nombres y contraseñas contenidos en estos archivos o, aún peor, podría dañar de algún modo un sistema principal remoto. Lo ideal sería solicitar a los usuarios remotos a escribir una contraseña después de emitir el mandato <b>rlogin</b>, pero es bastante posible pasar por alto esta función recomendada.</p> <p>Si ni el archivo <code>\$HOME/.rhosts</code> ni el archivo <code>/etc/hosts.equiv</code> contiene el nombre de un sistema principal remoto que está intentando iniciar la sesión, el sistema principal local solicita una contraseña. En primer lugar, se comprueba el archivo de contraseña remoto para verificar la contraseña especificada y, si no es correcta, vuelve a aparecer el indicador de inicio de sesión. Si se pulsa el carácter de tilde y un punto (~.) en el indicador de inicio de sesión, finalizará el intento de inicio de sesión remota.</p> <p>El mandato <b>rlogin</b> también se puede configurar para utilizar Kerberos V.5 a fin de autenticar al usuario. Esta opción permite identificar al usuario sin utilizar ningún archivo <code>\$HOME/.rhosts</code> o sin pasar la contraseña por la red. Para obtener más información sobre este uso del mandato <b>rlogin</b>, consulte el apartado <a href="#">“Autentificación y los rcmds seguros”</a> en la página 112.</p>

<b>Item</b>	<b>Descripción</b>
<b>rsh y remsh</b>	<p>Los mandatos <b>rsh</b> y <b>remsh</b> hacen que sea posible ejecutar mandatos en sistemas principales externos similares. El sistema principal remoto debe realizar toda la entrada necesaria. El gestor de sistema inhabilita los mandatos <b>rsh</b> y <b>remsh</b> si se necesita seguridad adicional para la red.</p> <p>El mandato <b>rsh</b> se puede utilizar de dos formas:</p> <ul style="list-style-type: none"> <li>• Para ejecutar un solo mandato en un sistema principal remoto cuando se especifica un nombre de mandato</li> <li>• Para ejecutar el mandato <b>rlogin</b> cuando no se especifica ningún nombre de mandato</li> </ul> <p>Cuando se emite el mandato <b>rsh</b>, el sistema principal local busca en el archivo <code>/etc/hosts.equiv</code> del sistema principal remoto el permiso para iniciar la sesión. Si la operación no es satisfactoria, se busca en el archivo <code>\$HOME/.rhosts</code>. Ambos archivos contienen una lista de los sistemas principales remotos con permiso de inicio de sesión. Se deberá solicitar a los usuarios remotos que escriban una contraseña después de emitir el mandato <b>rsh</b>.</p> <p>También es posible eliminar la necesidad de emitir el mandato <b>rlogin</b>. El mandato <b>rsh</b> permite la ejecución de mandatos en un sistema principal remoto, pero no proporciona un medio para ignorar el requisito de contraseña. Si se necesita una contraseña para acceder a un sistema principal remoto, se necesita también una contraseña para utilizar el mandato <b>rsh</b> porque ambos mandatos acceden a los archivos <code>\$HOME/.rhosts</code> y <code>/etc/hosts.equiv</code>.</p> <p>El mandato <b>rsh</b> también se puede configurar para utilizar Kerberos V.5 a fin de autenticar al usuario. Esta opción permite identificar al usuario sin utilizar un archivo <code>\$HOME/.rhosts</code> o sin pasar la contraseña por la red. Para obtener más información sobre este uso del mandato <b>rsh</b>, consulte el apartado “<a href="#">Autentificación y los rcmds seguros</a>” en la página 112.</p>

---

Item	Descripción
<b>telnet, tn y tn3270</b>	<p>El mandato <b>telnet</b> es un programa de emulación de terminal que implementa el protocolo TELNET y le permite iniciar la sesión en un sistema principal externo similar o diferente. TCP/IP se utiliza para comunicarse con otros sistemas principales de la red.</p> <p><b>Nota:</b> Por comodidad, a partir de ahora <b>telnet</b> hará referencia a los mandatos <b>telnet, tn y tn3270</b>.</p> <p>El mandato <b>telnet</b> es uno de los procedimientos que un usuario puede utilizar para iniciar la sesión en un sistema principal remoto. La característica más importante del mandato <b>telnet</b> es que es un mandato <i>autorizado</i>. En cambio, el mandato <b>rlogin</b>, que también permite el inicio de sesión remoto, no se considera un mandato autorizado.</p> <p>Un sistema puede necesitar seguridad adicional para evitar que usuarios no autorizados puedan acceder a los archivos, robar datos delicados, suprimir archivos o colocar virus o elementos nocivos en el sistema. Las funciones de seguridad de TCP/IP están diseñadas para evitar estas situaciones.</p> <p>Un usuario que desea iniciar la sesión en un sistema principal remoto con el mandato <b>telnet</b> deberá proporcionar el nombre de usuario y la contraseña de un usuario aprobado para dicho sistema. Este procedimiento es similar al empleado para iniciar la sesión en un sistema principal local. Una vez iniciada satisfactoriamente la sesión en un sistema principal remoto, el terminal del usuario funcionará como si estuviera conectado directamente al sistema principal.</p> <p>El mandato <b>telnet</b> soporta una opción denominada <i>negociación de terminal</i>. Si el sistema principal remoto da soporte a la negociación de terminal, el mandato <b>telnet</b> envía el tipo de terminal local al sistema principal remoto. Si el sistema principal remoto no acepta el tipo de terminal local, el mandato <b>telnet</b> intenta emular un terminal 3270 y un terminal DEC VT100. Si especifica un terminal para emular, el mandato <b>telnet</b> no negocia el tipo de terminal. Si los sistemas principales local y remoto no se ponen de acuerdo sobre un tipo de terminal, el sistema principal local adopta el valor predeterminado <b>none</b>.</p> <p>El mandato <b>telnet</b> soporta estos tipos de terminal 3270: 3277-1, 3278-1, 3278-2, 3278-3, 3278-4 y 3278-5. Si está utilizando el mandato <b>telnet</b> en modalidad 3270 en una pantalla de color, los colores y los campos se visualizarán, de forma predeterminada, igual que los de una pantalla 3279. Puede seleccionar otros colores editando uno de los archivos de correlación de teclado en la lista anterior de tipos de terminal. Una vez finalizada la sesión <b>telnet</b>, la pantalla se restablecerá a los colores que se utilizaban antes de que empezara la sesión.</p> <p>El mandato <b>telnet</b> también se puede configurar para utilizar Kerberos V.5 con el objeto de autenticar al usuario. Esta opción permite identificar al usuario sin utilizar un archivo \$HOME/.rhosts o sin pasar la contraseña por la red. Para obtener más información sobre esta utilización del mandato <b>telnet</b>, consulte <a href="#">“Autenticación y los rcmds seguros” en la página 112</a>.</p>

**Nota:** Se pueden utilizar los mandatos **rsh** y **rexec** para ejecutar mandatos en un sistema principal remoto, pero dado que ninguno de los dos es un mandato autorizado, es posible que no cumplan todos los niveles de seguridad configurados en el sistema. Como consecuencia, estos mandatos pueden inhabilitarse si su sistema necesita seguridad adicional.

### Inicios de sesión en un sistema principal remoto

Puede iniciar la sesión en un sistema principal remoto mediante el mandato **telnet**

Para ello, debe disponer de un ID de usuario y una contraseña que sean válidos para el sistema principal remoto.

Para iniciar la sesión en un sistema principal remoto (host1 en este ejemplo), escriba:

```
telnet host1
```

En la pantalla, aparecerá información similar a la siguiente:

```
Trying . . .
Connected to sistpral1
Escape character is '^T'.
AIX telnet (host1)

AIX Operating System
Versión 7.1
(/dev/pts0)
login:_
```

Cuando haya iniciado la sesión, podrá emitir mandatos. Para finalizar la sesión en el sistema y cerrar la conexión, pulse la secuencia de teclas Control-D.

Si no puede iniciar la sesión, cancele la conexión pulsando la secuencia de teclas Control-T.

### Conversación con un usuario remoto

Utilice el mandato **talk** para tener una conversación en tiempo real con otro usuario en un sistema principal remoto.

1. El daemon **talkd** debe estar activo tanto en el sistema principal local como en el remoto.
2. El usuario del sistema principal remoto debe haber iniciado la sesión.

El mandato **talk** precisa de una dirección válida para enlazarse a ella. El nombre de sistema principal del terminal remoto debe estar enlazado a una interfaz de red en funcionamiento que puedan utilizar otros mandatos de la red, como el mandato **ping**. Si una máquina no tiene ninguna interfaz de red que sea un terminal autónomo, debe enlazar su nombre de sistema principal con la dirección de bucle de retorno (127.0.0.1) para que el mandato **talk** funcione.

Mediante un correo electrónico, puede enviar mensajes de texto a otros usuarios de una red local y recibir también correo de ellos. Si un sistema está configurado correctamente y conoce la dirección electrónica correspondiente, puede enviar mensajes de correo electrónico en el mundo entero a alguien de un sistema remoto.

**TCP/IP** contiene los siguientes mandatos para las comunicaciones remotas:

Item	Descripción
<b>mail</b>	Envía y recibe memorándums y cartas electrónicas
<b>talk</b>	Permite tener una conversación interactiva con un usuario de un sistema principal remoto

- |  |  |
| --- | --- |
| **mail** | Envía y recibe memorándums y cartas electrónicas |
- |  |  |
| --- | --- |
| **talk** | Permite tener una conversación interactiva con un usuario de un sistema principal remoto |

1. Para conversar con el usuario remoto dale@host2 que ha iniciado la sesión en un sistema principal remoto, jane@host1 escribe:

```
talk dale@host2
```

En la pantalla de dale@host2 aparecerá un mensaje similar al siguiente:

```
Message from TalkDaemon@host1 at 15:16...
talk: connection requested by jane@host1.
talk: respond with: talk jane@host1.
```

Este mensaje informa a dale@host2 que jane@host1 está intentando conversar con ella.

2. Para aceptar la invitación, dale@host2 escribe:

```
talk jane@host1
```

Ahora, los usuarios dale@host2 y jane@host1 pueden tener una conversación interactiva.

3. Para finalizar una conversación en cualquier momento, cualquiera de los dos usuarios puede pulsar la secuencia de teclas Control-C.

Volverán al indicador de la línea de mandatos.

## Transferencia de archivos

Aunque es posible enviar archivos relativamente pequeños utilizando el correo electrónico, existen modos más eficaces para transferir archivos de mayor tamaño.

Los programas de correo electrónico suelen estar diseñados para transmitir cantidades de texto no muy grandes y, por consiguiente, es preciso utilizar otros métodos para transferir archivos grandes con eficacia. Los mandatos **ftp**, **rcp** y **tftp** se basan en **TCP/IP** para establecer conexiones directas desde el sistema principal local a un sistema principal remoto. BNU (Basic Network Utilities - Programas de utilidad básicos de red) también pueden utilizar **TCP/IP** para proporcionar conexiones directas con sistemas principales externos.

### Transferencias de archivo utilizando los mandatos **ftp** y **rcp**

Utilice el mandato **ftp** para copiar un archivo de un sistema principal remoto. El mandato **ftp** no conserva los atributos de archivo ni copia los subdirectorios. Si es necesaria alguna de estas condiciones, utilice el mandato **rcp**.

#### Ite Descripción

##### m

- ft** Utiliza **File Transfer Protocol (FTP)** para transferir archivos entre sistemas principales que utilizan diferentes sistemas de archivos o representaciones de caracteres, EBCDIC y ASCII. Proporciona seguridad enviando contraseñas al sistema principal remoto y también permite el inicio de sesión automático, las transferencias de archivos y la terminación de sesión.
- rc** Copia uno o más archivos entre un sistema principal remoto y uno local, entre dos sistemas principales remotos separados, o entre archivos del mismo sistema principal remoto. Este mandato es parecido al mandato **cp**, pero se diferencia en que sólo funciona para operaciones de archivo remotas. Si su red precisa seguridad adicional, el gestor del sistema se encarga de inhabilitar este mandato.

Antes de intentar la transferencia de archivos utilizando los mandatos **ftp** y **rcp**, asegúrese de que las siguientes condiciones sean ciertas:

1. Debe estar especificado el permiso de inicio de sesión remoto en el archivo `$HOME/.netrc` del sistema principal remoto si se debe utilizar la característica de inicio de sesión automático. En caso contrario, deberá conocer el nombre de inicio de sesión y la contraseña del sistema principal remoto. Para obtener más información sobre el archivo `.netrc`, consulte el apartado “[Creación del archivo .netrc](#)” en la página 114.

Como alternativa, se puede configurar el sistema para que utilice la autenticación Kerberos V.5. Se utilizará en lugar de los archivos `.netrc` o `$HOME/.rhosts`. Consulte el apartado “[Autentificación y los rcmds seguros](#)” en la página 112.

2. Si desea copiar un archivo de un sistema principal remoto, debe disponer de permiso de lectura para dicho archivo.

**Nota:** Los permisos de lectura y grabación para archivos y directorios de un sistema principal remoto los determina el nombre de inicio de sesión utilizado.

3. Si desea copiar un archivo del sistema principal local en el sistema principal remoto, debe disponer de permiso de grabación para el directorio que va a contener el archivo copiado. Asimismo, si el directorio del sistema principal remoto contiene un archivo cuyo nombre coincide con el archivo que desea copiar en dicho directorio, debe tener permiso de grabación para poder añadirlo al sistema principal remoto.

### *[Inicio de sesión directo en un sistema principal remoto](#)*

Al utilizar **TCP/IP** para transferir archivos, puede utilizar este procedimiento para iniciar la sesión directamente en un sistema principal remoto.

1. Utilice el mandato **cd** para cambiar al directorio que contiene el archivo que desea enviar (enviar un archivo) o al directorio en el que desea que resida el archivo transferido (recibir un archivo).

2. Inicie la sesión directamente en el sistema principal remoto escribiendo:

```
ftp NombreSistpral
```

Si tiene permiso de inicio de sesión automático, se visualizará información similar a la siguiente en el sistema principal local:

```
Connected to canopus.austin.century.com.  
220 canopus.austin.century.com FTP server  
(Version 4.1 Sat Nov 23 12:52:09 CST 1995) ready.  
331 Password required for dee.  
230 User dee logged in.  
ftp>
```

De lo contrario, en el sistema principal local se visualizará información similar a la siguiente:

```
Connected to canopus.austin.century.com.  
220 canopus.austin.century.com FTP server  
(Version 4.1 Sat Nov 23 12:52:09 CST 1995) ready.  
Name (canopus:eric): dee  
331 Password required for dee.  
Password:  
230 User dee logged in.  
ftp>
```

3. Entre el nombre de inicio de sesión y la contraseña cuando se lo solicite el sistema.

Ahora ya puede empezar a copiar un archivo entre los dos sistemas principales.

#### ***Inicio de sesión indirecto en un sistema principal remoto***

Cuando se utiliza **TCP/IP** para transferir archivos, puede utilizar este procedimiento para iniciar la sesión en un sistema principal remoto indirectamente.

1. Utilice el mandato **cd** para cambiar al directorio que contiene el archivo que desea enviar (enviar un archivo) o al directorio en el que desea que resida el archivo transferido (recibir un archivo).
2. Inicie la sesión indirectamente en el sistema principal remoto escribiendo:

```
ftp
```

3. Cuando se visualice **ftp>**, escriba:

```
open NombreSistpral
```

Si tiene permiso de inicio de sesión automático, se visualizará información similar a la siguiente en el sistema principal local:

```
Connected to canopus.austin.century.com.  
220 canopus.austin.century.com FTP server  
(Version 4.1 Sat Nov 23 12:52:09 CST 1995) ready.  
331 Password required for dee.  
230 User dee logged in.  
ftp>
```

De lo contrario, en el sistema principal local se visualizará información similar a la siguiente:

```
Connected to canopus.austin.century.com.  
220 canopus.austin.century.com FTP server  
(Version 4.1 Sat Nov 23 12:52:09 CST 1995) ready.  
Name (canopus:eric): dee  
331 Password required for dee.  
Password:  
230 User dee logged in.  
ftp>
```

4. Escriba el nombre y la contraseña cuando se lo solicite el sistema.

#### ***Copia de un archivo de un sistema principal remoto en un sistema principal local***

Utilice el mandato **ftp** para copiar un archivo de un sistema principal remoto en un sistema principal local.

Para copiar un archivo de un sistema principal remoto en un sistema principal local mediante el mandato **ftp**, primero debe iniciar la sesión en el sistema remoto directa o indirectamente. Para obtener instrucciones, consulte el apartado [Inicio de sesión directo en un sistema principal remoto](#) o [Inicio de sesión indirecto en un sistema principal remoto](#).

**Nota:** El mandato **ftp** utiliza el tipo de transferencia predeterminado ASCII para copiar archivos.

Para copiar un archivo desde un sistema principal remoto hasta un sistema principal local:

1. Determine si el archivo que desea copiar se encuentra en el directorio actual ejecutando el submandato **dir**.

(El submandato **dir** para el mandato **ftp** funciona del mismo modo que el mandato **ls -l**). Si el archivo no se encuentra allí, utilice el submandato **cd** para mover el directorio correcto.

2. Para copiar el archivo local mediante una imagina binaria, escriba:

```
binary
```

3. Para copiar un archivo en el sistema principal, escriba:

```
get FileName
```

El archivo se coloca en el directorio desde el que ha emitido el mandato **ftp**.

4. Para finalizar la sesión, pulse la secuencia de teclas Control-D o escriba **quit**.

#### [\*\*Copia de un archivo de un sistema principal local en un sistema principal remoto\*\*](#)

Utilice el mandato **ftp** para copiar un archivo de un sistema principal local en un sistema principal remoto.

Para copiar un archivo de un sistema principal local en un sistema principal remoto mediante el mandato **ftp**, primero debe iniciar la sesión en el sistema remoto directa o indirectamente. Para obtener instrucciones, consulte el apartado [Inicio de sesión directo en un sistema principal remoto](#) o [Inicio de sesión indirecto en un sistema principal remoto](#).

**Nota:** El mandato **ftp** utiliza el tipo de transferencia predeterminado ASCII para copiar archivos.

Para copiar un archivo de un sistema principal local a un sistema principal remoto:

1. Si desea colocar el archivo en un directorio distinto del directorio \$HOME, utilice el submandato **cd** para ir hasta el directorio deseado.
2. Para copiar el archivo local mediante una imagina binaria, escriba:

```
binary
```

3. Para copiar un archivo en el sistema principal remoto, escriba:

```
put FileName
```

4. Para finalizar la sesión, pulse la secuencia de teclas Control-D o escriba **quit**.

#### **Transferencias de archivo utilizando los mandatos tftp y utftp**

Utilice los mandatos **tftp** y **utftp** para que **Trivial File Transfer Protocol (TFTP)** transfiera archivos entre sistemas principales.

Dado que **TFTP** es un protocolo de transferencia de un solo archivo, los mandatos **tftp** y **utftp** no proporcionan todas las características del mandato **ftp**. Si su red precisa seguridad adicional, el gestor del sistema puede inhabilitar este mandato.

**Nota:** El mandato **tftp** no está disponible cuando el sistema principal funciona con un alto nivel de seguridad.

Antes de intentar una transferencia de archivos utilizando los mandatos **tftp** y **utftp**, asegúrese de que las siguientes condiciones sean ciertas:

1. Si desea copiar un archivo de un sistema principal remoto, debe tener permiso de *lectura* para el directorio que contiene el archivo deseado.

- Si desea copiar un archivo en un sistema principal remoto, debe tener permiso de grabación para el directorio en el que se debe poner el archivo.

#### Copia de un archivo de un sistema principal remoto

Cuando se utiliza **TCP/IP** para copiar archivos, puede utilizar este procedimiento para copiar archivos de un sistema principal remoto.

- Para establecer una conexión con un sistema principal remoto, escriba:

```
tftp sistpral1
```

En este ejemplo, `sistpral1` es el nombre del sistema principal al que desea conectarse.

Se visualiza el indicador `tftp>`.

- Para determinar si se ha establecido una conexión, escriba:

```
estado
```

Se muestra un mensaje similar al siguiente:

```
Connected to sistpral1
Mode: netascii Verbose: off Tracing: off
Remxt-interval: 5 seconds, Max-timeout: 25 seconds
tftp>
```

- Entre el submandato **get**, el nombre del archivo que se debe transferir y el nombre que se debe asignar al archivo en el sistema remoto:

```
get /home/alice/update update
```

El directorio `/home/alice` del sistema principal remoto debe tener el permiso de lectura establecido para otros usuarios. En este ejemplo, el archivo `/home/alice/update` se transfiere de `host1` al archivo `update` en el directorio actual del sistema local.

- Para finalizar la sesión, escriba:

```
quit
```

o pulse la secuencia de teclas Control-D.

#### Copia de un archivo en un sistema principal remoto

Al utilizar **TCP/IP** para copiar archivos, puede utilizar este procedimiento para copiar un archivo en un sistema principal remoto.

- Para establecer una conexión con un sistema principal remoto, escriba:

```
tftp sistpral1
```

En este ejemplo, `sistpral1` es el nombre del sistema principal al que desea conectarse.

Se visualiza el indicador `tftp>`.

- Para determinar si se ha establecido una conexión, escriba:

```
estado
```

Se muestra un mensaje similar al siguiente:

```
Connected to sistpral1
Mode: netascii Verbose: off Tracing: off
Remxt-interval: 5 seconds, Max-timeout: 25 seconds
tftp>
```

- Entre el submandato **put**, el nombre del archivo que se debe transferir del sistema principal local y la vía de acceso y el nombre del archivo en el sistema principal remoto:

```
put miarchivo /home/alice/suarchivo
```

El directorio /home/alice del sistema principal remoto debe tener el permiso de grabación establecido para otros.

El archivo miarchivo, situado en el directorio de trabajo actual del usuario se transfiere a sistpral1. Debe especificar el nombre de la vía de acceso, a menos que se haya indicado un nombre predeterminado. El archivo miarchivo aparece en el sistema principal remoto como tuarchivo.

4. Para finalizar la sesión, escriba:

```
quit
```

o utilice la secuencia de teclas Control-D.

## Impresión de archivos en un sistema remoto

Si tiene una impresora local conectada al sistema principal, los procedimientos siguientes hacen referencia a la impresión en una impresora remota. Si no tiene impresora local, los procedimientos siguientes hacen referencia a la impresión en una impresora remota distinta de la impresora predeterminada.

1. El nombre del sistema principal debe aparecer en el archivo /etc/hosts.1pd del sistema principal remoto.

**Nota:** El sistema de colas no soporta los nombres de sistema principal de varios bytes.

Para implementar los cambios en el archivo /etc/hosts.1pd sin reiniciar el sistema, utilice el mandato **refresh** de System Resource Controller (SRC).

2. Debe poder determinar el nombre de cola y el nombre de impresora remota en el archivo /usr/lib/lpd/qconfig local

Puede utilizar el mandato **enq** o la System Management Interface Tool (SMIT) para llevar a cabo esta tarea.

**Nota:** Esta sección explica cómo imprimir en un sistema principal remoto de la forma más sencilla posible. Para obtener más información e ideas sobre la impresión remota, consulte el mandato **enq**.

## Colocación de un trabajo de impresión en una cola de impresión remota

Cuando se utiliza **TCP/IP** para imprimir archivos, puede utilizar este procedimiento para poner un trabajo en una cola de impresión remota.

Para colocar un trabajo en una cola de impresión remota, el nombre de sistema principal debe aparecer en el archivo /etc/hosts.1pd del sistema principal remoto (el sistema de colas no soporta nombres de sistemas principales de múltiples bytes). Para implementar los cambios en el archivo /etc/hosts.1pd sin reiniciar el sistema, utilice el mandato **refresh** de System Resource Controller (SRC). Asimismo, debe poder determinar el nombre de la cola y el nombre de la impresora remota en el archivo /usr/lib/lpd/qconfig local.

1. Localice el nombre de cola y el nombre de dispositivo remoto apropiados. El nombre de cola suele empezar por las letras rp seguidas de uno o más números. El nombre de la impresora remota suele empezar por las letras drp seguidas de uno o más números.
2. Entre el mandato siguiente:

```
enq -P NombreCola:NombreImpresora NombreArchivo
```

donde *NombreCola* es el nombre de la cola (por ejemplo rp1) y *NombreImpresora* es el nombre de la impresora (por ejemplo drp1) tal como se encuentra en el archivo /usr/lib/lpd/qconfig. No omita el signo de dos puntos (:) entre *NombreCola* y *NombreImpresora*. *NombreArchivo* es el nombre del archivo que desea imprimir.

Los siguientes ejemplos muestran cómo se puede utilizar el mandato **enq**:

- Para imprimir el archivo memo en la impresora predeterminada, escriba:

```
enq memo
```

- Para imprimir el archivo prog.c con números de página, escriba:

```
pr prog.c | enq
```

El mandato **pr** coloca una cabecera al principio de cada página que incluye la fecha en que se modificó el archivo por última vez, el nombre del archivo y el número de la página. Entonces el mandato **enq** imprime el archivo.

- Para imprimir el archivo report en la siguiente impresora disponible configurada para la cola fred, escriba:

```
enq -P fred report
```

- Para imprimir varios archivos que empiezan con el prefijo sam en la siguiente impresora disponible configurada para la cola fred, escriba:

```
enq -P fred sam*
```

Todos los archivos que empiecen por el prefijo sam se incluirán en un trabajo de impresión. Los mandatos de estado normal sólo muestran el título del trabajo de impresión, que en este caso es el nombre del primer archivo de la cola, a menos que se haya especificado un valor diferente con el distintivo **-T**. Para listar los nombres de todos los archivos del trabajo de impresión, utilice el mandato de estado largo **enq -A -L**.

### Cómo poner en cola un trabajo utilizando SMIT

Al utilizar **TCP/IP** para poner en cola archivos, puede utilizar el mandato **smit**.

1. Para poner en cola un trabajo utilizando SMIT, escriba el mandato siguiente:

```
smit
```

2. Seleccione el **Spooler** e inicie un menú de trabajo de impresión.
3. Seleccione la opción **Archivo a imprimir** y escriba el nombre del archivo que desea imprimir.
4. Seleccione la opción **Cola de impresión** y seleccione el nombre de la impresora remota en la que desea imprimir.

A partir de ese momento, ya puede imprimir en una impresora remota.

### Impresión de archivos de un sistema remoto

Es posible que a veces necesite imprimir un archivo que está ubicado en un sistema principal remoto. La ubicación de la salida impresa dependerá de las impresoras remotas que estén disponibles en el sistema remoto.

1. Debe poder iniciar la sesión en el sistema remoto utilizando el mandato **rlogin** o **telnet**.
2. Debe tener permiso de lectura para el archivo remoto que desea imprimir en la impresora local.

**Nota:** Este procedimiento explica cómo imprimir en un sistema principal remoto en el nivel más simple posible. Para obtener más información e ideas sobre la impresión remota, lea la documentación sobre el mandato **enq**.

Para imprimir desde un sistema remoto:

1. Inicie la sesión en el sistema remoto utilizando el mandato **rlogin** o **telnet**.
2. Localice el nombre de cola y el nombre de dispositivo remoto apropiados. El nombre de cola suele empezar por las letras **rp** seguidas de uno o más números. El nombre de la impresora remota suele empezar por las letras **d rp** seguidas de uno o más números.
3. Escriba el mandato siguiente:

```
enq -P NombreCola:NombreImpresora NombreArchivo
```

donde *NombreCola* es el nombre de la cola (por ejemplo `rp1`) y *NombreImpresora* es el nombre de la impresora (por ejemplo `d rp1`) tal como se encuentra en el archivo `/usr/lib/lpd/qconfig`. No omita el signo : (dos puntos) entre *NombreCola* y *NombreImpresora*. *NombreArchivo* es el nombre del archivo que desea imprimir.

4. Finalice la conexión con el sistema principal remoto pulsando la secuencia Control-D o escribiendo `quit`.

## Visualización de información de estado

Se pueden utilizar mandatos **TCP/IP** para determinar el estado de una red, visualizar información acerca de un usuario y resolver la información de sistema principal necesaria para comunicarse con otro sistema principal o usuario.

### Mandatos de estado de TCP/IP

**TCP/IP** contiene mandatos de estado para determinar el estado de los sistemas principales locales y remotos y de sus redes.

Item	Descripción
<b>finger</b> o <b>f</b>	Visualiza información sobre los usuarios actuales de un determinado sistema principal. Esta información puede incluir datos como, por ejemplo, el nombre de inicio de sesión del usuario, el nombre completo y el nombre del terminal; así como la fecha y la hora del inicio de sesión.
<b>host</b>	Resuelve un nombre de sistema principal en una dirección de Internet o viceversa.
<b>ping</b>	Ayuda a determinar el estado de una red o sistema principal. Se utiliza habitualmente para verificar que se está ejecutando una red o sistema principal.
<b>rwho</b>	Muestra los usuarios que han iniciado una sesión en una red local. Visualiza el nombre del usuario, el nombre del sistema principal y la fecha y hora del inicio de sesión de todos los usuarios de la red local.
<b>whois</b>	Identifica a quién pertenece un ID de usuario o apodo. Este mandato sólo se puede utilizar si la red local está conectada a la red Internet.

### Visualización de información sobre todos los usuarios conectados a un sistema principal

Utilice este procedimiento para ver información sobre *todos* los usuarios conectados a un sistema principal remoto.

Para visualizar información sobre todos los usuarios conectados a un sistema principal remoto:

1. Inicie la sesión en el sistema principal remoto con el que desea establecer comunicación.
2. Para visualizar información sobre todos los usuarios conectados al sistema principal remoto `alcatraz`, escriba:

```
finger @alcatraz
```

Se visualiza información similar a la siguiente:

```
brown    console  Mar 15 13:19
smith    pts0     Mar 15 13:01
jones    tty0     Mar 15 13:01
```

El usuario `bosch` está conectado a la consola, el usuario `valle` está conectado desde una pseudolínea de teletipo `pts0` y el usuario `marin` está conectado desde `tty0`. El administrador de sistemas puede configurar el sistema para que el mandato **finger** funcione de forma diferente. Si registra algún problema al utilizar el mandato **finger**, póngase en contacto con el administrador de sistemas.

## Visualización de información sobre un usuario conectado a un sistema principal

Utilice este procedimiento para ver información sobre un usuario *específico* conectado a un sistema principal remoto.

Para visualizar información sobre un único usuario conectado a un sistema principal remoto:

1. Inicie la sesión en el sistema principal remoto con el que desea establecer comunicación.
2. Para visualizar información sobre el usuario brown en un sistema principal alcatraz, escriba:

```
finger brown@alcatraz
```

Se visualiza información similar a la siguiente:

```
Login name: brown
Directory: /home/brown      Shell: /home/bin/xinit -L -n Startup
On since May 8 07:13:49 on console
No Plan.
```

El administrador de sistemas puede configurar el sistema para que el mandato **finger** funcione de forma diferente. Si registra algún problema al utilizar el mandato **finger**, póngase en contacto con el administrador de sistemas.

## Protocolos TCP/IP

Los protocolos son conjuntos de normas para formatos de mensaje y procedimientos que permiten a las máquinas y los programas de aplicación intercambiar información. Cada máquina implicada en la comunicación debe seguir estas normas para que el sistema principal de recepción pueda interpretar el mensaje. El *conjunto* de protocolos TCP/IP puede interpretarse en términos de capas (o niveles).

Esta figura muestra las capas del protocolo **TCP/IP**. Empezando por la parte superior son: capa de aplicación, capa de transporte, capa de red, capa de interfaz de red y hardware.

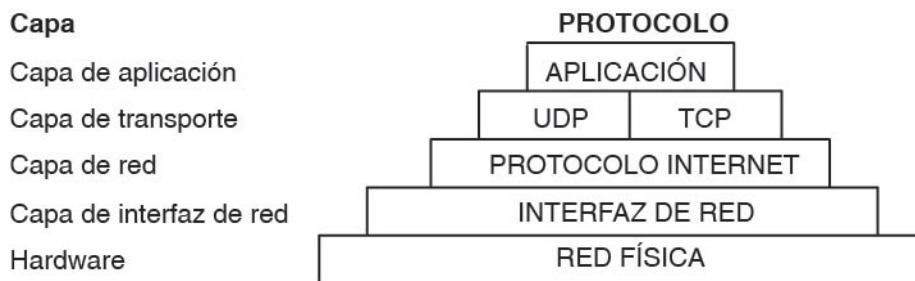


Figura 4. Conjunto de protocolos TCP/IP

TCP/IP define cuidadosamente cómo se mueve la información desde el remitente hasta el destinatario. En primer lugar, los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, **UDP (User Datagram Protocol)** o **TCP (Transmission Control Protocol)**. Estos protocolos reciben los datos de la aplicación, los dividen en partes más pequeñas llamadas *paquetes*, añaden una dirección de destino y, a continuación, pasan los paquetes a la siguiente capa de protocolo, la capa de red de Internet.

La capa de red de Internet pone el paquete en un datagrama de **IP (Internet Protocol)**, pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (directamente a un destino o a una pasarela) y pasa el datagrama a la capa de interfaz de red.

La capa de interfaz de red acepta los datagramas **IP** y los transmite como *tramas* a través de un hardware de red específico, por ejemplo redes Ethernet o de Red en anillo.

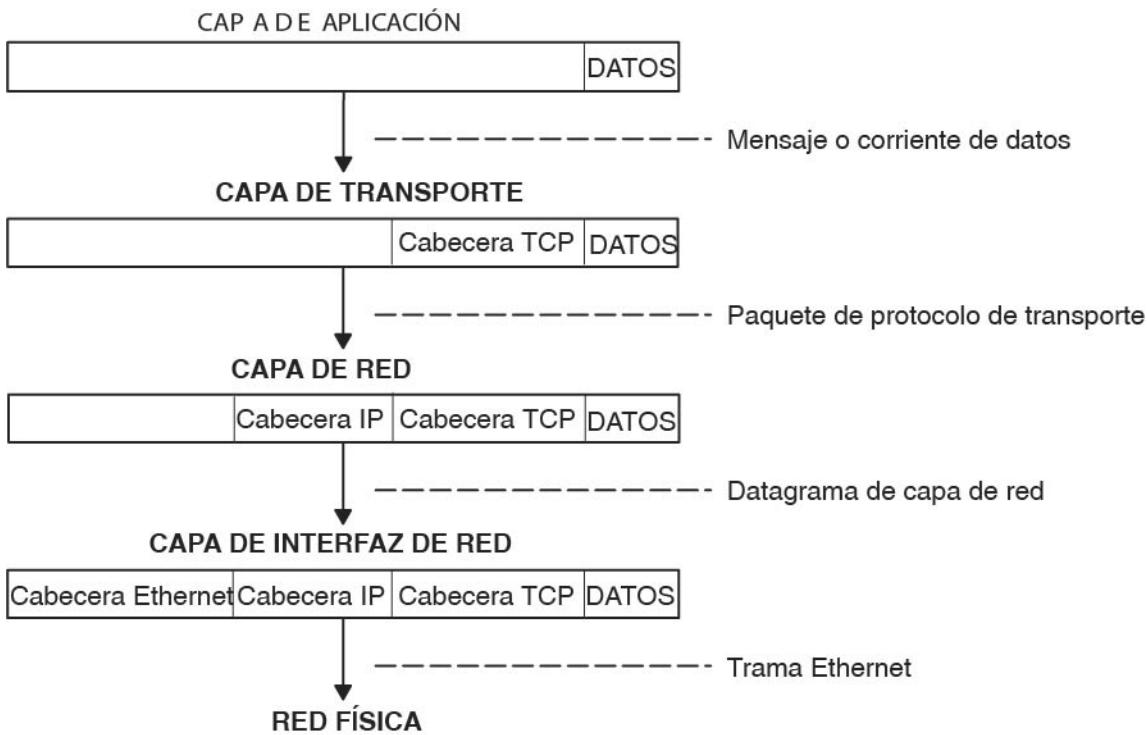


Figura 5. Movimiento de la información desde la aplicación remitente hasta el sistema principal destinatario

Esta figura muestra el flujo de información de las capas de protocolo TCP/IP del remitente al host.

Las tramas recibidas por un sistema principal pasan a través de las capas de protocolo en sentido inverso. Cada capa quita la información de cabecera correspondiente, hasta que los datos regresan a la capa de aplicación.

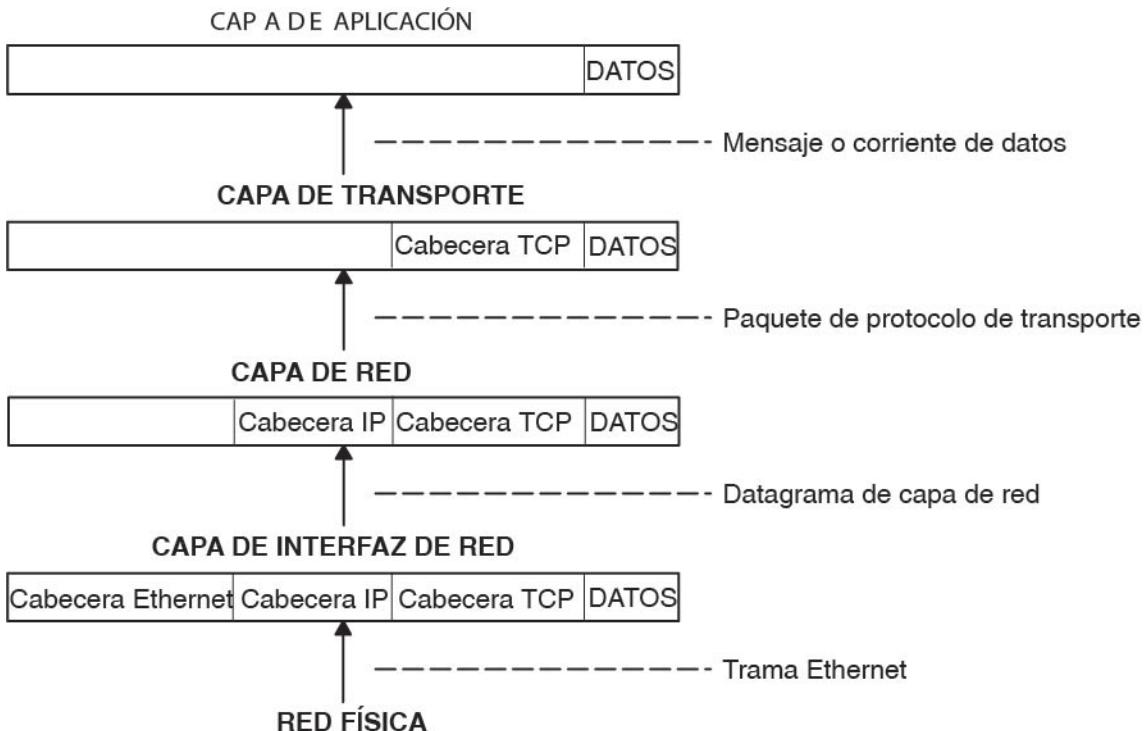
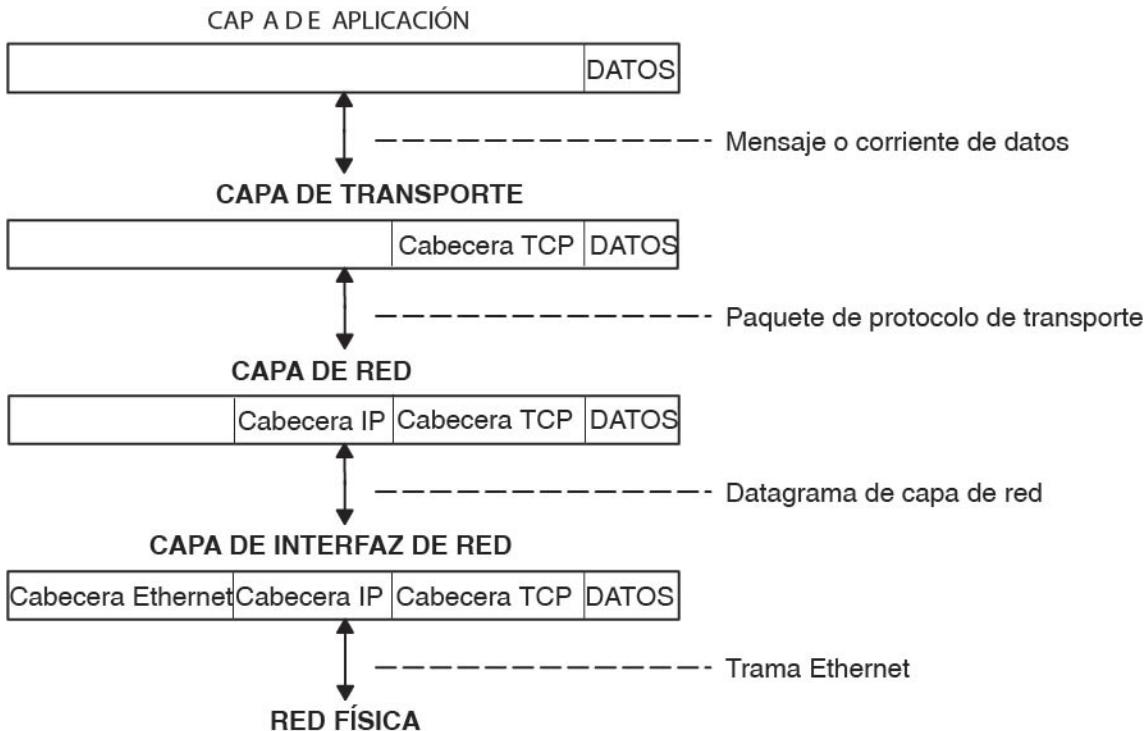


Figura 6. Movimiento de la información desde el sistema principal hasta la aplicación

Esta figura muestra el flujo de información de las capas de protocolo **TCP/IP** desde el sistema principal al remitente.

La capa de interfaz de red (en este caso, un adaptador Ethernet) recibe las tramas. La capa de interfaz de red quita la cabecera Ethernet y envía el datagrama hacia arriba hasta la capa de red. En la capa de red, Protocolo Internet quita la cabecera IP y envía el paquete hacia arriba hasta la capa de transporte. En la capa de transporte, **TCP** (en este caso) quita la cabecera **TCP** y envía los datos hacia arriba hasta la capa de aplicación.

Los sistemas principales de una red envían y reciben información simultáneamente. [Figura 7 en la página 130](#) representa de forma más precisa un sistema principal mientras se comunica.



**Nota:** las cabeceras se añaden y separan en cada capa de protocolo a medida que los host transmiten y reciben datos.

*Figura 7. Transmisiones y recepciones de datos de sistema principal*

Esta figura muestra los datos que fluyen en ambas direcciones a través de las capas **TCP/IP**.

#### Protocolo Internet (IP) versión 6

**Internet Protocol (IP)** versión 6 (**IPv6** o IPng) es la siguiente generación de **IP** y se ha diseñado para ser un paso de desarrollo de **IP** versión 4 (**IPv4**).

Aunque **IPv4** ha permitido el desarrollo de una Internet global, no es capaz de aportar mucho más en el futuro debido a dos factores fundamentales: espacio de direcciones limitado y complejidad de direccionamiento. Las direcciones **IPv4** de 32 bits no proporcionan suficiente flexibilidad para el direccionamiento global de Internet. El despliegue de CIDR (Classless InterDomain Routing - Direccionamiento entre dominios sin clase) ha ampliado el tiempo de vida del direccionamiento de **IPv4** en varios años, pero se continuará realizando el esfuerzo de gestionar mejor el direccionamiento. Incluso si el direccionamiento de **IPv4** se pudiera escalar, finalmente Internet se quedaría sin números de red.

Internet Engineering Task Force (IETF) ha reconocido que **IPv4** no será capaz de soportar el fenomenal crecimiento de Internet, de modo que se ha creado el grupo de trabajo de IPng de IETF. Entre las propuestas que se realizaron, se eligió **Simple Internet Protocol Plus (SIPP)** como paso revolucionario en el desarrollo de IP. Éste se redenominó como IPng y se finalizó la RFC1883 en diciembre de 1995.

IPv6 amplía el número máximo de direcciones de Internet para manejar la continuamente creciente población usuarios de Internet. Como cambio evolutivo respecto a **IPv4**, **IPv6** tiene la ventaja de permitir

la coexistencia de lo antiguo y lo nuevo en la misma red. Esta coexistencia permite una migración ordenada de **IPv4** (direcccionamiento de 32 bits) a **IPv6** (direcccionamiento de 128 bits) en una red operativa.

Esta visión general está destinada a proporcionar al lector una comprensión general del protocolo IPng. Para obtener información detallada, consulte las RFC 2460, 2373, 2465, 1886, 2461, 2462 y 2553.

La publicación *Security* proporciona información de seguridad sobre el conjunto de protocolos **TCP/IP**, incluido **IPv6**. Para obtener detalles sobre la Seguridad de IP, versiones 4 y 6, consulte [Seguridad del Protocolo Internet](#).

## Configuración automática de IPv6

Los mecanismos primarios disponibles que permiten que un nodo arranque y se comunique con otros nodos a través de una red **IPv4** son la codificación fija, **BOOTP** y **DHCP**.

**IPv6** presenta el concepto de *ámbito* en las direcciones **IP**, una de las cuales es local del enlace. Esto permite que un sistema principal construya una dirección válida a partir del prefijo predefinido local del enlace y del identificador local. Este identificador local se obtiene normalmente de la dirección de control de acceso al medio (MAC) de la interfaz que se debe configurar. Utilizando esta dirección, el nodo puede comunicarse con otros sistemas principales de la misma subred y, para una subred totalmente aislada, es posible que no necesite ninguna otra configuración de dirección.

## Direcciones de IPv6 significativas

Con **IPv4**, el único significado generalmente reconocible en las direcciones son la difusión (normalmente todos los 1 o todos los 0) y las clases (por ejemplo, una clase D es multidifusión). Con **IPv6**, se puede examinar rápidamente el prefijo para determinar el *ámbito* (por ejemplo, local del enlace), multidifusión frente a difusión individual y un mecanismo de asignación (basado en proveedor o basado en geografía).

La información de direcccionamiento también se puede cargar explícitamente en los bits de direcciones más altos, pero IETF aún no ha finalizado esta tarea (para direcciones basadas en proveedor, la información de direcccionamiento está presente de forma implícita en la dirección).

## Detección de direcciones duplicadas de IPv6

Cuando una interfaz se inicializa o reinicializa, utiliza la configuración automática para asociar a título de ensayo una dirección local de enlace con esa interfaz (la dirección aún no se ha asignado a esa interfaz en el sentido tradicional). En este punto, la interfaz une los grupos de multidifusión de todos los nodos y los nodos solicitados y envía un mensaje de descubrimiento de vecino a estos grupos. Mediante el uso de la dirección de multidifusión, el nodo puede determinar si esa dirección local de enlace determinada se ha asignado anteriormente y elegir una dirección alternativa.

Esto evita que se asigne accidentalmente la misma dirección a dos interfaces diferentes en el mismo enlace. (Sigue siendo posible crear direcciones de ámbito global duplicadas para nodos que no están en el mismo enlace.)

## Configuración automática de direcciones de descubrimiento de vecino/sin estado

Los nodos (sistemas principales y direccionadores) utilizan **NDP (Neighbor Discovery Protocol - Protocolo de descubrimiento de vecino)** para **IPv6** a fin de determinar las direcciones de la capa de enlace para los vecinos conocidos como residentes en enlaces conectados y mantener tablas de direcccionamiento por destino para conexiones activas. **IPv6** define un mecanismo de configuración automática de direcciones con estado y sin estado. La *configuración automática sin estado* no requiere ninguna configuración manual de los sistemas principales; sólo una configuración mínima de los direccionadores, si es necesaria y ningún servidor adicional.

Los sistemas principales también utilizan **NDP** para buscar direccionadores vecinos que deseen reenviar paquetes en su nombre y detectar direcciones cambiadas de la capa de enlace. **NDP** utiliza **Internet Control Message Protocol (ICMP)** Versión 6 con sus propios tipos de mensaje exclusivos. En términos generales, el protocolo de Descubrimiento de vecino de **IPv6** corresponde a una combinación de los

protocolos **Address Resolution Protocol (ARP)**, ICMP Router Discovery (RDISC) e **ICMP Redirect** (ICMPv4) de **IPv4**, pero con muchas mejoras respecto a estos protocolos de **IPv4**.

El mecanismo sin estado permite a un sistema principal generar sus propias direcciones utilizando una combinación de información localmente disponible e información anunciada por los direccionadores. Los direccionadores anuncian prefijos que identifican las subredes asociadas con un enlace, mientras que los sistemas principales generan una señal de interfaz que identifica de forma exclusiva una interfaz en una subred. Una dirección se forma combinando las dos. En ausencia de direccionadores, un sistema principal sólo puede generar direcciones locales de enlace. Sin embargo, las direcciones locales de enlace son suficientes para permitir las comunicaciones entre nodos conectados al mismo enlace.

### Rutas y direcciones ampliadas de IPv6

**IPv6** incrementa el tamaño de dirección **IP** de 32 bits a 128 bits, soportando de este modo más niveles de jerarquía de direccionamiento, un número mucho mayor de nodos direccionables y la configuración automática de direcciones más simple.

**IPv6** tiene tres tipos de direcciones:

Item	Descripción
<b>unicast</b>	(difusión individual) Un paquete enviado a una dirección de difusión individual se entrega a la interfaz identificada por dicha dirección. Una dirección de difusión individual tiene un ámbito determinado: local de enlace, local de sitio, global. También hay dos direcciones de difusión individual especiales: <ul style="list-style-type: none"><li>• ::/128 (dirección no especificada)</li><li>• ::1/128 (dirección de bucle de retorno)</li></ul>
<b>multicast</b>	(multidifusión) Un paquete enviado a una dirección de multidifusión se entrega a todas las interfaces identificadas por dicha dirección. Una dirección de multidifusión se identifica por el prefijo ff::/8. Como con las direcciones de difusión individual, las direcciones de multidifusión tienen un ámbito similar: local de nodo, local de enlace, local de sitio y local de organización.
<b>anycast</b>	(cualquier difusión) Una dirección anycast es una dirección que tiene un remitente individual, varios escuchas y un solo respondedor (normalmente el "más cercano", de acuerdo con la medida de distancia de los protocolos de direccionamiento). Por ejemplo, varios servidores web que escuchan en cualquier dirección anycast. Cuando se envía una petición a la dirección anycast, sólo uno responde.  Una dirección anycast no se puede distinguir de una dirección unicast. Una dirección unicast se convierte en una dirección anycast cuando se configura más de una interfaz con dicha dirección.

**Nota:** No hay direcciones de difusión en **IPv6**. La función de éstas se ha reemplazado por la dirección de multidifusión.

### Configuración automática de IPv6

Los mecanismos primarios disponibles que permiten que un nodo arranque y se comunique con otros nodos a través de una red **IPv4** son la codificación fija, **BOOTP** y **DHCP**.

**IPv6** presenta el concepto de **ámbito** en las direcciones **IP**, una de las cuales es local del enlace. Esto permite que un sistema principal construya una dirección válida a partir del prefijo predefinido local del enlace y del identificador local. Este identificador local se obtiene normalmente de la dirección de control de acceso al medio (MAC) de la interfaz que se debe configurar. Utilizando esta dirección, el nodo puede comunicarse con otros sistemas principales de la misma subred y, para una subred totalmente aislada, es posible que no necesite ninguna otra configuración de dirección.

## Direcciones de IPv6 significativas

Con **IPv4**, el único significado generalmente reconocible en las direcciones son la difusión (normalmente todos los 1 o todos los 0) y las clases (por ejemplo, una clase D es multidifusión). Con **IPv6**, se puede examinar rápidamente el prefijo para determinar el **ámbito** (por ejemplo, local del enlace), multidifusión frente a difusión individual y un mecanismo de asignación (basado en proveedor o basado en geografía).

La información de direccionamiento también se puede cargar explícitamente en los bits de direcciones más altos, pero IETF aún no ha finalizado esta tarea (para direcciones basadas en proveedor, la información de direccionamiento está presente de forma implícita en la dirección).

## Detección de direcciones duplicadas de IPv6

Cuando una interfaz se inicializa o reinicializa, utiliza la configuración automática para asociar a título de ensayo una dirección local de enlace con esa interfaz (la dirección aún no se ha asignado a esa interfaz en el sentido tradicional). En este punto, la interfaz une los grupos de multidifusión de todos los nodos y los nodos solicitados y envía un mensaje de descubrimiento de vecino a estos grupos. Mediante el uso de la dirección de multidifusión, el nodo puede determinar si esa dirección local de enlace determinada se ha asignado anteriormente y elegir una dirección alternativa.

Esto evita que se asigne accidentalmente la misma dirección a dos interfaces diferentes en el mismo enlace. (Sigue siendo posible crear direcciones de ámbito global duplicadas para nodos que no están en el mismo enlace.)

## Configuración automática de direcciones de descubrimiento de vecino/sin estado

Los nodos (sistemas principales y direccionadores) utilizan **NDP (Neighbor Discovery Protocol - Protocolo de descubrimiento de vecino)** para **IPv6** a fin de determinar las direcciones de la capa de enlace para los vecinos conocidos como residentes en enlaces conectados y mantener tablas de direccionamiento por destino para conexiones activas. **IPv6** define un mecanismo de configuración automática de direcciones con estado y sin estado. La *configuración automática sin estado* no requiere ninguna configuración manual de los sistemas principales; sólo una configuración mínima de los direccionadores, si es necesaria y ningún servidor adicional.

Los sistemas principales también utilizan **NDP** para buscar direccionadores vecinos que deseen reenviar paquetes en su nombre y detectar direcciones cambiadas de la capa de enlace. **NDP** utiliza **Internet Control Message Protocol (ICMP)** Versión 6 con sus propios tipos de mensaje exclusivos. En términos generales, el protocolo de Descubrimiento de vecino de **IPv6** corresponde a una combinación de los protocolos **Address Resolution Protocol (ARP)**, ICMP Router Discovery (RDISC) e **ICMP Redirect** (ICMPv4) de **IPv4**, pero con muchas mejoras respecto a estos protocolos de **IPv4**.

El mecanismo sin estado permite a un sistema principal generar sus propias direcciones utilizando una combinación de información localmente disponible e información anunciada por los direccionadores. Los direccionadores anuncian prefijos que identifican las subredes asociadas con un enlace, mientras que los sistemas principales generan una señal de interfaz que identifica de forma exclusiva una interfaz en una subred. Una dirección se forma combinando las dos. En ausencia de direccionadores, un sistema principal sólo puede generar direcciones locales de enlace. Sin embargo, las direcciones locales de enlace son suficientes para permitir las comunicaciones entre nodos conectados al mismo enlace.

## Simplificación del direccionamiento

Para simplificar los problemas de direccionamiento, se considera que las direcciones de **IPv6** tienen dos partes: un prefijo y un ID. Esto puede parecer lo mismo que el desglose de dirección de red-sistema principal de **IPv4**, pero tiene dos ventajas.

Item	Descripción
<b>ninguna clase</b>	Ningún número fijo de bits para el prefijo o ID, lo que permite reducir las pérdidas debido a la asignación excesiva
<b>anidamiento</b>	Se puede emplear un número arbitrario de divisiones teniendo en cuenta diferentes números de bits como prefijo.

Caso 1

<b>128 bits</b>
dirección de nodo

Caso 2

Item	Descripción
$n$ bits	128- $n$ bits
Prefijo de subred	ID de interfaz

Caso 3:

Item	Descripción	
$n$ bits	80- $n$ bits	48 bits
Prefijo de suscriptor	ID de subred	ID de interfaz

Caso 4:

Item	Descripción		
$s$ bits	$n$ bits	$m$ bits	128- $s-n-m$ bits
Prefijo de suscripción	ID de área	ID de subred	ID de interfaz

Generalmente, IPv4 no puede ir más allá del Caso 3, incluso con la VLSM (la Máscara de subred de longitud variable (Variable Length Subnet Mask) es un medio para asignar recursos de direccionamiento de **IP** a subredes de acuerdo con las necesidades individuales en lugar de hacerlo según alguna norma de general de toda la red). Aunque se trate tanto de un artefacto de la longitud de dirección de más corta como de la definición de prefijos de longitud variable, merece la pena tenerlo en cuenta.

#### *Simplificación del formato de cabecera*

**IPv6** simplifica la cabecera de **IP** eliminando enteramente algunos de los campos encontrados en la cabecera de **IPv4** o moviendo dichos campos a una cabecera de extensión. Define un formato más flexible para información opcional (las cabeceras de extensión).

Especificamente, tenga en cuenta la ausencia de:

- longitud de cabecera (la longitud es constante)
- identificación
- distintivos
- desplazamiento de fragmento (movido a las cabeceras de extensión de fragmentación)
- suma de comprobación de cabecera (la cabecera de extensión de seguridad o de protocolo de capa superior maneja la integridad de datos).

Tabla 54. Cabecera de IPv4

Item	Descripción	Descripción	Descripción	Descripción
Versión	IHL	Tipo de servicio	Longitud total	
Identificación	Identificación	Identificación	Distintivos	Desplazamiento de fragmento

Tabla 54. Cabecera de IPv4 (continuación)

Item	Descripción	Descripción	Descripción	Descripción
Tiempo de vida	Tiempo de vida	Protocolo	Suma de comprobación de cabecera	Suma de comprobación de cabecera
Dirección de origen	Dirección de origen	Dirección de origen	Dirección de origen	Dirección de origen
Dirección de destino	Dirección de destino	Dirección de destino	Dirección de destino	Dirección de destino
Opciones	Opciones	Opciones	Opciones	Relleno

Tabla 55. Cabecera de IPv6

Item	Descripción	Descripción	Descripción	Descripción
Versión	Prio		Etiqueta de flujo	
Longitud de carga	Longitud de carga	Longitud de carga	Siguiente cabecera	Límite de saltos
Dirección de origen				
Dirección de destino				

IPng incluye un mecanismo de opciones mejorado respecto a **IPv4**. Las opciones de **IPv6** se ponen en cabeceras de extensión independientes que están ubicadas entre la cabecera de **IPv6** y la cabecera de la capa de transporte de un paquete. A la mayoría de cabeceras de extensión no las examina o procesa ningún direccionador a lo largo de la vía de acceso de entrega de paquete hasta que llegan al destino final. Este mecanismo facilita una importante mejora en el rendimiento de direccionador para los paquetes que contienen opciones. En **IPv4** la presencia de cualquier opción requiere que el direccionador examine todas las opciones.

Otra mejora es que, a diferencia de las opciones de **IPv4**, las cabeceras de extensión de **IPv6** pueden tener una longitud arbitraria y la cantidad total de opciones transportadas en un paquete no está limitada a 40 bytes. Esta característica, más el modo en que se procesa, permite utilizar las opciones de **IPv6** para funciones que no eran prácticas en **IPv4**, por ejemplo las opciones Encapsulación de seguridad y de Autenticación de **IPv6**.

Para mejorar el rendimiento al manejar las cabeceras de opción subsiguientes y el protocolo de transporte que sigue, las opciones de IPv6 son siempre un múltiplo entero de ocho octetos de longitud para retener esta alineación para las cabeceras subsiguientes.

Mediante la utilización de cabeceras de extensión en lugar de un especificador de protocolo y de campos de opciones, se pueden integrar más fácilmente las extensiones recién definidas.

Las especificaciones actuales definen las cabeceras de extensiones de las siguientes maneras:

- Opciones de salto a salto que se aplican a cada salto (dirección) a lo largo de la vía de acceso
- Cabecera de direccionamiento para direccionamiento de origen flexible/estricto (no utilizado frecuentemente)
- Un fragmento define el paquete como un fragmento y contiene información sobre el fragmento (los direcciones de **IPv6** no se fragmentan)
- Autenticación (consulte la seguridad de **TCP/IP** en la publicación *Security*)
- Cifrado (Consulte la seguridad de **TCP/IP** en la publicación *Security*)

- Opciones de destino para el nodo de destino (ignoradas por los direccionadores).

### **Control mejorado de calidad de servidor/tráfico**

Mientras que la calidad de servicio se puede controlar con el uso de un protocolo de control como **RSVP**, **IPv6** proporciona la definición de prioridad explícita para paquetes utilizando el campo de prioridad de la cabecera **IP**.

Un nodo puede establecer este valor para indicar la prioridad relativa de un paquete o conjunto de paquetes determinado, que a continuación el nodo, uno o más direccionadores o el destino pueden utilizar para realizar las elecciones concernientes al paquete (es decir, descartarlo o no).

**IPv6** especifica dos tipos de prioridades, las del tráfico controlado por congestión y las del tráfico no controlado por congestión. No hay ningún orden relativo implícito entre los dos tipos.

El *tráfico controlador por congestión* se define como tráfico que responde a la congestión mediante alguna clase de "retroceso" u otro algoritmo de limitación. Las prioridades para el tráfico controlado por congestión son:

<b>Item</b>	<b>Descripción</b>
0	tráfico no representado
1	tráfico de "relleno" (por ejemplo noticias de red)
2	transferencia de datos desatendida (por ejemplo correo)
3	(reservado)
4	transferencia masiva atendida (por ejemplo <b>FTP</b> )
5	(reservado)
6	tráfico interactivo (por ejemplo Telnet)
7	tráfico de control (por ejemplo protocolos de direccionamiento)

El *tráfico no controlado por congestión* se define como tráfico que responde a la congestión eliminando (o simplemente no reenviando) paquetes, por ejemplo vídeo, audio u otro tráfico en tiempo real. Los niveles explícitos no se definen con ejemplos, pero el orden es similar al del tráfico controlado por congestión:

- Se deberá utilizar para el tráfico el valor más bajo que el origen esté más dispuesto a que se descarte.
- Se deberá utilizar para el tráfico el valor más alto que el origen esté menos dispuesto a que se descarte.

Este control de prioridad sólo es aplicable al tráfico de una dirección de origen determinada. El tráfico de control de una dirección no es una prioridad explícitamente más alta que la transferencia masiva atendida de otra dirección.

### **Etiquetado de flujo**

Además de establecer la prioridad básica del tráfico, **IPv6** define un mecanismo para especificar un flujo determinado de paquetes. En términos de **IPv6**, un *flujo* se define como una secuencia de paquetes enviados de un origen determinado a un destino (difusión individual o multidifusión) determinado para los que el origen desea un manejo especial por parte de los direccionadores que intervienen.

Esta identificación de flujo se puede utilizar para el control de prioridad, pero también se puede utilizar para cualquier número de controles diferentes.

La etiqueta de flujo se elige al azar y no identifica ninguna característica del tráfico distinta del flujo al que pertenece. Esto significa que un direccionador no puede determinar que un paquete es un tipo determinado examinando la etiqueta de flujo. Sin embargo, puede determinar que forma parte de la misma secuencia de paquetes que el último paquete que contiene esa etiqueta.

**Nota:** Hasta que **IPv6** sea de uso general, la etiqueta de flujo es principalmente experimental. Los usos y los controles que incluyen etiquetas de flujo aún no se han definido ni estandarizado.

## Tunelización de IPv6

La tunelización proporciona un modo de utilizar una infraestructura de direccionamiento de **IPv4** existente para llevar el tráfico de **IPv6**.

La clave para una transición de **IPv6** satisfactoria es la compatibilidad con la base instalada existente de sistemas principales y direccionadores **IPv4**. El mantenimiento de la compatibilidad con **IPv4** mientras se despliega **IPv6** optimiza la tarea de transición de Internet a **IPv6**. Mientras se está desplegando la infraestructura **IPv6**, la infraestructura de direccionamiento de **IPv4** existente puede permanecer funcional y se puede utilizar para llevar a cabo el tráfico **IPv6**.

Los sistemas principales y los direccionadores **IPv6** o **IPv4** pueden establecer túneles de datagramas de **IPv6** a través de regiones de topología de direccionamiento de **IPv4** encapsulándolos en paquetes **IPv4**. La tunelización se puede utilizar de varias formas:

Item	Descripción
Direccionador a direccionador	Los direccionadores <b>IPv6</b> o <b>IPv4</b> interconectados por una infraestructura <b>IPv4</b> pueden establecer túneles de paquetes <b>IPv6</b> entre dichos paquetes. En este caso, el túnel abarca un segmento de la vía de acceso de extremo a extremo que toma el paquete <b>IPv6</b> .
Sistema principal a direccionador	Los sistemas principales <b>IPv6</b> o <b>IPv4</b> pueden establecer túneles de paquetes <b>IPv6</b> hacia un direccionador <b>IPv6</b> o <b>IPv4</b> intermedio que se pueda alcanzar a través de una infraestructura de <b>IPv4</b> . Este tipo de túnel abarca el primer segmento de la vía de acceso de extremo a extremo del paquete.
Sistema principal a sistema principal	Los sistemas principales <b>IPv6</b> o <b>IPv4</b> que están interconectados por una infraestructura <b>IPv4</b> pueden establecer túneles de paquetes <b>IPv6</b> entre dichos paquetes. En este caso, el túnel abarca la vía de acceso entera de extremo a extremo que toma el paquete.
Direccionador a sistema principal	Los direccionadores <b>IPv6/IPv4</b> pueden establecer túneles de paquetes <b>IPv6</b> hasta el sistema principal <b>IPv6</b> o <b>IPv4</b> de destino final. Este túnel sólo abarca el último segmento de la vía de acceso de extremo a extremo.

Las técnicas de tunelización se suelen clasificar de acuerdo con el mecanismo mediante el cual el nodo de encapsulación determina la dirección del nodo al final del túnel. En los métodos de direccionador a direccionador o de sistema principal a direccionador, el paquete **IPv6** se envía por el túnel a un direccionador. En los métodos de sistema principal a sistema principal o de direccionador a sistema principal, el paquete **IPv6** se envía por el túnel directamente hasta el destino final.

El nodo de entrada del túnel (el nodo de encapsulación) crea una cabecera **IPv4** de encapsulación y transmite el paquete encapsulado. El nodo de salida del túnel (el nodo de desencapsulación) recibe el paquete encapsulado, elimina la cabecera **IPv4**, actualiza la cabecera **IPv6** y procesa el paquete **IPv6** recibido. Sin embargo, el nodo de encapsulación necesita mantener información de estado flexible para cada túnel, por ejemplo la unidad máxima de transmisión (MTU) del túnel, para procesar paquetes **IPv6** reenviados al túnel.

Existen dos tipos de túneles en **IPv6**:

### túneles automáticos

Los túneles automáticos se configuran utilizando la información de dirección **IPv4** incorporada en una dirección **IPv6** – la dirección **IPv6** del sistema principal de destino incluye información sobre la dirección **IPv4** a la que se debe enviar el paquete a través del túnel.

### túneles configurados

Los túneles configurados se deben configurar manualmente. Estos túneles se utilizan cuando se emplean direcciones **IPv6** que no tienen ninguna información **IPv4** incorporada. Se deben especificar las direcciones **IPv6** e **IPv4** de los puntos finales del túnel.

Para obtener información sobre cómo configurar túneles automáticos y túneles configurados, consulte el apartado “Configuración de la tunelización en IPv6” en la página 145.

### **Soporte local de enlace y local de sitio de varios inicios de IPv6**

Un sistema principal puede tener definida más de una interfaz. Un sistema principal con dos o más interfaces activas se conoce como sistema principal de varios inicios. Cada interfaz tiene una dirección local de enlace asociada a ella.

Las direcciones locales de enlace son suficientes para permitir las comunicaciones entre los nodos conectados al mismo enlace.

Un sistema principal de varios inicios tiene dos o más direcciones locales de enlace asociadas. La implementación de AIX **IPv6** tiene 4 opciones para manejar el modo en que se resuelve la resolución de direcciones de la capa de enlace en sistemas principales de varios inicios. La opción 1 es el valor predeterminado.

<b>Item</b>	<b>Descripción</b>
<b>Opción 0</b>	No se realiza ninguna acción de varios inicios. Las transmisiones salen en la primera interfaz local de enlace. Cuando el protocolo <b>Neighbor Discovery Protocol (NDP - Protocolo de descubrimiento de vecino)</b> debe realizar la resolución de direcciones, efectúa una multidifusión de un mensaje de Solicitud de vecino en cada interfaz con una dirección local de enlace definida. NDP pone en cola el paquete de datos hasta que se recibe el primer mensaje de Aviso de vecino. Entonces el paquete de datos se envía en este enlace.
<b>Opción 1</b>	Cuando el <b>NDP</b> debe realizar la resolución de direcciones, es decir, cuando envía un paquete de datos a un destino y la información de capa de enlace para el siguiente salto no está en la Antememoria de vecino, realiza una multidifusión de un mensaje de Solicitud de vecino a cada interfaz con una dirección local de enlace definida. Entonces <b>NDP</b> pone en cola el paquete de datos hasta que obtiene la información de capa de enlace. A continuación, <b>NDP</b> espera hasta que se recibe una respuesta para cada interfaz. Esto garantiza que los paquetes de datos se envíen en las interfaces de salida apropiadas. Si <b>NDP</b> no ha esperado, pero ha respondido al primer Aviso de vecino recibido, será posible enviar un paquete de datos en un enlace no asociado con la dirección de origen de paquete. Dado que <b>NDP</b> debe esperar, se produce un retardo en el primer paquete que se envía. Sin embargo, el retardo se produce de todos modos al esperar la primera respuesta.
<b>Opción 2</b>	Se permite la operación de varios inicios, pero el despacho de un paquete de datos está limitado a la interfaz especificada por <code>main_if6</code> . Cuando el <b>NDP</b> debe realizar la resolución de direcciones, efectúa una multidifusión de un mensaje de Solicitud de vecino en cada interfaz con una dirección local de enlace definida. Entonces espera un mensaje de Aviso de vecino de la interfaz especificada por <code>main_if6</code> (consulte el mandato <code>no</code> ). Al recibir una respuesta de esta interfaz, el paquete de datos se envía en este enlace.
<b>Opción 3</b>	Se permite la operación de varios inicios, pero el despacho de un paquete de datos está limitado a la interfaz especificada por <code>main_if6</code> y las direcciones locales de sitio sólo se dirigen para la interfaz especificada por <code>main_site6</code> (consulte el mandato <code>no</code> ). El NDP funciona exactamente igual que para la Opción 2. Para las aplicaciones que dirigen paquetes de datos utilizando direcciones locales de sitio en un sistema principal de varios inicios, sólo se utilizan las direcciones locales de sitio especificadas por <code>main_site6</code> .

### **Actualización a IPv6 con IPv4 configurado**

Este ejemplo le llevará por los pasos necesarios para realizar una actualización manual de **IPv4 a IPv6**.

La red utilizada en este ejemplo consta de un router y dos subredes. Hay dos sistemas principales en cada subred: el router y otro sistema principal. Deberá actualizar la máquina en esta red a

**IPv6.** Al final del ejemplo, el direccionador anunciará el prefijo 3ffe:0:0:aaaa:: /64 en la interfaz de red en0 y el prefijo 3ffe:0:0:bbbb:: /64 en la interfaz de red en1. En primer lugar, deberá configurar las máquinas para dar soporte temporal a **IPv6** para poderlas probar. A continuación, deberá configurar las máquinas para estén preparadas para **IPv6** en tiempo de arranque.

Si está ejecutando el sistema operativo AIX y no tiene los valores de **IPv4** configurados, consulte el apartado “Actualización a IPv6 con IPv4 no configurado” en la página 141.

#### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

#### Paso 1: Configurar los sistemas principales para IPv6

En los sistemas principales en ambas subredes, realice lo siguiente:

1. Asegúrese de que **IPv4** está configurado escribiendo el siguiente mandato:

```
netstat -ni
```

Los resultados deberían ser similares a los siguientes:

Name	Mtu	Network	Address	Ipkts	Ierr	Opkts	Oerr	Coll
en0	1500	link#2	0.6.29.4.55.ec	279393	0	2510	0	0
en0	1500	9.3.230.64	9.3.230.117	279393	0	2510	0	0
lo0	16896	link#1		913	0	919	0	0
lo0	16896	127	127.0.0.1	913	0	919	0	0
lo0	16896	::1		913	0	919	0	0

2. Con autorización de usuario root, configure los valores de **IPv6** escribiendo el mandato siguiente:

```
autoconf6
```

3. Vuelva a ejecutar el siguiente mandato:

```
netstat -ni
```

Los resultados deberían ser similares a los siguientes:

Name	Mtu	Network	Address	Ipkts	Ierr	Opkts	Oerr	Coll
en0	1500	link#2	0.6.29.4.55.ec	279679	0	2658	0	0
en0	1500	9.3.230.64	9.3.230.117	279679	0	2658	0	0
en0	1500	fe80::206:29ff:fe04:55ec		279679	0	2658	0	0
sit0	1480	link#3	9.3.230.117	0	0	0	0	0
sit0	1480	::9.3.230.117		0	0	0	0	0
lo0	16896	link#1		2343	0	2350	0	0
lo0	16896	127	127.0.0.1	2343	0	2350	0	0
lo0	16896	::1		2343	0	2350	0	0

4. Inicie el daemon **ndpd-host** escribiendo el siguiente mandato:

```
startsrc -s ndpd-host
```

#### Paso 2: Configurar el direccionador para IPv6

1. Asegúrese de que los valores de **IPv4** están configurados escribiendo el siguiente mandato:

```
netstat -ni
```

2. Con autorización de usuario root, escriba el siguiente mandato:

```
autoconf6
```

3. Configure manualmente las direcciones globales en las interfaces del direccionador que pertenecen a cada una de las dos subredes, escribiendo los mandatos siguientes:

```
# ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
# ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
```

Deberá realizarlo para cada subred al que el direccionador le está enviando paquetes.

4. Para activar el reenvío de IPv6, escriba lo siguiente:

```
no -o ip6forwarding=1
```

5. Para iniciar el daemon **ndpd-router**, escriba lo siguiente:

```
startsrc -s ndpd-router
```

El daemon **ndpd-router** anunciará prefijos correspondientes a las direcciones globales que haya configurado en el direccionador. En este caso, ndpd-router anunciará el prefijo 3ffe:0:0:aaaa::/64 en en0 y el prefijo 3ffe:0:0:bbbb::/64 en en1

### Paso 3. Poner a punto IPv6 para configurarlo en los sistemas principales en tiempo de arranque

**IPv6** quedará suprimido cuando vuelva a arrancar la máquina. Para habilitar la funcionalidad del sistema principal **IPv6** cada vez que vuelva a arrancar, realice las acciones siguientes:

1. Abra el archivo /etc/rc.tcpip mediante el editor de texto favorito.
2. Elimine los comentarios de las líneas siguientes en dicho archivos:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

```
# Start up ndpd-host daemon
start /usr/sbin/ndpd-host "$src_running"
```

3. Añada el distintivo **-A** a start /usr/sbin/autoconf6 "":

```
start /usr/sbin/autoconf6 "" -A
```

Cuando vuelva a arrancar, se habrá realizado la configuración de **IPv6**. Repita este proceso para cada sistema principal.

### Paso 4: Poner a punto IPv6 para configurarlo en el direccionador en tiempo de arranque

El sistema principal **IPv6** que acaba de configurar se suprimirá cuando rearanneque la máquina. Para habilitar la funcionalidad del direccionador **IPv6** cada vez que rearanneque, realice lo siguiente:

1. Abra el archivo /etc/rc.tcpip en el editor de texto favorito.
2. Elimine los comentarios de la línea siguiente en dicho archivo:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

3. Añada las líneas siguientes inmediatamente después de la línea que acaba de descomentar en el paso anterior:

```
# Configure global addresses for router
ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
```

En este caso, nuestra red sólo contiene dos subredes, en0 y en1. Deberá añadir una línea a este archivo para cada subred a la que el direccionador le esté enviando paquetes.

4. Elimine los comentarios de la línea siguiente en el archivo:

```
# Start up ndpd-router daemon
start /usr/sbin/ndpd-router "$src_running"
```

Cuando vuelva a arrancar la máquina, **IPv6** se iniciará automáticamente.

## Actualización a IPv6 con IPv4 no configurado

En este ejemplo se muestra cómo configurar sistemas principales y un direccionador para **IPv6** sin los valores de **IPv4** configurados.

La red utilizada en este ejemplo consta de un direccionador y dos subredes. Hay dos sistemas principales en cada subred: el direccionador y otro sistema principal. Al final del caso, el direccionador anunciará el prefijo `3ffe:0:0:aaaa::` /64 en la interfaz de red en0 y el prefijo `3ffe:0:0:bbbb::` /64 en la interfaz de red en1. En primer lugar, deberá configurar las máquinas para dar soporte temporal a **IPv6** para poderlas probar. A continuación, deberá configurar las máquinas para que estén preparadas para IPv6 en tiempo de arranque.

En este caso se presupone que el catálogo de archivos `bos.net.tcp.client` está instalado.

Para actualizar a **IPv6** teniendo ya configurado **IPv4**, consulte el apartado “[Actualización a IPv6 con IPv4 configurado](#)” en la página 138.

### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

## Paso 1: Configurar los sistemas principales para IPv6

1. Con autorización de usuario root, escriba el mandato en cada sistema principal de la subred:

```
autoconf6 -A
```

Se activarán todas las interfaces con capacidad **IPv6** en el sistema.

**Nota:** Para activar un subconjunto de interfaces, utilice el distintivo **-i**. Por ejemplo, `autoconf6 -i en0 en1` activará las interfaces en0 y en1.

2. Escriba el mandato siguiente para ver las interfaces:

```
netstat -ni
```

Los resultados deberían ser similares a los siguientes:

Name	Mtu	Network	Address	Ipkts	Ierrrs	Opkts	Oerrrs	Coll
en0	1500	link#3	0.4.ac.17.b4.11	7	0	17	0	0
en0	1500	fe80::204:acff:fe17:b411		7	0	17	0	0
lo0	16896	link#1		436	0	481	0	0
lo0	16896	127	127.0.0.1	436	0	481	0	0
lo0	16896	::1		436	0	481	0	0

3. Inicie el daemon **ndpd-host** escribiendo el siguiente mandato:

```
startsrc -s ndpd-host
```

## Paso 2: Configurar el direccionador para IPv6

1. Con autorización de usuario root, escriba el siguiente mandato en el sistema principal del direccionador:

```
autoconf6 -A
```

Se activarán todas las interfaces con capacidad **IPv6** en el sistema.

**Nota:** Para activar un subconjunto de interfaces, utilice el distintivo **-i**. Por ejemplo, `autoconf6 -i en0 en1` activará las interfaces en0 y en1.

Los resultados deberían ser similares a los siguientes:

Name	Mtu	Network	Address	Ipkts	Ierrrs	Opkts	Oerrrs	Coll
en1	1500	link#2	0.6.29.dc.15.45	0	0	7	0	0
en1	1500	fe80::206:29ff:fedc:1545		0	0	7	0	0
en0	1500	link#3	0.4.ac.17.b4.11	7	0	17	0	0

en0	1500	fe80::204:acff:fe17:b411	7	0	17	0	0
lo0	16896	link#1	436	0	481	0	0
lo0	16896	127 127.0.0.1	436	0	481	0	0
lo0	16896	::1	436	0	481	0	0

2. Configure manualmente las direcciones globales en las interfaces del directorio que pertenecen a cada una de las dos subredes, escribiendo los mandatos siguientes:

```
# ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
# ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
```

**Nota:** Deberá realizarlo para cada subred al que el directorio le está enviando paquetes.

3. Para activar el reenvío de **IPv6**, escribe lo siguiente:

```
no -o ip6forwarding=1
```

4. Para iniciar el daemon **ndpd-router**, escriba lo siguiente:

```
startsrc -s ndpd-router
```

El daemon **ndpd-router** anunciará prefijos correspondientes a las direcciones globales que haya configurado en el directorio. En este caso, el daemon ndpd-router anunciará el prefijo 3ffe:0:0:aaaa::/64 en en0 y el prefijo 3ffe:0:0:bbbb::/64 en en1.

5. Pulse Intro para continuar.

6. Pulse Intro una segunda vez para confirmar la decisión e iniciar la instalación del paquete de software.

### Paso 3. Poner a punto IPv6 para configurarlo en los sistemas principales en tiempo de arranque

Cuando haya completado el Paso 1 para cada sistema principal, **IPv6** se suprimirá cuando vuelva a arrancar la máquina. Para habilitar la funcionalidad del sistema principal **IPv6** cada vez que vuelva a arrancar, realice las acciones siguientes:

1. Abra el archivo /etc/rc.tcpip mediante el editor de texto favorito.
2. Elimine los comentarios de las líneas siguientes en dicho archivo:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

```
# Start up ndpd-host daemon
start /usr/sbin/ndpd-host "$src_running"
```

3. Añada el distintivo **-A** a start /usr/sbin/autoconf6 "":

```
start /usr/sbin/autoconf6 "" -A
```

4. Repita este proceso para cada sistema principal.

Cuando vuelva a arrancar la máquina, **IPv6** se iniciará automáticamente.

### Paso 4: Poner a punto IPv6 para configurarlo en el directorio en tiempo de arranque

Cuando haya completado el Paso 2 para el directorio, **IPv6** se suprimirá cuando rearrene. Para habilitar la funcionalidad del directorio **IPv6** cada vez que rearrene, realice lo siguiente:

1. Abra el archivo /etc/rc.tcpip en el editor de texto favorito.
2. Elimine los comentarios de la línea siguiente en dicho archivo:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

3. Añada el distintivo **-A** a esa línea:

```
start /usr/sbin/autoconf6 "" -A
```

4. Añada las líneas siguientes inmediatamente después de la línea que acaba de descomentar en el paso anterior:

```
# Configure global addresses for router
ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
```

En este caso, nuestra red sólo contiene dos subredes, en0 y en1. Deberá añadir una línea a este archivo para cada subred a la que el direccionador le esté enviando paquetes.

5. Elimine los comentarios de la línea siguiente en el archivo:

```
# Start up ndpd-router daemon
start /usr/sbin/ndpd-router "$src_running"
```

6. Ejecute el mandato siguiente para habilitar el reenvío de IP en tiempo de arranque:

```
no -r -o ip6forwarding=1
```

Cuando vuelva a arrancar la máquina, **IPv6** se iniciará automáticamente.

### **Configuración de la interfaz de IPv6 en un sistema principal**

Este caso de ejemplo le guiará a través de la configuración del tiempo de ejecución de un nodo utilizando IP estáticas y rutas.

La red que se utiliza en este ejemplo consta de un sistema principal y de un direccionador. Al final de este caso de ejemplo, se configurará una interfaz IPv6 en el sistema principal. Configure en primer lugar las máquinas para que soporten temporalmente IPv6 para que se puedan probar. A continuación, configure las máquinas para que estén listas para IPv6 en el momento del arranque.

#### **Cuestiones que deben tenerse en cuenta**

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.
- El ejemplo presupone que **2001:1:2::/48** es la Aggregate Global Unicast Address para la interfaz IPv6 asignada por la IANA (Internet Assigned Numbers Authority) al proveedor. Y **2001:1:2:3:4::/64** es la subred que utiliza los bits 49 - 64 asignados por el administrador de red.
- Debe hacer referencia a RFC 3587 para comprender el Global Unicast Address Format de IPv6.

#### **Paso 1. Configuración de los sistemas principales para IPv6**

Siga este procedimiento para configurar sistemas principales para IPv6.

1. Con la autorización de root, configure los valores de IPv6 especificando el siguiente mandato:

```
# autoconf6
```

2. Vuelva a ejecutar el siguiente mandato:

```
# netstat -ni
```

Los resultados deben ser similares al resultado siguiente:

Name	Mtu	Network	Address	Ipkts	Ierrrs	Opkts	Oerrrs	Coll
en0	1500	link#2	0.6.29.4.55.ec	279679	0	2658	0	0
en0	1500	9.3.230.64	9.3.230.117	279679	0	2658	0	0
en0	1500	fe80::206:29ff:fe04:55ec		279679	0	2658	0	0
sit0	1480	link#3	9.3.230.117	0	0	0	0	0
sit0	1480	::9.3.230.117		0	0	0	0	0
lo0	16896	link#1		2343	0	2350	0	0
lo0	16896	127	127.0.0.1	2343	0	2350	0	0
lo0	16896	::1		2343	0	2350	0	0

3. Utilice el mandato **chdev** para añadir la dirección IPv6 a la interfaz del host. Para este ejemplo, los 64 bits de orden bajo se toman de los 64 bits de orden bajo de la IP de enlace local generada por **autoconf6** en la interfaz **en0**.

```
# chdev -l en0 -a netaddr6='2001:2:3:4:206:29ff:fe04:55ec' -a prefixlen=64
```

4. Suprima cualquier ruta de enlace de prefijo existente para el prefijo siguiente:

```
# route delete -inet6 2001:2:3:4::/64
```

5. Configure la ruta estática del prefijo en el sistema principal para añadir la posibilidad de alcance para el direccionador, donde **fe80::206:29ff:fe04:66e** es el direccionador o una pasarela que tiene conectividad con el direccionador.

```
# route add -inet6 -net 2001:2:3:4::/64 fe80::206:29ff:fe04:66e -static
```

**Nota:** Si es necesario un cambio para la ruta predeterminada, asegúrese de que **autoconf6** se ejecuta con la opción **-R** que le impide añadir o sobrescribir cualquier ruta predeterminada en el nodo. A continuación, repita los pasos 3-5.

## Paso 2. Configuración del direccionador para IPv6

Siga este procedimiento para configurar el direccionador para IPv6.

1. Compruebe para asegurarse de que se han configurado los valores de IPv4, especificando el mandato siguiente:

```
# netstat -ni
```

2. Con autorización de root, escriba el siguiente mandato:

```
# autoconf6
```

3. Para activar el reenvío de IPv6, especifique el mandato siguiente:

```
# no -o ip6forwarding=1
```

4. Configure la IP global en la interfaz del direccionador, especificando el mandato siguiente:

```
# chdev -l en0 -a netaddr6='2001:4:5:6:207:30ff:fe05:66ec' -a prefixlen=64
```

5. Configure manualmente rutas en el direccionador para habilitar la entrega precisa de paquetes. Por ejemplo, si **fe80:: 3ca6:70ff:fe00:3004/64** es la pasarela para el prefijo **2001:2:3:4::/64**, añada una ruta de prefijo como se indica a continuación:

```
# route add -inet6 -net 2001:2:3:4::/64 fe80::3ca6:70ff:fe00:3004 -static
```

## Paso 3. Configuración de IPv6 para que se configure en sistemas principales en cada reinicio

Los valores del sistema principal IPv6 configurados en el **Paso 1. Configuración del sistema principal para IPv6** se suprimen al reiniciar la máquina. Para habilitar la funcionalidad de sistemas principales de IPv6 cada vez que reinicie la máquina, siga este procedimiento.

1. Abra el archivo **/etc/rc.tcpip** en un editor de texto.
2. Elimine los comentarios de la línea siguiente en el archivo **/etc/rc.tcpip**:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

**Nota:** Si la línea anterior no está presente en el archivo **/etc/rc.tcpip**, añádala en el archivo.

3. Añada el distintivo **-A** a **start /usr/sbin/autoconf6 ""**.

```
start /usr/sbin/autoconf6 "" -A
```

4. Añada la línea siguiente en el archivo **/etc/rc.tcpip** después de la línea de la que ha eliminado la marca de comentario (o que ha añadido):

```
chdev -l en0 -a netaddr6='2001:2:3:4:206:29ff:fe04:55ec' -a prefixlen=64
```

5. Suprima las rutas de prefijo existentes previamente, especificando el mandato siguiente:

```
chdev -l inet0 -a delrout6='-net, 2001:2:3:4::/64'
```

6. Configure una ruta, especificando el mandato siguiente:

```
chdev -l inet0 -a rout6='-net, 2001:2:3:4::/64 ,fe80::206:29ff:fe04:66e,-static'
```

#### Paso 4. Configuración de IPv6 para que se configure en el directorio en cada reinicio

Los valores del directorio IPv6 configurados en el **Paso 2. Configuración del directorio para IPv6** se suprimen al reiniciar la máquina. Para habilitar la funcionalidad del directorio IPv6 cada vez que reinicie la máquina, siga este procedimiento.

1. Abra el archivo **/etc/rc.tcpip** en un editor de texto.

2. Elimine los comentarios de la siguiente línea en el archivo **/etc/rc.tcpip**:

```
# Start up autoconf6 process
start /usr/sbin/autoconf6 ""
```

**Nota:** Si la línea anterior no está presente en el archivo **/etc/rc.tcpip**, añádala en el archivo.

3. Añada el distintivo **-A** a **start /usr/sbin/autoconf6 ""**.

```
start /usr/sbin/autoconf6 "" -A
```

4. Añada las líneas siguientes después de la línea de la que ha eliminado la marca de comentario (o añadido) en el paso 2 para configurar la IP Global en el directorio y para configurar la ruta del prefijo.

```
chdev -l en0 -a netaddr6='2001:4:5:6:207:30ff:fe05:66ec' -a prefixlen=64
chdev -l inet0 -a rout6='-net,2001:2:3:4::/64,fe80::3ca6:70ff:fe00:3004,-static'
```

En este caso de ejemplo, la red sólo tiene una subred, **en0**. Debe añadir una línea a este archivo para cada subred a la que el directorio envía paquetes.

#### Configuración de la tunelización en IPv6

Puede elegir entre dos métodos para configurar la tunelización en IPv6. El primero configura un túnel automático. El segundo establece un túnel configurado.

#### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

#### Configurar un túnel automático en IPv6

En este caso, se utilizará el mandato **autoconf6** para configurar IPv6 y configurar un túnel automático mediante la interfaz primaria, en2. A continuación, se utilizará el mandato **autoconf6** para configurar un túnel mediante la interfaz secundaria, en0.

A continuación, viene el resultado del mandato **netstat -ni** que muestra la configuración actual de la red del sistema:

en0	1500	link#2	MAC address here	0	0	33	0	0
en0	1500	1.1	1.1.1.3	0	0	33	0	0
en2	1500	link#3	MAC address here	79428	0	409	0	0
en2	1500	10.1	10.1.1.1	79428	0	409	0	0

- Para habilitar IPv6 y un túnel automático, escriba el siguiente mandato:

```
autoconf6
```

La ejecución del mandato **netstat -ni** produce ahora los resultados siguientes:

```
# netstat -in
en0 1500 link#2      MAC address here      0    0    33    0    0
en0 1500 1.1          1.1.1.3                0    0    33    0    0
en0 1500 fe80::204:acff:fe49:4910        0    0    33    0    0
en2 1500 link#3      MAC address here      79428 0    409    0    0
en2 1500 10.1         10.1.1.1              79428 0    409    0    0
en2 1500 fe80::220:35ff:fe12:3ae8        0    0    0    0    0
sit0 1480 link#7      10.1.1.1              0    0    0    0    0
sit0 1480 ::10.1.1.1                  0    0    0    0    0
```

Si en2 (dirección IP 10.1.1.1) es la interfaz primaria, la dirección ::10.1.1.1 estará ahora disponible para la tunelización automática a través de la interfaz en2.

- Para habilitar un túnel automático mediante la interfaz en0, escriba el siguiente mandato:

```
autoconf6 -s -i en0
```

La ejecución del mandato **netstat -ni** produce ahora los resultados siguientes:

```
# netstat -in
en0 1500 link#2      MAC address here      0    0    33    0    0
en0 1500 1.1          1.1.1.3                0    0    33    0    0
en0 1500 fe80::204:acff:fe49:4910        0    0    33    0    0
en2 1500 link#3      MAC address here      79428 0    409    0    0
en2 1500 10.1         10.1.1.1              79428 0    409    0    0
en2 1500 fe80::220:35ff:fe12:3ae8        0    0    0    0    0
sit0 1480 link#7      1.1.1.3                0    0    3    0    0
sit0 1480 ::10.1.1.1                  0    0    3    0    0
sit0 1480 ::1.1.1.3                  0    0    3    0    0
```

Con esta acción se consigue que una dirección IPv6 compatible con IPv4 se añada a la interfaz SIT existente, sit0. Ahora la tunelización está habilitada para la interfaz en0 mediante la dirección ::1.1.1.3. Se utilizará la misma interfaz, sit0, para ambos túneles.

**Nota:** Los túneles automáticos se suprinen cuando se reinicia el sistema. Para que el túnel automático esté presente en tiempo de arranque, añada los argumentos necesarios al mandato **autoconf6** en el archivo /etc/rc.tcpip.

### Configurar túneles configurados

En este caso, se utilizará SMIT para establecer un túnel configurado. Este túnel estará disponible cuando se reinicie el sistema porque se almacenará en ODM. Se configurará un túnel entre los sistemas alpha y beta. La dirección IPv4 de alpha es 10.1.1.1 y la dirección IPv4 de beta es 10.1.1.2.

Para establecer túneles configurados, siga estos pasos:

1. Para configurar un túnel entre alpha y beta, escriba lo siguiente en ambos sistemas:

```
smit ctinet6
```

2. Seleccione **Añadir una IPV6 en Interfaz de Túnel IPV4** en ambos sistemas.

```
autoconf6
```

3. En este caso, hemos rellenado los valores tal como se indica en alpha, basándonos en las direcciones IPv4:

```
* IPV4 SOURCE ADDRESS (decimal con puntos)      [10.1.1.1]
* IPV4 DESTINATION ADDRESS (decimal con puntos)   [10.1.1.2]
IPV6 SOURCE ADDRESS (separado por dos puntos)     []
IPV6 DESTINATION ADDRESS (separado por dos puntos) []
```

En beta, se han especificado los valores siguientes:

```
* IPV4 SOURCE ADDRESS (decimal con puntos)      [10.1.1.2]
* IPV4 DESTINATION ADDRESS (decimal con puntos)   [10.1.1.1]
  IPV6 SOURCE ADDRESS (separado por dos puntos)    []
  IPV6 DESTINATION ADDRESS (separado por dos puntos) []
```

4. Para ver las interfaces configuradas, escriba el siguiente mandato:

```
ifconfig ctiX
```

donde X es el número de la interfaz. En este caso, se han devuelto los resultados siguientes: En alpha:

```
cti0: flags=8080051<UP,POINTOPOINT,RUNNING,MULTICAST>
      inet6 fe80::a01:101/128 --> fe80::a01:102
```

En beta:

```
cti0: flags=8080051 <UP,POINTOPOINT,RUNNING,MULTICAST>
      inet6 fe80::a01:102/128 --> fe80::a01:101
```

La SMIT crea automáticamente las direcciones IPv6 para ambos extremos del túnel utilizando el método siguiente:

- Los 32 bits inferiores contienen la dirección IPv4
- Los 96 bits superiores contienen el prefijo fe80::/96

Puede llenar direcciones IPv6 específicas, si lo desea.

### Rastreo de paquetes

El rastreo de paquetes es el proceso mediante el cual puede verificar la vía de acceso a través de las capas hasta el destino.

El mandato **iptrace** realiza el rastreo de paquetes de nivel de interfaz de red. El mandato **ipreport** emite salida en el rastreo de paquetes en formato hexadecimal y ASCII. El mandato **trpt** realiza el seguimiento de paquetes de nivel de protocolo de transporte para **TCP**. La salida de mandato **trpt** es más detallada, incluida la información sobre la hora, el estado de **TCP** y la secuencia de paquetes.

### Cabeceras de paquete de interfaz de red

En la capa de Interfaz de red, se adjuntan cabeceras de paquete a los datos de salida.

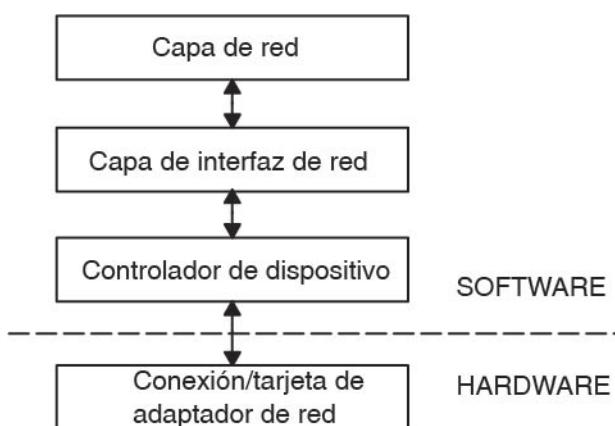


Figura 8. Flujo de paquetes a través de la Estructura de interfaz de red

Esta ilustración muestra el flujo de datos bidireccional a través de las capas de la Estructura de interfaz de red. Empezando desde la parte superior (software), son la Capa de red, la Capa de interfaz de red, el Controlador de dispositivo y (hardware) la Conexión o la Tarjeta adaptadora de red.

Entonces los paquetes se envían a través del adaptador de red a la red apropiada. Los paquetes pasan por muchas pasarelas antes de alcanzar los destinos. En la red de destino, las cabeceras se separan de los paquetes y se envían los datos al sistema principal apropiado.

El apartado siguiente contiene información de cabeceras de paquete para varias de las interfaces de red más comunes.

#### **Cabeceras de trama para los adaptadores Ethernet**

Una cabecera de trama **IP (Internet Protocol)** o **(ARP) (Protocolo de resolución de dirección)** para el adaptador Ethernet está formada por los tres campos siguientes.

Tabla 56. Cabecera de trama para un adaptador Ethernet		
Campo	Longitud	Definición
DA	6 bytes	Dirección de destino.
SA	6 bytes	Dirección de origen. Si el bit 0 de este campo está establecido en 1, ello indica la existencia de información de direccionamiento (RI).
Tipo	2 bytes	Especifica si el paquete es <b>IP</b> o <b>ARP</b> . Los valores numéricos para cada tipo se indican a continuación.

Números para el campo Tipo:

Item	Descripción
IP	0800
ARP	0806

#### **Cabeceras de trama de Red en anillo**

Hay cinco campos que constan de la cabecera de control de accesos al medio (MAC) para el adaptador de Red en anillo.

Tabla 57. Cabecera MAC de Red en anillo		
Campo	Longitud	Definición
AC	1 byte	Control de accesos. El valor de este campo x `00' proporciona la prioridad de cabecera 0.
FC	1 byte	Control de campo. El valor de este campo x `40' especifica la trama de Control de enlace lógico.
DA	6 bytes	Dirección de destino.
SA	6 bytes	Dirección de origen. Si el bit 0 de este campo está establecido en 1, ello indica la existencia de información de direccionamiento (RI).
RI	18 bytes	Información de direccionamiento. Los campos válidos se describen más abajo.

La cabecera MAC consta de dos campos de información de direccionamiento de dos bytes cada uno: control de direccionamiento (RC) y números de segmento. Se puede utilizar un máximo de ocho números de segmento para especificar destinatarios de una difusión limitada. La información de RC está contenida en los bytes 0 y 1 del campo RI. Los valores de los dos primeros bits del campo RC tienen los significados siguientes:

<b>Item</b>	<b>Descripción</b>
<b>bit (0) = 0</b>	Utilizar la ruta que no es de difusión especificada en el campo RI.
<b>bit (0) = 1</b>	Crear el campo RI y difundir a todos los anillos.
<b>bit (1) = 0</b>	Difundir a través de todos los puentes.
<b>bit (1) = 1</b>	Difundir a través de puentes limitados.

La cabecera de control de enlace lógico (LLC) está compuesta de cinco campos, como se muestra en la tabla de cabecera LLC siguiente.

<i>Tabla 58. Cabecera LLC 802.3</i>		
<b>Campo</b>	<b>Longitud</b>	<b>Definición</b>
DSAP	1 byte	Punto de acceso de servicio de destino. El valor de este campo es x`aa'.
SSAP	1 byte	Punto de acceso de servicio de origen. El valor de este campo es x`aa'.
CONTROL	1 byte	Determina los mandatos LLC y las respuestas. Más abajo se describen los tres valores posibles para este campo.
PROT_ID	3 bytes	ID de protocolo. Este campo está reservado. Tiene un valor de x`0'.
TYPE	2 bytes	Especifica si el paquete es <b>IP</b> o <b>ARP</b> .

#### *Valores de campo de control*

Los campos de control de Red en anillo incluyen una trama de información sin número, una trama de identificación de intercambio y una trama de prueba. Aquí se describen los valores.

<b>Item</b>	<b>Descripción</b>
x`03'	Trama de información sin número (UI). Es el modo normal, o sin secuencia, en el que se transmiten los datos de adaptador de red en anillo a través de la red. <b>TCP/IP</b> secuencia los datos.
x`AF'	Trama de identificación de intercambio (XID). Esta trama transmite las características del sistema principal de envío.
x`E3'	Trama de prueba. Esta trama soporta las pruebas de la vía de acceso de transmisión, volviendo a hacer eco de los datos que se reciben.

#### *Cabeceras de trama para 802.3*

La cabecera MAC para el adaptador 802.3 está formada por dos campos, tal como se muestra en la tabla de cabeceras de MAC.

Tabla 59. Cabecera MAC para 802.3

Campo	Longitud	Definición
DA	6 bytes	Dirección de destino.
SA	6 bytes	Dirección de origen. Si el bit 0 de este campo está establecido en 1, ello indica la existencia de información de direccionamiento (RI).

La cabecera LLC para 802.3 es igual que la cabecera MAC para Red en anillo.

### Protocolos a nivel de red Internet

Los protocolos a nivel de red Internet manejan las comunicaciones de máquina a máquina.

En otras palabras, esta capa implementa el direccionamiento **TCP/IP**. Estos protocolos aceptan peticiones de enviar paquetes (junto con la dirección de red de la máquina de destino) de la capa de transporte, convertir los paquetes a formato de datagrama y enviarlos hacia abajo a la capa de interfaz de red para su proceso adicional.

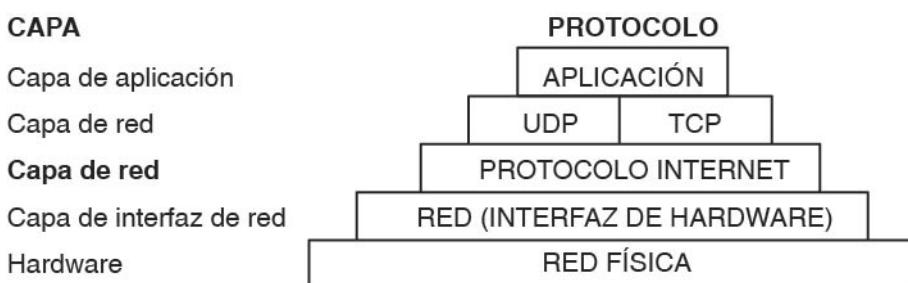


Figura 9. Capa de red del conjunto de protocolos de TCP/IP

Esta ilustración muestra las diversas capas del conjunto de protocolos de **TCP/IP**. Desde la parte superior, la capa de aplicaciones consta de la aplicación. La capa de transporte contiene **UDP** y **TCP**. La capa de red contiene la interfaz de red (hardware). Y finalmente, la capa de hardware contiene la red física.

**TCP/IP** proporciona los protocolos que son necesarios para satisfacer los requisitos de la RFC 1100, *Protocolos oficiales de Internet*, así como otros protocolos utilizados comúnmente por los sistemas principales de la comunidad de Internet.

**Nota:** El uso de los números de red, versión, socket, servicio y protocolo de Internet en **TCP/IP** también satisface los requisitos de la RFC 1010, *Números asignados*.

### **Address Resolution Protocol (Protocolo de resolución de direcciones)**

El primer protocolo a nivel de red es el **ARP (Address Resolution Protocol - Protocolo de resolución de direcciones)**. **ARP** convierte dinámicamente las direcciones de Internet en las direcciones de hardware exclusivas de las redes de área local.

Para ilustrar cómo funciona **ARP**, examine dos nodos, X y Y. Si el nodo X desea comunicarse con Y y X e Y están en redes de área local (LAN) diferentes, X e Y se comunican a través de *puentes*, *direcccionadores* o *pasarelas*, utilizando direcciones IP. En una LAN, los nodos se comunican utilizando direcciones de hardware de bajo nivel.

Los nodos del mismo segmento de la misma LAN utilizan **ARP** para determinar la dirección de hardware de otros nodos. En primer lugar, el nodo X difunde una petición **ARP** para la dirección de hardware del nodo Y. La petición **ARP** contiene las direcciones **IP** y de hardware de X y la dirección **IP** de Y. Cuando Y recibe la petición **ARP**, pone una entrada para X en la antememoria de **ARP** (que se utiliza para correlacionar rápidamente de la dirección IP a la dirección de hardware) y, a continuación responde directamente a X con una respuesta de **ARP** que contiene las direcciones **IP** y de hardware de Y. Cuando el nodo X recibe la respuesta **ARP** de Y, pone una entrada para Y en la antememoria de **ARP**.

Una vez que existe una entrada de antememoria **ARP** en X para Y, el nodo X puede de enviar paquetes directamente a Y sin recurrir otra vez a **ARP** (a menos que se suprima la entrada de antememoria de **ARP** para Y, en cuyo caso se vuelve a utilizar **ARP** para contactar con Y).

A diferencia de la mayoría de protocolos, los paquetes **ARP** no tienen cabeceras de formato fijo. En lugar de ello, el mensaje está diseñado para ser útil con diferentes tecnologías de red, tales como:

- Adaptador LAN Ethernet (soporta los protocolos Ethernet y 802.3)
- Adaptador de Red en anillo
- Adaptador de red FDDI (Fiber Distributed Data Interface - Interfaz de datos distribuidos por fibra)

Sin embargo, ARP no convierte direcciones para **SLIP (Serial Line Interface Protocol - Protocolo de interfaz de línea serie)** o **SOC (Serial Optical Channel Converter - Convertidor de canal óptico serie)** puesto que éstas son conexiones de punto a punto.

El kernel mantiene las tablas de conversión y el **ARP** no está directamente disponible a los usuarios o aplicaciones. Cuando una aplicación envía un paquete de Internet a uno de los controladores de interfaz, el controlador solicita la correlación de direcciones apropiada. Si la correlación no está en la tabla, se envía un paquete de difusión **ARP** a través del controlador de interfaz solicitante a los sistemas principales de la red de área local.

Las entradas de la tabla de correlación **ARP** se suprimen después de 20 minutos; las entradas incompletas se suprimen después de 3 minutos. Para crear una entrada permanente en las tablas de correlación **ARP**, utilice el mandato **arp** con el parámetro **pub**:

```
arp -s 802.3 host2 0:dd:0:a:8s:0 pub
```

Cuando cualquier sistema principal que soporta **ARP** recibe un paquete de petición **ARP**, el sistema principal anota las direcciones **IP** y de hardware del sistema solicitante y, si es necesario, actualiza la tabla de correlación. Si la dirección **IP** del sistema principal receptor no coincide con la dirección solicitada, el sistema principal elimina el paquete de petición. Si la dirección **IP** no coincide, el sistema principal receptor envía un paquete de respuesta al sistema solicitante. El sistema solicitante almacena la nueva correlación y la utiliza para transmitir cualquier paquete de Internet similar pendiente.

#### **Protocolo de mensajes de control de Internet (Internet Control Message Protocol)**

El segundo protocolo a nivel de red es el **ICMP (Internet Control Message Protocol - Protocolo de mensajes de control de Internet)**. **ICMP** es una parte necesaria de cada implementación de **IP**. **ICMP** maneja los mensajes de error y control para **IP**.

Este protocolo permite a las pasarelas y los sistemas principales enviar informes de problemas a la máquina que envía un paquete. **ICMP** realiza lo siguiente:

- Prueba si un destino está activo y es alcanzable
- Informa de los problemas de parámetros en una cabecera de datagrama
- Realiza la sincronización de reloj y las estimaciones de tiempo de tránsito
- Obtiene direcciones de Internet y máscaras de subred

**Nota:** **ICMP** utiliza el soporte básico de **IP** como si fuera un protocolo de nivel más alto. Sin embargo, **ICMP** es en realidad una parte integral de **IP** y cada módulo **IP** lo debe implementar.

**ICMP** proporciona información de retorno sobre problemas en el entorno de comunicaciones, pero no hace que **IP** sea fiable. Es decir, **ICMP** no garantiza que un paquete **IP** se entregue de forma fiable o que un mensaje **ICMP** se devuelva al sistema principal de origen cuando un paquete **IP** no se entrega o se entrega incorrectamente.

Los mensajes **ICMP** se pueden enviar en cualquiera de las situaciones siguientes:

- Cuando un paquete no puede alcanzar el destino
- Cuando un sistema principal de pasarela no tiene la capacidad de almacenamiento intermedio para reenviar un paquete
- Cuando una pasarela puede indicar a un sistema principal que envíe el tráfico en una ruta más corta

**TCP/IP** envía y recibe varios tipos de mensajes ICMP (consulte “[Tipos de mensaje del Protocolo de mensajes de control de Internet](#)” en la página 152). **ICMP** está incorporado en el kernel y no se proporciona ninguna interfaz de programación de aplicaciones (API) en este protocolo.

*Tipos de mensaje del Protocolo de mensajes de control de Internet*  
**ICMP** envía y recibe estos tipos de mensaje.

Item	Descripción
<b>petición de eco</b>	Los envían los sistemas principales y las pasarelas para probar si un destino está activo y es alcanzable.
<b>petición de información</b>	Lo envían los sistemas principales y las pasarelas para obtener una dirección de Internet para una red a la que están conectados. Este tipo de mensaje se envía con la parte de red de dirección de destino de <b>IP</b> establecida en un valor de 0.
<b>petición de indicación de la hora</b>	Se envía para solicitar que la máquina de destino devuelva el valor actual para la hora del día.
<b>petición de máscara de dirección</b>	Lo envía el sistema principal para conocer la máscara de subred. El sistema principal puede enviar a una pasarela, si conoce la dirección de pasarela, o enviar un mensaje de difusión.
<b>destino inalcanzable</b>	Se envía cuando una pasarela no puede entregar un datagrama <b>IP</b> .
<b>interrupción de origen</b>	Lo envía la máquina de eliminación cuando llegan datagramas demasiado rápidamente para que los procese una pasarela o un sistema principal, con el fin de solicitar que el origen original reduzca la velocidad de envío de datagramas.
<b>mensaje de redirección</b>	Se envía cuando una pasarela detecta que algún sistema principal está utilizando una ruta no óptima.
<b>respuesta de eco</b>	Lo envía cualquier máquina que recibe una petición de eco de respuesta a la máquina que ha enviado la petición.
<b>respuesta de información</b>	Lo envían las pasarelas en respuesta a las peticiones de direcciones de red, especificando los campos de origen y destino del datagrama <b>IP</b> .
<b>respuesta de indicación de la hora</b>	Se envía con el valor actual de la hora del día.
<b>respuesta de máscara de dirección</b>	Se envía a máquinas que solicitan máscaras de subred.
<b>problema de parámetro</b>	Se envía cuando un sistema principal o una pasarela encuentra un problema en una cabecera de datagrama.
<b>tiempo excedido</b>	Se envía cuando se cumple lo siguiente: <ul style="list-style-type: none"><li>• Cada datagrama <b>IP</b> contiene un contador de tiempo de vida (cuenta de saltos), que disminuye en cada pasarela.</li><li>• Una pasarela elimina un datagrama porque la cuenta de saltos ha alcanzado un valor de 0.</li></ul>
<b>Indicación de la hora de Internet</b>	Se utiliza para registrar las indicaciones de la hora a través de la ruta.

#### **Protocolo Internet (Internet Protocol)**

El tercer protocolo de nivel de red es **IP (Internet Protocol - Protocolo Internet)**, que proporciona la entrega de paquetes sin conexión no fiable para Internet.

**IP** no tiene conexiones porque trata cada paquete de información de forma independiente. No es fiable porque no garantiza la entrada, lo que significa que no necesita reconocimientos del sistema principal de envío, del sistema principal de recepción ni de los sistemas principales intermedios.

**IP** proporciona la interfaz en los protocolos de nivel de interfaz de red. Las conexiones físicas de una red transfieren la información de una trama con una cabecera y datos. La cabecera contiene la dirección de origen y la dirección de destino. **IP** utiliza un datagrama de Internet que contiene información similar a la trama física. El datagrama también tiene una cabecera que contiene direcciones de protocolo de Internet del origen y del destino de los datos.

**IP** define el formato de todos los datos enviados a través de Internet.

#### Bits

0	4	8	16	19	31
Versión	Longitud	Tipo de servicio		Longitud total	
		Identificación	Disntin- tivos	Desplazamiento de fragmento	
Tiempo de vida		Protocolo		Suma de comprobación de cabecera	
		Dirección de origen			
		Dirección de destino			
		Opciones			
		Datos			

Figura 10. Cabecera de paquete de Protocolo Internet

Esta ilustración muestra los primeros 32 bits de una cabecera de paquete IP típica. La tabla siguiente lista las diversas entidades.

#### Definiciones de campo de cabecera IP

Item	Descripción
<b>Version</b>	(Versión) Especifica la versión de <b>IP</b> utilizada. La versión actual del protocolo <b>IP</b> es 4.
<b>Length</b>	(Longitud) Especifica la longitud de cabecera de datagrama, medida en palabras de 32 bits.
<b>Type of Service</b>	(Tipo de servicio) contiene cinco subcampos que especifican el tipo de precedencia, retardo, rendimiento y fiabilidad deseados para dicho paquete. (Internet no garantiza esta petición.) Los valores predeterminados para estos cinco subcampos son precedencia de rutina, retardo normal, rendimiento normal y fiabilidad normal. Normalmente Internet no utiliza este campo en este momento. Esta implementación de <b>IP</b> satisface los requisitos de la especificación <b>IP</b> , RFC 791, <i>Protocolo Internet</i> .
<b>Total Length</b>	(Longitud total) Especifica la longitud del datagrama incluyendo la cabecera y los datos medidos en octetos. Se proporciona la fragmentación de paquetes en las pasarelas, con reensamblaje en los destinos. La longitud total del paquete <b>IP</b> se puede configurar de interfaz en interfaz con el mandato <b>ifconfig</b> o la vía de acceso rápida de System Management Interface Tool (SMIT), smit chinet. Utilice SMIT para establecer los valores permanentemente en la base de datos de configuración; utilice el mandato <b>ifconfig</b> para establecer o cambiar los valores en el sistema en ejecución.
<b>Identification</b>	(Identificación) Contiene un entero exclusivo que identifica el datagrama.

<b>Item</b>	<b>Descripción</b>
<b>Flags</b>	(Distintivos) Controla la fragmentación de datagrama, junto con el campo de identificación. Los distintivos de fragmento especifican si el datagrama se puede fragmentar y si el fragmento actual es el último.
<b>Fragment Offset</b>	(Desplazamiento de fragmento) Especifica el desplazamiento de este fragmento en el datagrama original medido en unidades de 8 octetos.
<b>Time to Live</b>	(Tiempo de vida) Especifica cuánto tiempo puede permanecer el datagrama en Internet. Esto evita que los datagramas direccionados incorrectamente permanezcan en Internet de forma indefinida. El tiempo de vida predeterminado es 255 segundos.
<b>Protocol</b>	(Protocolo) Especifica el tipo de protocolo de alto nivel.
<b>Header Checksum</b>	(Suma de comprobación de cabecera) Indica un número calculado para asegurar la integridad de los valores de cabecera.
<b>Source Address</b>	(Dirección de origen) Especifica la dirección de Internet del sistema principal de envío.
<b>Destination Address</b>	(Dirección de destino) Especifica la dirección de Internet del sistema principal de recepción.

<b>Item</b>	<b>Descripción</b>
<b>Options</b>	(Opciones) Proporciona pruebas y depuración de red. Este campo no es necesario para cada datagrama.
	<b>End of Option List</b> (Fin de lista de opciones) Indica el final de la lista de opciones. Se utiliza al final en la última opción, no al final de cada opción individualmente. Sólo se debe utilizar esta opción si, de otra forma, el final de las opciones no va a coincidir con el final de la cabecera <b>IP</b> . El fin de lista de opciones se utiliza si las opciones exceden la longitud del datagrama.
	<b>No Operation</b> (Ninguna operación) Proporciona alineación entre otras opciones; por ejemplo, para alinear el principio de una opción subsiguiente en un límite de 32 bits.
	<b>Loose Source and Record Route</b> Proporciona un medio para que el origen de un datagrama de Internet proporcione la información de direccionamiento utilizada por las pasarelas al reenviar el datagrama a un destino y al registrar la información de ruta. Esta ruta de origen es <i>flexible</i> : Se permite a la pasarela o al sistema principal <b>IP</b> utilizar cualquier ruta de cualquier número de otras pasarelas intermedias con el fin de alcanzar la siguiente dirección de la ruta.
	<b>Strict Source and Record Route</b> Proporciona un medio para que el origen de un datagrama de Internet proporcione la información de direccionamiento utilizada por las pasarelas al reenviar el datagrama a un destino y al registrar la información de ruta. Esta ruta de origen es <i>estricta</i> : Para alcanzar la siguiente pasarela o el siguiente sistema principal especificado en la ruta, la pasarela o el sistema principal <b>IP</b> debe enviar el datagrama directamente a la siguiente dirección de la ruta de origen y sólo a la red directamente conectada que se indica en la siguiente dirección.
	<b>Record Route</b> (Ruta de registro) Proporciona un medio para registrar la ruta de un datagrama de Internet.
	<b>Stream Identifier</b> (Identificador de corriente) Proporciona un medio para que un identificador de corriente pase por redes que no soportan el concepto de corriente.
	<b>Indicación de la hora de Internet</b> (Indicación de la hora de Internet) Proporciona un registro de las indicaciones de la hora por la ruta.

En los paquetes de salida se pone automáticamente como prefijo una cabecera **IP**. En los paquetes de entrada, la cabecera **IP** se elimina antes de enviar dichos paquetes a los protocolos de nivel más alto. El protocolo **IP** proporciona el direccionamiento universal de sistemas principales en la red Internet.

#### **Protocolos a nivel de transporte de Internet**

Los protocolos de nivel de transporte **TCP/IP** permiten a los programas de aplicación comunicarse con otros programas de aplicación.

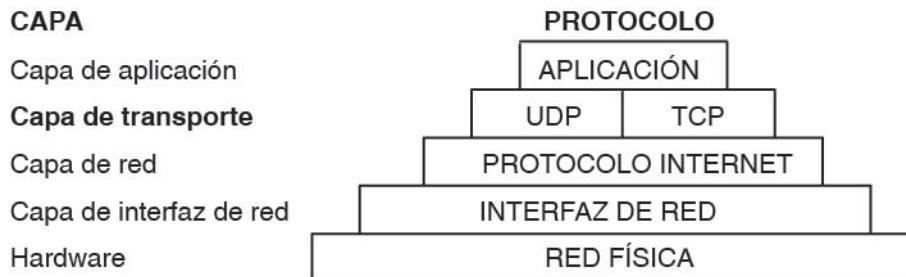


Figura 11. Capa de transporte del conjunto de protocolos de TCP/IP

Esta ilustración muestra las diversas capas del conjunto de protocolos de **TCP/IP**. Desde la parte superior, la capa de aplicaciones consta de la aplicación. La capa de transporte contiene **UDP** y **TCP**. La capa de red contiene la interfaz de red (hardware). Y finalmente, la capa de hardware contiene la red física.

**UDP (User Datagram Protocol)** y **TCP** son los protocolos básicos de nivel de transporte para realizar conexiones entre sistemas principales de Internet. **TCP** y **UDP** permiten que los programas envíen mensajes a las aplicaciones de otros sistemas principales y reciban mensajes de dichas aplicaciones. Cuando una aplicación envía a la capa de transporte una petición de envío de un mensaje, **UDP** y **TCP** dividen la información en paquetes, añaden una cabecera de paquete incluida la dirección de destino y envían la información a la capa de red para su proceso adicional. **TCP** y **UDP** utilizan puertos de protocolo en el sistema principal para identificar el destino específico del mensaje.

Las aplicaciones y los protocolos de nivel superior utilizan **UDP** para realizar conexiones de datagrama y **TCP** para realizar conexiones de corriente. La interfaz de sockets de sistema operativo implementa estos protocolos.

#### User Datagram Protocol

A veces una aplicación de una red necesita enviar mensajes a una aplicación o proceso específicos de otra red. El **UDP** proporciona un medio de datagrama de comunicación entre aplicaciones de sistemas principales de Internet.

Dado que los remitentes no saben qué procesos están activos en un momento determinado, **UDP** utiliza los puertos de protocolo de destino (o puntos de destino abstractos en una máquina), identificados por enteros positivos, para enviar mensaje a uno de los múltiples destinos de un sistema principal. Los puertos de protocolo reciben y conservan los mensajes en las colas hasta que las aplicaciones de la red de recepción puede recuperarlos.

Puesto que **UDP** se basa en el **IP** subyacente para enviar los datagramas, **UDP** proporciona la misma entrega de mensaje sin conexión que **IP**. No ofrece ninguna garantía de entrega de datagrama o de protección de duplicación. Sin embargo, **UDP** permite al remitente especificar números de puerto de origen y destino para el mensaje y calcula la suma de comprobación de los datos y la cabecera. Estos dos características permiten a las aplicaciones de envío y recepción asegurar la entrega correcta de un mensaje.

#### Bits

0	16	31
NÚMERO PUERTO DE ORIGEN	NÚMERO PUERTO DE DESTINO	
LONGITUD	SUMA DE COMPROBACIÓN	

Figura 12. Cabecera de paquete de User Datagram Protocol (UDP)

Esta ilustración muestra los primeros 32 bits de la cabecera de paquete **UDP**. Los primeros 16 bits contienen el número de puerto de origen y la longitud. Los segundos 16 bits contienen el número de puerto de destino y la suma de comprobación.

Las aplicaciones que necesitan la entrega fiable de datagramas deben implementar sus propias comprobaciones de fiabilidad cuando utilicen **UDP**. Las aplicaciones que necesitan la entrega fiable de las corrientes de datos deben utilizar **TCP**.

## Definiciones de campos de cabecera de UDP

Item	Descripción
<b>Source Port Number</b>	(Número de puerto de origen) Dirección del puerto de protocolo que envía la información.
<b>Destination Port Number</b>	(Número de puerto de destino) Dirección del puerto de protocolo que recibe la información.
<b>Length</b>	(Longitud) Longitud en octetos del datagrama <b>UDP</b> .
<b>Checksum</b>	(Suma de comprobación) Proporciona una comprobación en el datagrama <b>UDP</b> utilizando el mismo algoritmo que <b>IP</b> .

La interfaz de programación de aplicaciones (API) en **UDP** es un conjunto de subrutinas de biblioteca proporcionadas por la interfaz de sockets.

### *Reliable Datagram Sockets sobre InfiniBand y RoCE*

RDS (Reliable Datagram Sockets) es un protocolo sin conexión y orientado al registro que proporciona un servicio en orden y no duplicado sobre InfiniBand y RDMA over Converged Ethernet (RoCE).. RDS expone el conjunto UDP (User Datagram Protocol) de la API del socket.

El RDS forma parte del dominio **AF\_BYPASS** que se utiliza para protocolos que han omitido la pila TCP/IP del kernel.

El sistema operativo AIX proporciona dos versiones de RDS: RDSv2 y RDSv3. RDSv3 es la versión más reciente e incluye soporte para RDMA (Remote Direct Memory Access).RDSv3 en AIX 7.2 y posteriores incluye soporte a Open Fabrics Enterprise Distribution (OFED) que se basa en RDMA over Converged Ethernet (RoCE).

### *Creación de un socket RDS*

Para crear un socket RDS, invoque la llamada del sistema **socket()** añadiendo las líneas siguientes al programa de aplicaciones:

```
#include <sys/bypass.h>
#include <net/rds_rdma.h>           /* for RDSv3 only */
sock = socket (AF_BYPASS, SOCK_SEQPACKET,BYPASSPROTO_RDS);
```

Si el protocolo **BYPASSPROTO\_RDS** es el único protocolo de datagrama fiable admitido en la familia **AF\_BYPASS**, también puede llamar a la llamada del sistema **socket()** tal como se indica a continuación:

```
sock = socket (AF_BYPASS, SOCK_SEQPACKET,0);
```

### **Llamadas del sistema**

El RDS también admite las siguientes llamadas del sistema:

- **blind()**
- **close()**
- **getsockopt()**
- **recvform()**
- **recvmsg()**
- **sendmsg()**
- **sendto()**
- **setsockopt()**

Además, RDSv3 también admite las siguientes llamadas del sistema:

- **connect()**

- `read()`
- `recv()`
- `send()`
- `write()`

**Nota:** Aunque los sockets de RDS son sin conexión, la llamada del sistema `connect()` está admitida por RDSv3. Sin embargo, en este caso, `connect()` no crea una entidad de conexión de nivel de socket entre dos puntos finales de RDS. Simplemente asocia un punto final de destino predeterminado con el socket. Por este motivo, las llamadas del sistema `listen()`, `accept()` y `shutdown()` no están admitidas para los sockets RDS.

*El programa de utilidad rdsctrl para RDSv2*

Utilice el programa de utilidad `rdsctrl` (`/usr/sbin/rdsctrl`) para cambiar los valores ajustables y los diagnósticos para las estadísticas de RDS. Para RDSv2, el programa de utilidad se puede utilizar una vez que se cargue RDS (**bypassctrl load rds**). Para obtener más información para este programa de utilidad, ejecute el mandato `rdsctrl` sin argumentos.

#### Estadísticas

Para visualizar varias estadísticas de RDS, ejecute el mandato `# rdsctrl stats`.

Para restablecer las estadísticas, ejecute el mandato `# rdsctrl stats reset`.

#### Parámetros de ajuste

Los siguientes parámetros RDS se pueden ajustar una vez que se cargue RDS, pero antes de que se ejecute una aplicación RDS:

##### `rds_sendspace`

Especifica la marca de límite superior del almacenamiento intermedio de envío por flujo. Cada socket puede tener varios flujos. El valor predeterminado es 524288 bytes (512 KB). El valor se establece utilizando el mandato siguiente: `# rdsctrl set rds_sendspace= <valor en bytes>`.

##### `rds_recvspace`

Especifica la marca de límite superior por flujo del almacenamiento intermedio de recepción por socket. Para cada flujo adicional de este socket, la marca **de límite superior de recepción** aumentará mediante este valor. El valor predeterminado es 524288 bytes (512 KB). El valor se establece utilizando el mandato siguiente: `# rdsctrl set rds_recvspace= <valor en bytes>`.

**Nota:** Para mayor rendimiento de corriente de datos RDS, los valores del parámetro `rds_sendspace` y del parámetro `rds_recvspace` deben ser como mínimo el valor del tamaño `sendmsg()` RDS mayor, multiplicado por cuatro. RDS envía un ACK por cada conjunto de cuatro mensajes que se reciban. Si el `rds_recvspace` no es al menos cuatro veces mayor que el tamaño del mensaje, el rendimiento será muy bajo.

##### `rds_mclustsize`

Especifica el tamaño del clúster de memoria individual, que también es el tamaño de fragmento del mensaje. El tamaño predeterminado es 16384 bytes (16 KB). El valor, siempre un múltiplo de 4096, se establece utilizando el siguiente mandato: `# rdsctrl set rds_mclustsize= <múltiplo de 4096, en bytes>`.



**Atención:** El valor `rds_mclustsize` debe ser el mismo en todos los sistemas (nodos) del clúster. El cambio de este valor también tiene implicaciones de rendimiento.

Los valores actuales de los parámetros precedentes se pueden recuperar utilizando el mandato `# rdsctrl get <parámetro>`.

Para obtener la lista de todos los ajustables y sus valores, ejecute el mandato `# rdsctrl get`.

*El programa de utilidad rdsctrl para RDSv3*

Para RDSv3, el mandato `rdsctrl` admite sus opciones. Estas opciones están listadas aquí:

Item	Descripción
<b>help [&lt;nombre de ajustable&gt;]</b>	La opción <b>ayuda</b> muestra un mensaje descriptivo del ajustable RDSv3 especificado. Si no se especifica ningún ajustable, esta opción muestra la lista de todos los ajustables admitidos para RDSv3, junto con la descripción de cada ajustable.
<b>set [-p] {&lt;nombre de ajustable&gt;} = &lt;valor&gt;</b>	La opción <b>establecer</b> establece el valor del ajustable RDSv3 especificado. Verifica que el usuario tiene los privilegios necesarios para evitar que los usuarios no autorizados cambien los ajustables RDS. También ordena la validación para los nuevos valores ajustables.  El distintivo <b>-p</b> convierte a la asignación en permanente a través de las operaciones de rearranque.
<b>get [&lt;nombre de ajustable&gt;]</b>	La opción <b>obtener</b> obtiene el valor actual del ajustable consultado. Cuando no se especifique ningún campo de nombre para este mandato, devuelve el valor actual de todos los ajustables RDS disponibles.
<b>default [-p] [&lt;nombre de ajustable&gt;]</b>	La opción <b>valor predeterminado</b> se utiliza para restablecer un ajustable a su valor predeterminado. Cuando se especifica el campo de nombre, sólo se restablece dicho ajustable. Si no se especifica ningún campo de nombre, este mandato restablece todos los ajustables a sus valores predeterminados.  Esta opción también proporciona una forma de realizar el cambio permanente entre rearranques utilizando el distintivo <b>-p</b> .
<b>load [ ofed   aixib ]</b>	La opción <b>cargar</b> carga la ampliación de kernel RDSv3 (si aún no se ha cargado).  El argumento <b>ofed</b> carga la extensión de kernel en RDSv3 en verbs de OFED en modo RoCE. El argumento <b>aixib</b> carga la extensión de kernel en RDSv3 en modo InfiniBand. Es opcional especificar un argumento para la opción <b>load</b> . Cuando el argumento <b>aixib</b> no se especifica, la opción <b>load</b> es el valor predeterminado.  De forma predeterminada, el programa de utilidad <b>rdsctrl</b> carga el dispositivo InfiniBand a menos que especifique el nuevo atributo en ( <b>ofed</b> ) en la línea de mandatos.
<b>descargar</b>	La opción <b>descargar</b> se utiliza para descargar la ampliación de kernel RDSv3.
<b>ras [-p] &lt;mínimo / normal / detalle / máximo&gt;</b>	La opción <b>ras</b> establece el rastreo RAS de sistema operativo AIX y los valores de comprobación de errores para RDSv3 en el nivel especificado. Internamente, este mandato llama a los mandatos <b>errctrl</b> y <b>ctctrl</b> del sistema operativo AIX.  El distintivo <b>-p</b> convierte a los valores en persistentes en las operaciones de rearranque.
<b>extraer ras</b>	La opción <b>extraer ras</b> vuelve el contenido de los almacenamientos intermedios de rastreo de error y no error de RAS para RDS en la salida estándar.
<b>info [&lt;distintivos&gt;]</b>	La opción <b>información</b> es un alias para el mandato <b>rds-info</b> .
<b>ping [&lt;dirección IP v4&gt;]</b>	La opción <b>ping</b> es un alias para el mandato <b>rds-ping</b> .

Item	Descripción
<b>conn &lt;reiniciar / terminar&gt; &lt;dirección IP de origen&gt; &lt;dirección IP de destino&gt;</b>	La opción <b>conn</b> reinicia la conexión RDS especificada (subopción <b>restart</b> ) o finaliza de manera permanente la conexión RDS especificada (subopción <b>kill</b> ). La conexión RDS que se va a reiniciar o a finalizar se especifica proporcionando las direcciones IP de los nodos locales y remotos para la conexión. El reinicio de una conexión elimina la conexión InfiniBand subyacente y los intentos de establecer la conexión de nuevo. En cambio, la finalización de una conexión (subopción <b>kill</b> ) elimina la conexión InfiniBand subyacente y desasigna todos los recursos asociados con la conexión RDS correspondiente.
<b>trace start &lt;vía de acceso de archivo de rastreo&gt; &lt;máximo de datos capturados por fragmento RDS&gt;</b>	La opción <b>iniciar rastreo</b> inicia una sesión de rastreo para capturar tráfico por cable para el protocolo RDSv3. Los mensajes RDSv3 se transmiten en fragmentos. Cada fragmento RDS que se transmite o se recibe se captura como un paquete de rastreo en el archivo de rastreo especificado. Para cada fragmento RDS, su carga útil se captura hasta los bytes de <máximo de datos capturados por fragmento RDS>. Sólo los usuarios con privilegios pueden rastrear el tráfico RDS y sólo puede estar activa a la vez una sesión de rastreo.
<b>detener rastreo</b>	La opción <b>detener rastreo</b> finaliza una sesión de rastreo que se había iniciado previamente con un mandato <b>iniciar rastreo</b> . Cierra el archivo de rastreo asociado con la sesión de rastreo. Después de este mandato, el mandato <b>informe de rastreo</b> se puede utilizar para generar un informe de texto del archivo de rastreo.
<b>trace report &lt;vía de acceso de archivo de rastreo&gt;</b>	La opción <b>informe de rastreo</b> imprime un informe de texto en la salida estándar, a partir de un archivo de rastreo de protocolo RDS capturado previamente.
<b>versión</b>	La opción <b>versión</b> imprime la versión de protocolo RDS que se ha cargado actualmente en el sistema.

#### Ajustables RDSv3

Para ver la lista de los ajustables admitidos para RDSv3, ejecute el mandato **rdsctrl help** sin argumentos.

#### API RDMA (sólo RDSv3)

El modelo de programación para trabajar en RDMA con sockets de RDS se basa en el modelo cliente/servidor. El cliente RDMA es la aplicación que inicia una operación de lectura o grabación RDMA desde un servidor RDMA especificado. El servidor RDMA es la aplicación que procesa la transferencia de datos RDMA. Una operación de lectura de RDMA es una transferencia de datos del espacio de direcciones del cliente al espacio de direcciones del servidor, donde una operación de grabación de RDMA es una transferencia de datos del espacio de direcciones del servidor al espacio de direcciones del cliente. En cualquiera de los casos, los datos se transfieren directamente entre la memoria de espacio del usuario en ambos lados, sin que se copien en la memoria de espacio de kernel de cualquier lado.

Una aplicación cliente de RDMA puede iniciar una operación de lectura o grabación de RDMA mediante el envío de una solicitud de nivel de aplicación, junto con una cookie RDMA, a una aplicación de servidores RDMA. La solicitud de nivel de aplicaciones debe especificar si la operación es una operación de lectura o grabación RDMA así como la dirección y la longitud del área de la memoria del cliente para que se lean o se graben de forma remota mediante el servidor RDMA.

Hay dos métodos para enviar una solicitud RDMA del cliente RDMA al servidor RDMA.

El primer método es enviar un mensaje de control **RDS\_CMSG\_RDMA\_MAP** (contiene una estructura **rds\_get\_mr\_args**) junto con la solicitud RDMA de nivel de aplicación utilizando la llamada del sistema **sendmsg()** en un socket RDS. El kernel del sistema operativo AIX en el lado del cliente procesa el

mensaje de control de **RDS\_CMSG\_RDMA\_MAP** correlacionando el área especificada de la memoria local (desde el espacio de direcciones de la aplicación del cliente), para el acceso de DMA, y generando una cookie RDMA. A continuación, se enviará la solicitud de nivel de aplicación al servidor junto con la cookie RDMA.

El segundo método consta de dos pasos. El primer paso es llamar a la llamada del sistema **setsockopt()** con la opción de socket **RDS\_GET\_MR**, pasando una estructura **rds\_get\_mr\_args**. Esta llamada correlaciona el área especificada de la memoria local para el acceso de DMA, y devuelve una cookie RDMA. El segundo paso es enviar un mensaje de control **RDS\_CMSG\_RDMA\_DEST** (transportar la cookie RDMA que se obtiene desde el primer paso) junto con la solicitud RDMA de nivel de aplicación utilizando la llamada del sistema **sendmsg()**.

El primer método, que requiere una llamada al sistema, se prefiere al segundo método, que requiere dos llamadas al sistema.

Cuando la aplicación del servidor RDMA recibe la solicitud **RDMA read** de nivel de aplicaciones del cliente, también recibe un mensaje de control **RDS\_CMSG\_RDMA\_DEST** (transportar la cookie RDMA desde el cliente). A continuación, el servidor iniciará la operación **RDMA read**, enviando una respuesta de nivel de aplicaciones al cliente junto con un mensaje de control **RDS\_CMSG\_RDMA\_ARGS** (transportar una estructura **rds\_rdma\_args**). El kernel del sistema operativo AIX del lado del servidor procesa el mensaje de control **RDS\_CMSG\_RDMA\_ARGS**, correlacionando el área especificada de memoria local (desde el espacio de direcciones de la aplicación del servidor), para el acceso de DMA, e iniciando físicamente la operación de lectura de RDMA. La operación de lectura de RDMA se realiza mediante el adaptador InfiniBand del lado del servidor, que interactúa con el adaptador InfiniBand del lado del cliente, para hacer la transferencia de datos directamente desde la memoria de la aplicación del cliente a la memoria de la aplicación del servidor, sin más intervención del software. Una vez que se complete la operación de lectura de RDMA, el adaptador del lado del servidor enviará la respuesta de nivel de la aplicación al cliente. Este es el modo en que la aplicación cliente sabe que su operación de lectura RDMA se ha completado.

**Nota:** El cliente ha solicitado una operación RDMA utilizando un control **RDS\_CMSG\_RDMA\_MAP** en el que se establece el distintivo **RDS\_RDMA\_USE\_ONCE**. Para esta solicitud, se elimina la correlación automáticamente del área de memoria correlacionada para DMA en el espacio de direcciones del cliente de la memoria para DMA, cuando el cliente recibe la respuesta de nivel de aplicaciones del servidor.

Aunque este mecanismo de correlación o de eliminación de correlación implícito de DMA hace más sencillo grabar aplicaciones RDMA, los desarrolladores deben tener en cuenta que registrar memoria para DMA en el sistema operativo AIX es una operación costosa. Por lo tanto, si se va a acceder a la misma área de memoria utilizando RDMA varias veces, resulta más eficaz registrar DMA sólo la primera vez. Para hacer esta actividad, una aplicación cliente necesita utilizar un mensaje de control **RDS\_CMSG\_RDMA\_MAP** sin el conjunto de distintivos **RDS\_RDMA\_USE\_ONCE** al enviar la solicitud RDMA al servidor. A continuación, las posteriores transferencias RDMA a la misma área de la memoria del cliente se pueden iniciar mediante la aplicación del servidor RDMA sin que sea necesario que el cliente envíe otra solicitud al servidor. Al final, la aplicación cliente necesita eliminar la correlación de forma explícita de la memoria correlacionada para DMA utilizando la llamada al sistema **setsockopt()** con la opción de socket **RDS\_FREE\_MR**.

Las opciones de socket específicas de RDS se especifican utilizando **SOL\_RDS** como el parámetro de nivel para la llamada al sistema **setsockopt()** o **getsockopt()**.

#### **Protocolo de control de transmisiones (Transmission Control Protocol)**

**TCP** proporciona entrega continua fiable de datos entre sistemas principales de Internet.

Igual que **UDP**, **TCP** utiliza el Protocolo Internet, el protocolo subyacente, para transportar datagramas, y soporte la transmisión de bloques de una corriente continua de datagramas entre puertos de proceso. A diferencia de **UDP**, **TCP** proporciona entrega de mensajes fiable. **TCP** asegura que los datos no se dañen, se pierdan, se dupliquen o se entregan desordenados a un proceso receptor. Esta seguridad de fiabilidad de transporte evita que los programadores de aplicaciones tengan que crear protecciones de comunicaciones en el software.

A continuación se indican las características operativas de **TCP**:

Item	Descripción
<b>Transferencia de datos básica</b>	<b>TCP</b> puede transferir una corriente continua de octetos de 8 bits en cada dirección entre los usuarios empaquetando un número de bytes en segmentos para transmitirlos por el sistema de Internet. La implementación de <b>TCP</b> permite un tamaño de segmento de 1024 bytes como mínimo. En general, <b>TCP</b> decide cuándo se deben bloquear y enviar paquetes según su propia comodidad.
<b>Fiabilidad</b>	<b>TCP</b> debe recuperar datos que están dañados, perdidos, duplicados o entregados en desorden por Internet. <b>TCP</b> logra esta fiabilidad asignando un número de secuencia a cada octeto que transmite y exigiendo un reconocimiento (ACK) del <b>TCP</b> receptor. Si no se recibe el ACK dentro del intervalo de tiempo de espera, los datos se vuelven a transmitir. El valor de tiempo de espera de retransmisión de <b>TCP</b> se determina dinámicamente para cada conexión, basándose en el tiempo de ida y vuelta. En el destinatario, se utilizan los números de secuencia para ordenar correctamente los segmentos que se puedan recibir desordenados y para eliminar duplicados. Los daños se manejan añadiendo una suma de comprobación a cada segmento transmitido, comprobándolo en el destinatario y descartando los segmentos dañados.
<b>Control de flujo</b>	<b>TCP</b> controla la cantidad de datos enviados devolviendo una ventana con cada ACK para indicar un rango de números de secuencia aceptables más allá del último segmento recibido satisfactoriamente. La ventana indica un número permitido de octetos que el remitente puede transmitir antes de recibir permiso adicional.
<b>Multiplexado</b>	<b>TCP</b> permite que muchos procesos en un solo sistema principal utilicen recursos de comunicaciones <b>TCP</b> de forma simultánea. <b>TCP</b> recibe un conjunto de direcciones de puertos en cada sistema principal. <b>TCP</b> combina el número de puerto con la dirección de red y la dirección de sistema principal para identificar de forma exclusiva cada socket. Un par de sockets identifica de forma exclusiva cada conexión.
<b>Conexiones</b>	<b>TCP</b> debe inicializar y mantener determinada información de estado para cada corriente de datos. La combinación de esta información, incluyendo sockets, números de secuencia y tamaños de ventana, se denomina conexión. Cada conexión se especifica de forma exclusiva mediante un par de sockets que identifican sus dos lados.
<b>Prioridad y seguridad</b>	Los usuarios de <b>TCP</b> pueden indicar la seguridad y la prioridad de las comunicaciones. Cuando no se necesitan estas funciones, se utilizan los valores predeterminados.

La figura de **Cabecera de paquete TCP** ilustra estas características.

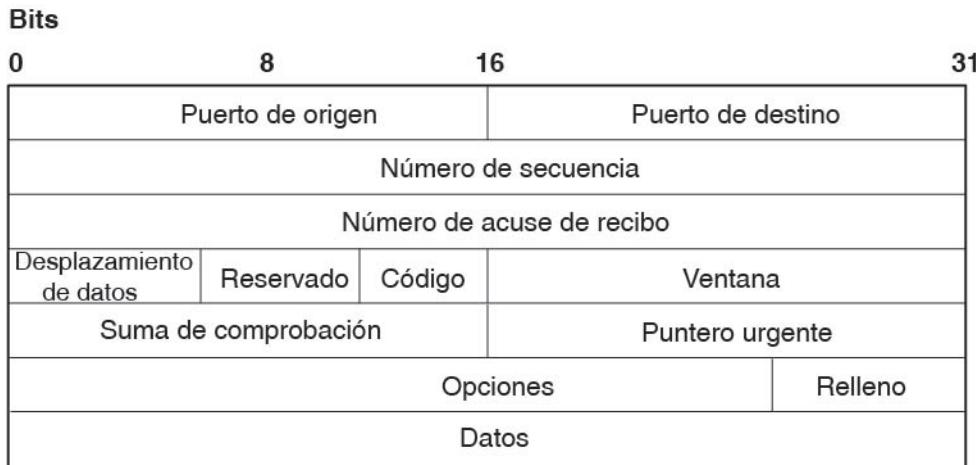


Figura 13. Cabecera de paquete de TCP (Transmission Control Protocol)

Esta ilustración muestra el contenido de la cabecera de paquete **TCP**. En el texto siguiente se listan las entidades individuales.

#### **Definiciones de campo de cabecera de TCP**

A continuación, se proporciona unas descripciones breves de cada uno de los campos de **TCP** (**Transmission Control Protocol - Protocolo de control de transmisiones**).

Item	Descripción
<b>Source Port</b>	(Puerto de origen) Identifica el número de puerto de un programa de aplicación de origen.
<b>Destination Port</b>	(Puerto de destino) Identifica el número de puerto de un programa de aplicación de destino.
<b>Sequence Number</b>	(Número de secuencia) Especifica el número de secuencia del primer byte de datos de este segmento.
<b>Acknowledgment Number</b>	(Número de reconocimiento) Identifica la posición del byte más alto recibido.
<b>Data Offset</b>	(Desplazamiento de datos) Especifica el desplazamiento de la parte de datos del segmento.
<b>Reserved</b>	(Reservado) Reservado para uso futuro.
<b>Code</b>	(Código) Bits de control para identificar la finalidad del segmento:
	<b>URG</b> El campo de puntero urgente es válido.
	<b>ACK</b> El campo de reconocimiento es válido.
	<b>PSH</b> El segmento solicita un PUSH.
	<b>RTS</b> Restablece la conexión.
	<b>SYN</b> Sincroniza los números de secuencia.
	<b>FIN</b> El remitente ha alcanzado el final de la corriente de bytes.
<b>Window</b>	(Ventana) Especifica la cantidad de datos que el destino está dispuesto a aceptar.

Item	Descripción
<b>Checksum</b>	(Suma de comprobación) Verifica la integridad de la cabecera y los datos de segmento.
<b>Urgent Pointer</b>	(Puntero urgente) Indica datos que se deben entregar lo más rápidamente posible. Este puntero especifica la posición donde finalizan los datos urgentes.
<b>Options (Opciones)</b>	<p><b>End of Option List</b>            (Fin de lista de opciones) Indica el final de la lista de opciones. Se utiliza en la opción final, no al final de cada opción individualmente. Sólo es necesario utilizar esta opción si el final de las opciones no coincidirá con el final de la cabecera <b>TCP</b>.</p> <p><b>No Operation</b>            (Sin operación) Indica los límites entre las opciones. Se puede utilizar entre otras opciones; por ejemplo, para alinear el principio de una opción subsiguiente en un límite de palabra. No existe ninguna garantía de que los remitentes vayan a utilizar esta opción, de modo que los destinatarios deben estar preparados para procesar opciones incluso aunque éstas no empiecen en un límite de palabra.</p> <p><b>Maximum Segment Size</b>            (Tamaño máximo de segmento) Indica el tamaño máximo de segmento que <b>TCP</b> puede recibir. Esto sólo se envía en la petición de conexión inicial.</p>

La interfaz de programación de aplicaciones en **TCP** consta de un conjunto de subrutinas de biblioteca proporcionadas por la interfaz de sockets.

### Protocolos a nivel de aplicación de Internet

**TCP/IP** implementa protocolos de Internet de nivel superior en el nivel de programa de aplicación.

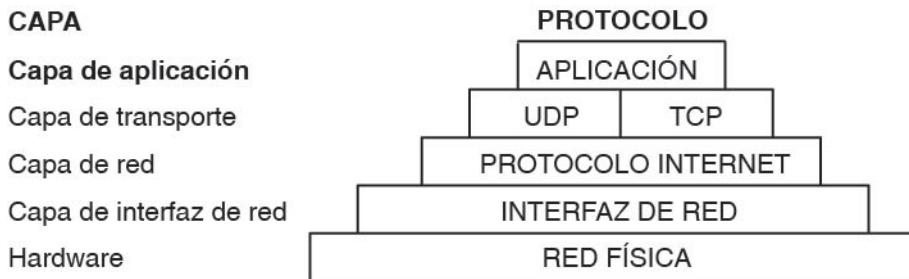


Figura 14. Capa de aplicación del conjunto de protocolos de TCP/IP

Esta ilustración muestra las diversas capas del conjunto de protocolos de **TCP/IP**. Desde la parte superior, la capa de aplicaciones consta de la aplicación. La capa de transporte contiene **UDP** y **TCP**. La capa de red contiene la interfaz de red (hardware). Y finalmente, la capa de hardware contiene la red física.

Cuando una aplicación necesita enviar datos a otra aplicación de otro sistema principal, las aplicaciones envían la información hasta los protocolos de nivel de transporte para preparar la información para la transmisión.

Los protocolos de nivel de aplicaciones oficiales de Internet incluyen:

- **Domain Name Protocol** (Protocolo de nombres de dominio)
- **Exterior Gateway Protocol** (Protocolo de pasarela exterior)
- **File Transfer Protocol** (Protocolo de transferencia de archivos)
- **Name/Finger Protocol** (Protocolo de nombres/finger)

- **Telnet Protocol** (Protocolo Telnet)
- **Trivial File Transfer Protocol** (Protocolo de transferencia de archivos trivial)

TCP/IP implementa otros protocolos de nivel superior que no son protocolos oficiales de Internet pero que se utilizan comúnmente en la comunidad de Internet a nivel de programa de aplicación. Estos protocolos incluyen:

- **Protocolo de red local DCN (Distributed Computer Network)**
- **Protocolo de ejecución remota de mandatos**
- **Protocolo de inicio de sesión remoto**
- **Protocolo de shell remoto**
- **Protocolo Wake On LAN**
- **Protocolo de información de direccionamiento**
- **Protocolo de servidor horario**

**TCP/IP** no proporciona las API a ninguno de estos protocolos de nivel de aplicación.

### **Protocolo de nombres de dominio**

El **Protocolo de nombres de dominio (DOMAIN)** permite a un sistema principal de un dominio actuar como un *servidor de nombres* para otros sistemas principales del dominio.

**DOMAIN** utiliza **UDP** o **TCP** como protocolo subyacente y permite a un red local asignar nombres de sistema principal en el dominio independientemente de otros dominios. Normalmente, el protocolo **DOMAIN** utiliza **UDP**. Sin embargo, si la respuesta de **UDP** se trunca, se puede utilizar **TCP**. El protocolo **DOMAIN** en **TCP/IP** los soporta ambos.

En el sistema de denominación jerárquica de **DOMAIN**, las rutinas de resolución locales pueden resolver nombres y direcciones de Internet utilizando una base de datos de resolución de nombres local mantenida por el daemon **named**. Si el nombre solicitado por el sistema principal no está en la base de datos local, la rutina de resolución consulta un servidor de nombres **DOMAIN** remoto. En cualquier caso, si la información de resolución de nombres no está disponible, las rutinas de resolución intentan utilizar el archivo `/etc/hosts` para la resolución de nombres.

**Nota:** **TCP/IP** configura rutinas de resolución locales para el protocolo **DOMAIN** si el archivo local `/etc/resolv.conf` existe. Si este archivo no existe, **TCP/IP** configura las rutinas de resolución locales para utilizar la base de datos `/etc/hosts`.

**TCP/IP** implementa el protocolo **DOMAIN** en el daemon **named** y en las rutinas de resolución y no proporciona ninguna API en este protocolo.

### **Exterior Gateway Protocol (Protocolo de pasarela exterior)**

**Exterior Gateway Protocol (EGP)** es el mecanismo que permite a la pasarela exterior de un *sistema autónomo* compartir la información de direccionamiento con pasarelas exteriores de otros sistemas autónomos.

### **Sistemas autónomos**

Las pasarelas son *vecinos interiores* si residen en el mismo sistema autónomo y *vecinos exteriores* si residen en sistema autónomos diferentes. Las pasarelas que intercambian información de direccionamiento utilizando **EGP** se conocen como *iguales* o *vecinos EGP*. Las pasarelas de sistemas autónomos utilizan **EGP** para proporcionar información de acceso a los vecinos **EGP**.

**EGP** permite a una pasarela exterior solicitar a otra pasarela exterior que acceda a intercambiar información de acceso, comprueba continuamente que los vecinos **EGP** respondan y ayuda a los vecinos **EGP** a intercambiar información de acceso pasando mensajes de actualización de direccionamiento.

**EGP** restringe las pasarelas exteriores permitiéndoles anunciar sólo las redes de destino totalmente alcanzables dentro del sistema autónomo de esa pasarela. De este modo, una pasarela exterior que

utiliza **EGP** para informar a los vecinos **EGP** pero no anuncia información de acceso acerca de los vecinos **EGP** fuera del sistema autónomo.

**EGP** no interpreta ninguna de la métrica de distancia que aparecen en los mensajes de actualización de direccionamiento de otros protocolos. **EGP** utiliza el campo de distancia para especificar si existe una vía de acceso (un valor de 255 significa que no se puede alcanzar la red). El valor no se puede utilizar para calcular la ruta más corta entre dos, a menos que ambas rutas estén contenidas en un solo sistema autónomo. Por consiguiente, **EGP** no se puede utilizar como algoritmo de direccionamiento. Como resultado, sólo habrá una vía de acceso de la pasarela exterior a cualquier red.

A diferencia de **RIP (Routing Information Protocol - Protocolo de información de direccionamiento)**, que se puede utilizar en un sistema autónomo de redes de Internet que reconfiguran dinámicamente las rutas, las rutas de **EGP** están predeterminadas en el archivo **/etc/gated.conf**. **EGP** supone que **IP** es el protocolo subyacente.

### Tipos de mensajes de EGP

Aquí se definen los diversos tipos de mensajes de EGP (Exterior Gateway Protocol - Protocolo de pasarela exterior).

Item	Descripción
<b>Neighbor Acquisition Request</b>	(Petición de adquisición de vecino) Lo utilizan las pasarelas exteriores para solicitar convertirse en vecinos unos de otros.
<b>Neighbor Acquisition Reply</b>	(Respuesta de adquisición de vecino) Lo utilizan las pasarelas exteriores para aceptar convertirse en vecinos.
<b>Neighbor Acquisition Refusal</b>	(Rechazo de adquisición de vecino) Lo utilizan las pasarelas exteriores para rechazar la petición de convertirse en vecinos. El mensaje de rechazo incluye las razones del rechazo, por ejemplo porque no hay espacio de tablas (out of table space).
<b>Neighbor Cease</b>	(Cese de vecino) Lo utilizan las pasarelas exteriores para cesar la relación de vecinos. El mensaje de cese incluye las razones del cese, por ejemplo quedarse inactivo (going down).
<b>Neighbor Cease Acknowledgment</b>	(Reconocimiento de cese de vecino) Lo utilizan las pasarelas exteriores para reconocer la petición de cese de la relación de vecinos.
<b>Neighbor Hello</b>	(Saludo del vecino) Los utilizan las pasarelas exteriores para determinar la conectividad. Una pasarela emite un mensaje Hello y otra pasarela emite un mensaje I Heard You.
<b>I Heard You</b>	(Le he oído) Lo utilizan las pasarelas exteriores para responder a un mensaje Hello. El mensaje I Heard You incluye el acceso de la pasarela que responde y, si la pasarela es inalcanzable, una razón por la falta de acceso, por ejemplo porque es inalcanzable debido a problemas con la interfaz de red (You are unreachable because of problems with my network interface).
<b>NR Poll</b>	(Sondeo de NR) Lo utilizan las pasarelas exteriores para consultar a las pasarelas de vecino la posibilidad que tienen de alcanzar otras pasarelas.

Item	Descripción
<b>Network Reachability</b>	(Posibilidad de alcanzar la red) Lo utilizan las pasarelas exteriores para responder al mensaje NR Poll. Para cada pasarela del mensaje, el mensaje Network Reachability contiene información sobre las direcciones que esta pasarela puede alcanzar a través de los vecinos.
<b>EGP Error</b>	(Error de EGP) Lo utilizan las pasarelas exteriores para responder a los mensajes EGP que contienen sumas de comprobación incorrectas o tienen campos que contienen valores incorrectos.

**TCP/IP** implementa el protocolo **EGP** en el mandato de servidor **gated** y no proporciona una API a este protocolo.

#### Protocolo de transferencia de archivos (File Transfer Protocol)

**FTP (File Transfer Protocol - FTP)** permite a los sistemas principales transferir datos entre sistemas principales diferentes, así como archivos entre dos sistemas principales externos de forma indirecta.

**FTP** proporciona tareas tales como listar directorios remotos, cambiar el directorio remoto actual, crear y eliminar directorios remotos y transferir varios archivos en una sola petición. **FTP** mantiene el transporte seguro pasando contraseñas de usuario y cuenta al sistema principal externo. Aunque **FTP** está principalmente diseñado para que lo utilicen las aplicaciones, también permite sesiones interactivas orientadas al usuario.

**FTP** utiliza la entrega de corriente fiable (**TCP/IP**) para enviar los archivos y utiliza una conexión Telnet para transferir mandatos y respuestas. **FTP** también interpreta varios formatos de archivo básicos incluyendo NETASCII, IMAGE y Local 8.

**TCP/IP** implementa **FTP** en el mandato de usuario **ftp** y el mandato de servidor **ftpd** y no proporciona ninguna interfaz de programación de aplicaciones (API) a este protocolo.

Al crear usuarios y directorios ftp anónimos, asegúrese de que el directorio inicial para los usuarios ftp anónimos (por ejemplo /u/ftp) sea propiedad de root y no otorgue permisos de grabación (por ejemplo dr-xr-xr-x). El script /usr/samples/tcpip/anon.ftp se puede utilizar para crear estas cuentas, archivos y directorios.

#### Trivial File Transfer Protocol

**Trivial File Transfer Protocol (TFTP)** puede leer y grabar archivos en un sistema principal externo.

Puesto que **TFTP** utiliza el protocolo **User Datagram Protocol** no fiable para transportar archivos, generalmente es más rápido que **FTP**. Igual que **FTP**, **TFTP** puede transferir archivos como caracteres NETASCII o como datos binarios de 8 bits. A diferencia de **FTP**, **TFTP** no se puede utilizar para listar o cambiar directorios en un sistema principal externo y no toma medidas para la seguridad como la protección por contraseña. Asimismo, los datos sólo se pueden grabar o recuperar en directorios públicos.

**TCP/IP** implementa **TFTP** en los mandatos de usuario **tftp** o **utftp** y en el mandato de servidor **ftftpd**. El mandato **utftp** es una forma del mandato **ftftpd** para utilizarla en un conducto. **TCP/IP** no proporciona una API en este protocolo.

#### Protocolo Name/Finger

El **Protocolo de nombres/finger (FINGER)** es un protocolo de Internet a nivel de aplicación que proporciona una interfaz entre el mandato **finger** y el daemon **fingerd**.

El daemon **fingerd** devuelve información sobre los usuarios conectados actualmente a un sistema principal remoto especificado. Si ejecuta el mandato finger especificando un usuario en un sistema

principal determinado, obtendrá información específica sobre dicho usuario. El Protocolo **FINGER** debe estar presente en el sistema principal remoto y en el sistema principal solicitante. **FINGER** utiliza **Transmission Control Protocol** (“Protocolo de control de transmisiones (Transmission Control Protocol)” en la página 161) como protocolo subyacente.

**Nota:** **TCP/IP** no proporciona una API en este protocolo.

### Protocolo Telnet

El **Protocolo Telnet (TELNET)** proporciona un método estándar para que los dispositivos de terminal y los procesos orientados a terminal intercambien información.

Normalmente los programas de emulación de terminal que le permiten iniciar la sesión en un sistema principal remoto utilizan **TELNET**. Sin embargo, **TELNET** se puede utilizar para las comunicaciones de terminal a terminal y las comunicaciones entre procesos. **TELNET** también lo utilizan otros protocolos (por ejemplo **FTP**) para establecer un canal de control de protocolo.

**TCP/IP** implementa **TELNET** en los mandatos de usuario **tn**, **telnet** o **tn3270**. El daemon **telnetd** no proporciona ninguna API en **TELNET**.

**TCP/IP** soporta las siguientes opciones de **TELNET** que se negocian entre el cliente y el servidor.

Item	Descripción
<b>BINARY TRANSMISSION</b> (Se utiliza en sesiones <b>tn3270</b> )	Transmite caracteres como datos binarios.
<b>SUPPRESS GO_AHEAD</b> (El sistema operativo suprime las opciones GO-AHEAD.)	Indica que cuando está en vigor en una conexión entre un remitente de datos y el destinatario de los datos, el remitente no transmite una opción GO_AHEAD. Si no se desea la opción GO_AHEAD, las partes de la conexión probablemente la suprimirán en ambas direcciones. Esta acción debe tener lugar en ambas direcciones de forma independiente.
<b>TIMING MARK</b> (Se reconoce, pero tiene una respuesta negativa)	Se asegura de que los datos transmitidos anteriormente se han procesado por completo.
<b>EXTENDED OPTIONS LIST</b>	Amplía la lista de opciones de <b>TELNET</b> en 256 opciones más. Sin esta opción, la opción <b>TELNET</b> sólo permite 256 opciones.
<b>ECHO</b> (Mandato cambiable por el usuario)	Devuelve la transmisión de caracteres de datos de eco ya recibidos al remitente original.
<b>TERM TYPE</b>	Permite al servidor determinar el tipo de terminal conectado a un programa <b>TELNET</b> de usuario.
<b>SAK</b> (Tecla de atención de seguridad)	Establece el entorno necesario para las comunicaciones seguras entre el usuario y el sistema.
<b>NAWS</b> (Negociar el tamaño de ventana)	Permite al cliente y al servidor negociar dinámicamente el tamaño de ventana. La utilizan las aplicaciones que soportan el cambio de tamaño de ventana.

**Nota:** **TELNET** debe permitir la transmisión de caracteres de ocho bit cuando no está en modalidad binaria para implementar la página de códigos ISO 8859 Latin.

### Protocolo de red local de Red de sistemas distribuidos

Un sistema autónomo es un grupo de redes y pasarelas de las que es responsable una autoridad administrativa.

El **Protocolo de red local (HELLO)** es un protocolo de pasarela interior diseñado para utilizarse en sistemas autónomos. (Para obtener más información, consulte el apartado “[Exterior Gateway Protocol \(Protocolo de pasarela exterior\)](#)” en la página 165.) **HELLO** mantiene la información de conectividad, direccionamiento y mantenimiento de la hora. Permite a cada máquina de la red determinar la vía de

acceso más corta a un destino basándose en el retardo de tiempo y, a continuación, actualiza dinámicamente la información de direccionamiento en dicho destino.

Para obtener más información, consulte el daemon [\*\*gated\*\*](#).

### **Protocolo de ejecución remota de mandatos**

El mandato de usuario **rexec** y el daemon **rexecd** proporcionan el protocolo de ejecución de mandatos remota, permitiendo a los usuarios ejecutar mandatos en un sistema principal remoto compatible.

Para obtener más información, consulte el mandato [\*\*rexec\*\*](#) y el daemon [\*\*rexecd\*\*](#).

### **Remote Login Protocol (Protocolo de inicio de sesión remoto)**

El mandato de usuario **rlogin** y el daemon **rlogind** proporciona el **protocolo de inicio de sesión remoto**, permitiendo a los usuarios iniciar la sesión en un sistema principal remoto y utilizar los terminales como si estuvieran conectados directamente al sistema principal remoto.

Para obtener más información, consulte el mandato [\*\*rlogin\*\*](#) y el daemon [\*\*rlogind\*\*](#).

### **Remote Shell Protocol (Protocolo de shell remoto)**

El mandato de usuario **rsh** y el daemon **rshd** proporcionan el **protocolo de shell de mandato remoto**, permitiendo a los usuarios abrir un shell en un sistema principal externo compatible para ejecutar mandatos.

Para obtener más información, consulte el mandato [\*\*rsh\*\*](#) y el daemon [\*\*rshd\*\*](#).

### **Protocolo Wake On LAN**

**Wake On LAN (WOL)** le permite activar uno o más sistemas principales que están conectados a una red en modalidad suspendida enviando un Paquete mágico a la dirección o las direcciones especificadas de la subred especificada.

Para obtener más información sobre cómo utilizar **WOL**, consulte el mandato [\*\*wol\*\*](#).

### **Routing Information Protocol (Protocolo de información de direccionamiento)**

**Protocolo de información de direccionamiento (Routing Information Protocol - RIP)** y los daemons **routed** y **gated** que lo implementan hacen el seguimiento de la información de direccionamiento basándose en los saltos de pasarela y mantienen las entradas de tabla de direccionamiento de kernel.

Para obtener más información, consulte los daemons [\*\*routed\*\*](#) y [\*\*gated\*\*](#).

### **Time Server Protocol (Protocolo de servidor horario)**

El daemon **timed** se utiliza para sincronizar un sistema principal con la hora de los demás sistemas principales.

Se basa en el concepto de cliente/servidor. Para obtener más información, consulte el mandato [\*\*timedc\*\*](#) y el daemon [\*\*timed\*\*](#).

### **Números asignados**

Por compatibilidad con el entorno de red general, se asignan números conocidos públicamente para las versiones, las redes, los puertos, los protocolos y las opciones de protocolo de Internet. Adicionalmente, también se asignan nombres conocidos públicamente a máquinas, redes, sistemas operativos, protocolos, servicios y terminales.

**TCP/IP** se ajusta a los números y nombres asignados definidos en la RFC 1010, *Números asignados*.

El **Protocolo Internet (IP)** define un campo de 4 bits en la cabecera **IP** que identifica la versión del protocolo entre redes general en uso. Para **IP**, este número de versión es 4. Si desea detalles sobre los números y nombres asignados utilizados por **TCP/IP**, consulte los archivos */etc/protocols* y */etc/*

services incluidos con **TCP/IP**. Para obtener detalles adicionales sobre los números y nombres asignados, consulte la RFC 1010 y el archivo /etc/services.

## **Tarjetas adaptadoras de red de área local TCP/IP**

La tarjeta adaptadora de red es el hardware que se conecta físicamente al cableado de red. Es responsable de recibir y transmitir datos a nivel físico.

La tarjeta adaptadora de red está controlada por el controlador de dispositivo de adaptador de red.

Una máquina debe tener una tarjeta adaptadora de red (o conexión) para cada red (no tipo de red) a la que se conecta. Por ejemplo, si un sistema principal se conecta a dos Redes en anillo, debe tener dos tarjetas adaptadoras de red.

**TCP/IP** utiliza las tarjetas adaptadoras de red y las conexiones siguientes:

- Ethernet Versión 2 estándar
- IEEE 802.3
- Red en anillo
- Adaptadores asíncronos y puertos serie nativos
- FDDI (Fiber Distributed Data Interface - Interfaz de datos distribuidos por fibra)
- Convertidor de canal óptico serie (se describe en la publicación *Kernel Extensions and Device Support Programming Concepts*)
- Canal de fibra

Las tecnologías de red Ethernet y 802.3 utilizan el mismo tipo de adaptador.

Cada máquina proporciona un número limitado de ranuras de expansión, algunas de las cuales o todas las cuales puede desear utilizar para los adaptadores de comunicaciones. Adicionalmente, cada máquina soporta un número limitado de adaptadores de comunicaciones de un tipo determinado. Dentro de estos límites (limitaciones de software), puede instalar cualquier combinación de adaptadores hasta el número total de ranuras de expansión disponibles en la máquina (limitaciones de hardware).

Sólo se puede configurar una interfaz **TCP/IP (Transmission Control Protocol/Internet Protocol)** independientemente del número de Convertidores de canal óptico serie soportados por el sistema. El controlador de dispositivo óptico serie utiliza ambos convertidores de canal aunque sólo se haya configurado una interfaz **TCP/IP** lógica.

### **Instalación de un adaptador de red**

Siga este procedimiento para instalar un adaptador de red.

Para instalar un adaptador de red:

1. Apague el sistema. Consulte el mandato [shutdown](#) si desea información sobre cómo apagar un sistema.
2. Apague la alimentación del sistema.
3. Extraiga la caja del sistema.
4. Busque una ranura libre e inserta el adaptador de red. Tenga cuidado en colocar el adaptador en la ranura correctamente.
5. Vuelva a colocar la caja del sistema.
6. Reinicie el sistema.

### **Configuración y gestión de los adaptadores**

Para configurar y gestionar adaptadores de red en anillo o Ethernet, utilice las tareas de la tabla siguiente.

Tabla 60. Configuración y gestión de las tareas de los adaptadores

Tarea	Vía rápida de SMIT	Mandato o archivo
Configurar un adaptador	smit chgtok (red en anillo) smit chgenet (Ethernet)	<ol style="list-style-type: none"> <li>Determine el nombre del adaptador:<sup>1</sup>  <code>lsdev -C -c adaptador -t tokenring -H o lsdev -C -c adaptador -t ethernet -H</code></li> <li>Restablezca la velocidad del anillo (red en anillo) o el tipo de conector (Ethernet), en caso necesario. Por ejemplo: <code>chdev -l tok0 -a ring_speed=16 -P o chdev -l ent0 -a bnc_select=dix -P</code></li> </ol>
Determinar una dirección de hardware del adaptador de red	smit chgtok (red en anillo) smit chgenet (Ethernet)	<code>lscfg -l tok0 -v (token-ring)<sup>2</sup> lscfg -l ent0 -v (Ethernet)<sup>2</sup></code>
Establecer una dirección de hardware alternativa	smit chgtok (red en anillo) smit chgenet (Ethernet)	<ol style="list-style-type: none"> <li>Defina la dirección de hardware alternativa. Por ejemplo, para red en anillo:<sup>2,3</sup>  <code>chdev -l tok0 -a alt_addr=0X10005A4F1B7F</code>            Para Ethernet:<sup>2,3</sup>  <code>chdev -l ent0 -a alt_addr=0X10005A4F1B7F -p</code></li> <li>Empiece a utilizar la dirección alternativa para red en anillo:<sup>4</sup>  <code>chdev -l tok0 -a use_alt_addr=yes</code>            Para Ethernet:<sup>4</sup>  <code>chdev -l ent0 -a use_alt_addr=yes</code></li> </ol>

**Nota:**

- El nombre del adaptador de red puede cambiar si se mueve de una ranura a otra o si se elimina del sistema. Si alguna vez mueve el adaptador, utilice el mandato **diag -a** para actualizar la base de datos de configuración.
- Sustituya `tok0` y `ent0` por el nombre del adaptador.
- Sustituya `0X10005A4F1B7F` por su dirección de hardware.
- Después de realizar este procedimiento, es posible que observe una interrupción de la configuración con otros sistemas principales hasta que éstos descarten la memoria caché del protocolo de resolución de dirección (ARP) y obtengan la nueva dirección de hardware de este sistema principal.

#### Redes de área local virtuales (VLAN)

Las VLAN (redes de área local virtuales) pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas.

Esta implementación proporciona soporte al estándar de identificación IEEE 802.1Q VLAN con la posibilidad de permitir que en los adaptadores Ethernet se ejecuten varios ID de VLAN. Cada ID de VLAN está asociado a las capas superiores (IP, etc) con una interfaz de Ethernet independiente y crea instancias lógicas del adaptador Ethernet para cada VLAN, por ejemplo, `ent1`, `ent2` y así sucesivamente.

El soporte de VLAN IEEE 802.1Q puede configurarse a través de cualquier adaptador Ethernet soportado. Los adaptadores deben conectarse a un conmutador que proporcione soporte a IEEE 802.1Q VLAN.

Es posible configurar varios dispositivos lógicos VLAN en un solo sistema. Cada dispositivo lógico VLAN constituye una instancia adicional del adaptador Ethernet. Estos dispositivos lógicos pueden utilizarse para configurar las mismas interfaces IP de Ethernet que se utilizan con los adaptadores Ethernet físicos. En este caso, el valor *ifsize* de la opción **no** (0 por omisión), debe aumentarse para incluir no sólo las interfaces Ethernet para cada adaptador, sino los dispositivos lógicos VLAN que estén configurados. Consulte la documentación del mandato **no**.

Cada VLAN puede tener un valor distinto para la unidad de transmisión máxima (MTU) aunque comparta un solo adaptador Ethernet físico.

El soporta a VLAN se gestiona a través de SMIT. Escriba la vía rápida **smit vlan** desde la línea de mandatos y seleccione desde el menú principal de VLAN. Estará disponible ayuda en línea.

Después de configurar la VLAN, configure la interfaz IP, por ejemplo, **en1** para Ethernet estándar o **et1** para IEEE 802.3, utilizando SMIT o mandatos.

AIX 5.3 y versiones posteriores proporciona soporte a Ethernet virtual utilizando un conmutador de E/S virtual como método para realizar la comunicación en memoria entre particiones en un sistema POWER5. El conmutador también proporciona soporte a la identificación IEEE 802.1Q, que permite que los adaptadores Ethernet virtuales pertenezcan a distintas VLAN del conmutador. Los adaptadores Ethernet virtuales se crean y configuran en las particiones utilizando la Consola de gestión de hardware (HMC). Una vez creado, la partición verá el adaptador Ethernet virtual en el árbol de firmware que se abra cuando explore los dispositivos. Después de detectarse, el adaptador Ethernet virtual se configura y utiliza igual que un adaptador Ethernet físico. Para obtener más información, consulte la documentación del hardware del sistema POWER5.

**Nota:**

- Si intenta configurar un valor de ID de VLAN que ya se está utilizando para el adaptador especificado, la configuración falla y aparece el error siguiente:

```
Error de método (/usr/lib/methods/chgvlan):  
 0514-018 Los valores especificados para los atributos siguientes  
    no son válidos:  
      id_identificador_vlan    ID identificador VLAN
```

- Si un usuario (por ejemplo, una interfaz IP) actualmente está utilizando el dispositivo lógico VLAN, los intentos de eliminar el dispositivo lógico VLAN fallarán. Se muestra un mensaje similar al siguiente:

```
Error de método (/usr/lib/methods/ucfgcommo):  
 0514-062 No se puede realizar la función solicitada porque el  
    dispositivo especificado está ocupado.
```

Para eliminar el dispositivo lógico VLAN, desconecte al usuario primero. Por ejemplo, si el usuario es la interfaz IP **en1**, puede utilizar el mandato siguiente:

```
ifconfig en1 detach
```

Entonces puede eliminar la interfaz de red utilizando los menús TCP/IP de SMIT.

- Si un usuario (por ejemplo, una interfaz IP) actualmente está utilizando el dispositivo lógico VLAN, los intentos de cambiar la característica de VLAN (el ID de identificación de VLAN o el adaptador base) fallarán. Se muestra un mensaje similar al siguiente:

```
Error de método (/usr/lib/methods/chgvlan):  
 0514-062 No se puede realizar la función solicitada porque el  
    dispositivo especificado está ocupado.
```

Para cambiar el dispositivo lógico VLAN, desconecte al usuario primero. Por ejemplo, si el usuario es la interfaz IP **en1**, puede utilizar el mandato siguiente:

```
ifconfig en1 detach
```

Entonces puede cambiar la VLAN y volver a añadir la interfaz de red utilizando los menús TCP/IP de SMIT.

### **Resolución de problemas con VLAN**

Es posible utilizar **tcpdump** y **trace** para la resolución de problemas con VLAN.

A continuación se muestra el ID de enganche para cada tipo de transmisión de paquetes:

Item	Descripción
transmisión de paquetes	3FD
recepción de paquetes	3FE
Otros sucesos	3FF

El mandato **entstat** proporciona las estadísticas de agregación del adaptador físico para el que la VLAN está configurada. *No* proporciona las estadísticas individuales para este tipo de dispositivo lógico VLAN en concreto.

### **Restricciones de VLAN**

El vuelco remoto no está soportado a través de una VLAN. Además, los dispositivos lógicos VLAN no pueden utilizarse para crear un Etherchannel de Cisco Systems.

## **Interfaces de red TCP/IP**

La capa de interfaz de red **TCP/IP** formatea los datagramas IP de la capa de red en paquetes que las tecnologías de red específicas pueden interpretar y transmitir.

Una interfaz de red es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.

La capa IP selecciona la interfaz de red apropiada basándose en la dirección de destino del paquete que se debe transmitir. Cada interfaz de red tiene una dirección de red. La capa de interfaz de red es responsable de añadir o eliminar cualquier cabecera de protocolo de capa de enlace necesaria para entregar un mensaje a su destino. El controlador de dispositivo de **adaptador de red** controla la tarjeta adaptadora de red.

Aunque no es necesario, una interfaz de red se suele asociar con un adaptador de red. Por ejemplo, la interfaz de bucle de retorno no tiene ningún adaptador de red asociado. Una máquina debe tener una tarjeta adaptadora de red para cada red (no tipo de red) a la que se conecta. Sin embargo, una máquina sólo necesita una copia del software de interfaz de red para cada adaptador de red que utiliza. Por ejemplo, si un sistema principal se conecta a dos Redes en anillo, debe tener dos tarjetas adaptadoras de red. Sin embargo, sólo se necesita una copia del software de interfaz de **Red en anillo** y una copia del controlador de dispositivo de Red en anillo.

**TCP/IP** soporta los tipos de interfaces de red:

- Ethernet Versión 2 estándar (en)
- IEEE 802.3 (et)
- Red en anillo (tr)
- **SLIP (Serial Line Internet Protocol)**
- Bucle de retorno (lo)
- FDDI
- Óptica serie (so)
- **PPP (Point-to-Point Protocol - Protocolo de punto a punto)**
- Dirección IP virtual (vi)

Las interfaces Ethernet, 802.3 y de Red en anillo son para utilizarse con las redes de área local (LAN). La interfaz **SLIP** es para utilizarse con conexiones serie. La interfaz de bucle de retorno la utiliza un sistema principal para devolverse mensajes a sí mismo. La interfaz Óptica serie es para utilizarse con redes ópticas de punto a punto utilizando el Manejador de dispositivos de enlace óptico serie. El **Protocolo de punto a punto** se utiliza normalmente cuando se conecta a otro sistema o red a través de un módem. La

interfaz de Dirección IP virtual (también denominada *interfaz virtual*) no está asociada con ningún adaptador de red determinado. Se pueden configurar varias instancias de una interfaz virtual en un sistema principal. Cuando se configuran interfaces virtuales, la dirección de la primera interfaz virtual se convierte en la dirección de origen a menos que una aplicación haya elegido una interfaz diferente. Los procesos que utilizan una dirección IP virtual como dirección de origen pueden enviar paquetes a través de cualquier interfaz de red que proporcione la mejor ruta para dicho destino. Los paquetes de entrada destinados a una dirección IP virtual se entregan al proceso independientemente de la interfaz a través de la cual llegan.

### **Configuración automática de interfaces de red**

Cuando se instala físicamente en el sistema un adaptador de red nuevo, el sistema operativo añade automáticamente la interfaz de red apropiada para dicho adaptador.

Por ejemplo, si instala un adaptador de red en anillo en el sistema, el sistema operativo le asigna el nombre `tok0` y añade una interfaz de red en anillo denominada `tr0`. Si instala un adaptador Ethernet en el sistema, el sistema operativo le asigna el nombre `ent0` y añade una interfaz Ethernet Versión 2 y una interfaz IEEE 802.3, denominadas `en0` y `et0` respectivamente.

En la mayoría de los casos, hay una correspondencia de uno a uno entre los nombres de adaptador y los nombres de interfaz de red. Por ejemplo, el adaptador de red en anillo `tok0` corresponde a la interfaz `tr0`, el adaptador `tok1` corresponde a la interfaz `tr1`, etc. De forma similar, el adaptador Ethernet `ent0` corresponde a la interfaz `en0` (para Ethernet Versión 2) y `et0` (para IEEE 802.3) y el adaptador `ent1` corresponde a la interfaz `en1` (para Ethernet Versión 2) y `et1` (para IEEE 802.3).

**Nota:** En circunstancias normales, no necesita suprimir ni añadir una interfaz de red manualmente. Sin embargo, es posible que algunos procedimientos de determinación de problemas requieran que lo haga. En este caso, utilice la vía de acceso rápida de SMIT, `smit inet`, para suprimir y volver a añadir la interfaz adecuada.

### **Valores de configuración predeterminados para TCP/IP**

En cada arranque de sistema, el sistema operativo configura automáticamente el software de interfaz de red basándose en la información de la base de datos ODM. Inicialmente, la interfaz de red se configura con valores predeterminados.

Para comunicarse a través de una interfaz de red determinada, se debe establecer la dirección de Internet. Éste es el único atributo que es necesario establecer. Todos los demás atributos necesarios pueden utilizar los valores predeterminados. A continuación se proporcionan los valores predeterminados para cada interfaz de red.

#### **Valores de Ethernet predeterminados para TCP/IP**

Los valores de los atributos de adaptador de red Ethernet válidos se pueden cambiar utilizando el menú Selección de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
<code>netaddr</code>		
<code>state</code>	<code>down</code>	<code>up, down, detach</code>
<code>arp</code>	<code>yes</code>	<code>yes, no</code>
<code>netmask</code>		
<code>difusión</code>		

Se muestra el siguiente atributo de controlador de dispositivo de red Ethernet válido junto con los valores predeterminados, que se pueden cambiar utilizando el menú Controladores de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
<code>mtu</code>	1500	60 a 1500

### **Valores de 802.3 predeterminados para TCP/IP**

Los valores de los atributos de adaptador de red 802.3 válidos se pueden cambiar utilizando el menú Selección de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
netaddr		
state	down	up, down, detach
arp	yes	yes, no
netmask		
difusión		

Se muestra el siguiente atributo de controlador de dispositivo de red 802.3 válido junto con los valores predeterminados, que se pueden cambiar utilizando el menú Controladores de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
mtu	1492	60 a 1492

### **Valores de Red en anillo predeterminados para TCP/IP**

Los valores de los atributos de adaptador de red token-ring válidos se pueden cambiar utilizando el menú Selección de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
netaddr		
netmask		
state	down	up, down, detach
arp	yes	yes, no
hwloop	no	yes, no
netmask		
difusión		
allcast	no	yes, no

Se muestra el siguiente atributo de controlador de dispositivo de red token-ring válido junto con los valores predeterminados, que se pueden cambiar utilizando el menú Controladores de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
mtu (4 Mbps)	1500	60 a 4056
mtu (16 Mbps)	1500	60 a 17960

**Nota:** Cuando se opera a través de un puente, el valor predeterminado de 1500 para la unidad de transmisión máxima (MTU) se deberá cambiar a un valor que sea 8 menos que el campo de información máxima (I-frame máximo) anunciado por el puente en el campo de control de direccionamiento. Por ejemplo, si el valor de I-frame máximo es 1500 en el campo de control de direccionamiento, el tamaño de MTU se debe establecer en 1492. Esto sólo se aplica a interfaces de red en anillo. Para obtener más información, consulte el apartado “Problemas de TCP/IP con un puente de Red en anillo a Red en anillo” en la página 506.

Al utilizar el adaptador de red en anillo IBM® 16/4 PowerPC (ISA), la MTU está restringida a 2000.

### **Valores de SLIP predeterminados para TCP/IP**

Los valores de los atributos de adaptador de red SLIP válidos se pueden cambiar utilizando el menú Selección de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
netaddr		
dest		
state	up	up, down, detach
netmask		

Se muestra el siguiente atributo de controlador de dispositivo de red SLIP válido junto con los valores predeterminados, que se pueden cambiar utilizando el menú Controladores de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
mtu	1006	60 a 4096

### **Valores ópticos serie predeterminados para TCP/IP**

Los valores del convertidor válido de canal de red óptica serie se pueden cambiar los valores utilizando el menú Selección de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
netaddr		
state	down	up, down, detach
netmask		

Se muestra el siguiente atributo de manejador de dispositivo de red óptica serie válido junto con los valores predeterminados tal como se muestra en el menú Controladores de interfaz de red de SMIT.

Atributo	Valor predeterminado	Valores posibles
mtu	61428	1 a 61428

### **Implicaciones de varias interfaces de red en la misma red**

Si se conectan varias interfaces de red a una sola red, cada interfaz debe tener una dirección IP exclusiva.

La característica de direccionamiento de varias vías permite añadir rutas a la tabla de direccionamiento de IP para interfaces de varias vías de la misma subred. Esto permite que el tráfico de salida alterne entre las interfaces en lugar de enviarse sólo a través de una interfaz.

### **Gestión de interfaz de red**

Para gestionar interfaces de red, utilice la Red WSM, la Vía rápida (aplicación) o las tareas de esta tabla.

Tabla 61. Tareas de gestión de interfaces de red		
Tarea	Vía rápida de SMIT	Mandato o archivo
Listar todos los dispositivos de red	smit lsinet	lsdev -C -c if
Configurar un dispositivo de red	smit chinet	Consulte el mandato <b>ifconfig</b> y el archivo <b>rc.net</b>
Cambiar la información de interfaz de red con /usr montado de forma remota	smit chdev <sup>1,2</sup>	chgif <sup>1,2</sup>

Tabla 61. Tareas de gestión de interfaces de red (continuación)		
Tarea	Vía rápida de SMIT	Mandato o archivo
Obtener estadísticas para una interfaz de red		<code>netstat -v</code>

**Nota:**

1. Los cambios de un /usr montado de forma remota sólo afectan a la Base de datos de información (ODM) hasta que se reinicia la red o hasta que se utiliza el mandato **ifconfig** para que los cambios entren en vigor inmediatamente.
2. Cuando utilice un /usr montado de forma remota, tenga cuidado de no modificar la interfaz que se está utilizando, porque ésa es la ubicación de las bibliotecas, los mandatos y el kernel.

#### Opciones de red específicas de interfaz

Para lograr un rendimiento de red de alta velocidad (100 Mb o más) bueno, se deben ajustar especialmente las interfaces **TCP/IP**. Este esfuerzo se complica por el hecho de que en un solo sistema se pueden utilizar varias interfaces de red y una combinación de interfaces **TCP/IP** tradicionales y de alta velocidad.

En el sistema operativo AIX, las Opciones de red específicas de interfaz (ISNO) permiten a los administradores del sistema ajustar cada interfaz de **TCP/IP** individualmente para obtener un rendimiento óptimo.

Hay cinco parámetros ISNO para cada interfaz soportada: **rfc1323**, **tcp\_nodelay**, **tcp\_sendspace**, **tcp\_recvspace** y **tcp\_mssdflt**. Cuando se establecen, los valores de estos parámetros prevalecen sobre los parámetros de todo el sistema de los mismos nombres que se habían establecido con el mandato **no**. Cuando no se establecen opciones ISNO para una interfaz determinada, se utilizan opciones para todo el sistema. Cuando una aplicación ha establecido opciones para un socket determinado utilizando la subrutina **setsockopt**, dichas opciones prevalecen sobre las ISNO.

La opción de red **use\_isno**, establecida con el mandato **no**, debe tener un valor de 1 para que las ISNO entren en vigor. El valor predeterminado para **use\_isno** es 1.

Algunos adaptadores de alta velocidad tienen los parámetros ISNO establecidos de forma predeterminada en la base de datos ODM.

Las interfaces Gigabit Ethernet, cuando se configuran para utilizar una MTU de 9000, utilizan de forma predeterminada los siguientes valores de ISNO:

Nombre	Valor de AIX 4.3.3	Valor de AIX 4.3.3 (4330-08)	Valor de AIX 5.1 (y posterior)
tcp_sendspace	131072	262144	262144
tcp_recvspace	92160	131072	131072
rfc1323	1	1	1

Las interfaces Gigabit Ethernet, cuando se configuran para utilizar una MTU de 1500, utilizan de forma predeterminada los siguientes valores de ISNO:

Nombre	Valor de AIX 4.3.3	Valor de AIX 4.3.3 (4330-08)	Valor de AIX 5.1 (y posterior)
tcp_sendspace	65536	131072	131072
tcp_recvspace	16384	65536	65536
rfc1323	0	no establecido	no establecido

Las interfaces FDDI, cuando se configuran para utilizar una MTU de 4352, utilizan de forma predeterminada los siguientes valores de ISNO:

Nombre	Valor
tcp_sendspace	45046
tcp_recvspace	45046

Los parámetros de ISNO no se pueden visualizar o cambiar utilizando SMIT. Se pueden establecer utilizando el mandato **chdev** o el mandato **ifconfig**. El mandato **ifconfig** sólo cambia los valores hasta el siguiente rearranque. El mandato **chdev** cambia los valores en la base de datos de ODM para que se utilicen en los rearranques posteriores. Se puede utilizar el mandato **lsattr** o el mandato **ifconfig** para visualizar los valores actuales.

Los ejemplos siguientes muestran mandatos que en primer lugar se pueden utilizar para verificar el soporte de sistema y de interfaz y, a continuación, para establecer y verificar los valores nuevos.

1. Verifique el soporte general de sistema e interfaz utilizando los mandatos **no** y **lsattr**.

- Asegúrese de que la opción **use\_isno** esté habilitada utilizando un mandato similar al siguiente:

```
$ no -a | grep isno
use_isno=1
```

- Asegúrese de que la interfaz soporte los cinco ISNO nuevos utilizando el mandato **lsattr -El**, como se muestra a continuación:

```
$ lsattr -E -l en0 -H
atributo           valor  descripción
rfc1323            N/A
tcp_nodelay        N/A
tcp_sendspace      N/A
tcp_recvspace       N/A
tcp_mssdfilt       N/A
```

2. Establezca los valores específicos de interfaz, utilizando el mandato **ifconfig** o **chdev**. El mandato **ifconfig** establece los valores temporalmente, lo cual se recomienda para realizar pruebas. El mandato **chdev** modifica el ODM, de modo que los valores personalizados permanecen válidos después del rearranque.

- Establezca **tcp\_recvspace** y **tcp\_sendspace** en 64 K y habilite **tcp\_nodelay** utilizando uno de los siguientes:

```
$ ifconfig en0 tcp_recvspace 65536 tcp_sendspace 65536 tcp_nodelay 1
$ chdev -l en0 -a tcp_recvspace=65536 -a tcp_sendspace=65536 -a tcp_nodelay=1
```

- De forma alternativa, suponiendo que el mandato **no** informe de un valor global **rfc1323=1**, el usuario root puede desactivar **rfc1323** para todas las conexiones sobre en0 con los mandatos siguientes:

```
$ ifconfig en0 rfc1323 0
$ chdev -l en0 -a rfc1323=0
```

3. Verifique los valores utilizando el mandato **ifconfig** o **lsattr**, como se muestra en el ejemplo siguiente:

```
$ ifconfig en0 <UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT>
    en0: flags=e080863
          inet 9.19.161.100 netmask 0xffffffff broadcast 9.19.161.255
              tcp_sendspace 65536 tcp_recvspace 65536 tcp_nodelay 1 rfc1323 0
$ lsattr -El en0
    rfc1323      0      N/A      True
    tcp_nodelay   1      N/A      True
    tcp_sendspace 65536  N/A      True
    tcp_recvspace 65536  N/A      True
    tcp_mssdfilt 0      N/A      True
```

## Direccionamiento TCP/IP

**TCP/IP** incluye un esquema de dirección de Internet que permite a los usuarios y las aplicaciones identificar una red o un sistema principal específicos con los que comunicarse.

Una dirección de Internet funciona igual que una dirección postal, permitiendo que los datos se direccionen al destino elegido. **TCP/IP** proporciona estándares para asignar direcciones a redes, subredes, sistemas principales y sockets así como para utilizar direcciones especiales para difusiones y bucle de retorno local.

Las direcciones de Internet están formadas por una dirección de red y una dirección de sistema principal (o local). Esta dirección de dos partes permite al remitente especificar la red así como un sistema principal específico de la red. Se asigna una dirección red oficial exclusiva a cada red cuando se conecta a otras redes de Internet. Sin embargo, si una red local no se va a conectar a otras redes de Internet, se le puede asignar cualquier dirección de red que sea cómoda para el uso local.

El esquema de direccionamiento de Internet consta de direcciones de Internet Protocol (IP) y dos casos especiales de direcciones IP: direcciones de difusión y direcciones de bucle de retorno.

### Direcciones Internet

IP (Internet Protocol) utiliza un campo de dirección de 32 bits y dos partes.

Los 32 bits están divididos en cuatro *octetos* como se muestra a continuación:

01111101 00001101 01001001 00001111

Estos números binarios se convierten en:

125 13 73 15

Las dos partes de una dirección Internet son la parte de la dirección de red y la parte de la dirección del sistema principal. Esto permite que un sistema remoto especifique tanto la red remota como el sistema principal en la red remota al enviar información. Por convenio, se utiliza el número de sistema principal 0 para hacer referencia a la propia red.

TCP/IP proporciona soporte a tres clases de direcciones Internet: la Clase A, la Clase B y la Clase C. Las distintas clases de las direcciones Internet están en función de la forma en que se asignen los 32 bits de la dirección. La clase de dirección en concreto que se asigna a una red depende del tamaño de la red.

#### Direcciones de Clase A

Una dirección de Clase A está formada por una dirección de red de 8 bits y una dirección del sistema principal o local de 24 bits.

El primer bits de la dirección de red está dedicado a indicar la clase de red con lo que quedan 7 bits para la dirección de red propiamente dicha. Como el número más alto que 7 bits pueden representar en binario es el 128, existen 128 direcciones de red de Clase A posibles. De las 128 direcciones de red posibles, dos están reservadas para casos especiales: la dirección de red 127 está reservada para las direcciones de retorno de bucle locales y una dirección de red de todo unos indica una dirección de difusión.

Hay 126 direcciones de red de Clase A posibles y 16.777.216 direcciones del sistema principal local posibles. En una dirección de Clase A, el bit más significativo se establece en 0.

Dirección de red (8 bits)	Dirección de host local (24 bits)		
01111101	00001101	01001001	00001111

**Nota:** el bit de orden superior (o primer bit) será siempre 0 en una dirección de clase A

Figura 15. Dirección de Clase A

Esta ilustración muestra una estructura típica de una dirección de Clase A. Los 8 primeros bits contienen la dirección de red (que siempre empezará por cero). Los 24 bits restantes contienen la dirección del sistema principal local.

El primer octeto de la dirección de Clase A está comprendido entre 1 y 126.

#### Direcciones de Clase B

Una dirección de Clase B está formada por una dirección de red de 16 bits y una dirección del sistema principal o local de 16 bits.

Los dos primeros bits de la dirección de red están dedicados a indicar la clase de red con lo que quedan 14 bits para la dirección de red propiamente dicha. Existen 16.384 direcciones de red posibles y 65.536 direcciones del sistema principal local. En una dirección de Clase B, los bits más significativos se establecen en 1 y 0.

Dirección de red (16 bits)	Dirección de host local (16 bits)	
10011101	00001101	01001001 00001111

**Note:** los dos bits de orden superior (o los primeros dos bits) serán siempre 1 y 0 en una dirección de clase B.

Figura 16. Dirección de Clase B

Esta ilustración muestra una estructura típica de una dirección de Clase B. Los 16 primeros bits contienen la dirección de red. Los dos bits más significativos siempre serán uno y cero. Los 16 bits restantes contienen la dirección del sistema principal local.

El primer octeto de la dirección de Clase B está comprendido entre 128 y 191.

#### Direcciones de Clase C

Una dirección de Clase C está formada por una dirección de red de 24 bits y una dirección del sistema principal local de 8 bits.

Los tres primeros bits de la dirección de red indican la clase de red, dejando 21 bits para la dirección de red real. Por lo tanto, existen 2.097.152 direcciones de red posibles y 256 direcciones del sistema principal local posibles. En una dirección de Clase C, los bits más significativos se establecen en 1-1-0.

Dirección de red (24 bits)	Dirección host local (8 bits)	
11011101	00001101 01001001	00001111

**Nota:** los tres bits de orden superior (o los tres primeros bits) serán siempre 1-1-0 en una dirección de clase C.

Figura 17. Dirección de Clase C

Esta figura muestra una estructura de dirección de clase C típica. Los primeros 24 bits contienen la dirección de red (los tres bits más significativos siempre serán 1-1-0). Los 8 bits restantes contienen la dirección del sistema principal local.

En otras palabras, el primer octeto de una dirección de Clase C está comprendido entre 192 y 223.

Al decidir la dirección de red que desea utilizar, debe tener en cuenta el número de sistemas principales locales que habrá en la red y el número de subredes que habrá en la organización. Si la organización es pequeña y la red tendrá menos de 256 sistemas principales, probablemente tenga suficiente con una dirección de Clase C. Si la organización es grande, puede que sea más conveniente utilizar una dirección de Clase B o Clase A.

**Nota:** Las direcciones de Clase D (1-1-1-0 en los bits más significativos) proporcionan direcciones de difusión múltiple y UDP/IP les proporciona soporte bajo este sistema operativo.

Las máquinas leen las direcciones en código binario. La notación convencional de las direcciones de sistema principal para Internet es *decimal con puntos*, que divide la dirección de 32 bits en cuatro campos de 8 bits. El valor binario siguiente:

0001010 00000010 00000000 00110100

puede expresarse de esta forma:

010.002.000.052 o 10.2.0.52

donde el valor de cada campo viene especificado por un número decimal y los campos van separados por puntos.

**Nota:** El mandato **hostent** reconoce las direcciones siguientes: .08, .008, .09 y .009. Las direcciones con ceros iniciales se interpretan como octales y los numerales de un octal no pueden contener el número 8 ni el 9.

TCP/IP requiere una dirección Internet exclusiva para cada interfaz de red(adaptador) de una red. Estas direcciones vienen determinadas por las entradas de la base de datos de configuración, que deben acordar con las entradas del archivo /etc/hosts o la base de datos **named** si la red utiliza un servidor de nombres.

### Direcciones de Internet utilizando ceros

Cuando una dirección de Internet de la clase C contiene un 0 como la parte de la dirección del sistema principal(por ejemplo, 192.9.200.0), TCP/IP envía una dirección comodín a través de la red.

Todas las máquinas que tengan la dirección de la clase C 192.9.200.X (donde X representa un valor entre 0 y 254) deberían responder a la petición. Esto provoca el desbordamiento de la red con peticiones a máquinas que no existen.

De forma similar, se producen problemas con las direcciones de la clase B como, por ejemplo, 129.5.0.0. Todas las máquinas que tengan la dirección de la clase B 129.5.X.X (donde X representa un valor entre 0 y 254) están obligadas a responder a la petición). En este caso, como las direcciones de la clase B cuentan con redes más grandes que las direcciones de la clase C, la red se desborda con un número de peticiones a máquinas inexistentes significativamente superior que para una red de la clase C.

### Direcciones de subred

Las direcciones de subred permiten que un sistema autónomo formado por varias redes comparten la misma dirección Internet.

La función de subred de TCP/IP también permite dividir una sola red en varias redes lógicas (subredes). Por ejemplo, una organización puede tener una sola dirección de red Internet que los usuarios externos a la organización conozcan pero configurar su red internamente en subredes departamentales. En cualquier caso, se necesitan menos direcciones de red Internet y aumentan las posibilidades de direccionamiento local.

Un campo de dirección de IP (Internet Protocol) estándar tiene dos partes: una dirección de red y una dirección local. Para hacer posibles las subredes, la parte de la dirección local de una dirección Internet está dividida en un número de subred y un número de sistema principal. La subred está identificada de forma que el sistema autónomo local pueda direccionar mensajes de forma fiable.

En la dirección Internet de Clase A básica, que está formada por una dirección de red de 8 bits y una dirección local de 24 bits, la dirección local identifica la máquina del sistema principal en concreto de la red.

Dirección de red (8 bits)	Dirección host local (24 bits)		
01111101	00001101	01001001	00001111

Figura 18. Dirección de Clase A

Esta ilustración muestra una estructura típica de una dirección de Clase A. Los 8 primeros bits contienen la dirección de red (que siempre empezará por cero). Los 24 bits restantes contienen la dirección del sistema principal local.

Para crear una dirección de subred para esta dirección Internet de Clase A, la dirección local puede dividirse en un número que identifique la red (o subred) física y un número que identifique el sistema principal de la subred. Los emisores direccionan los mensajes a la dirección de red indicada y el sistema local se encarga de redireccionar los mensajes a las subredes y los sistemas principales correspondientes. Al decidir cómo dividir la dirección local en la dirección de subred y la dirección de sistema principal, debe tenerse en cuenta el número de subredes y el número de sistemas principales de estas subredes.

En la figura siguiente, la dirección local se ha dividido en una dirección de subred de 12 bits y una dirección de sistema principal de 12 bits.

Dirección de red (8 bits)	Dirección host local (24 bits)		
Dirección de red	Dirección de subred	Dirección de host	
01111101	00001101	0100	1001 00001111

**Nota:** el bit de orden superior (o primer bit) será siempre 0 en una dirección de clase A.

*Figura 19. Dirección de Clase A con la dirección de subred correspondiente*

Esta ilustración muestra una estructura típica de una dirección de Clase A. Los 8 primeros bits contienen la dirección de red (que siempre empezará por cero). Los 24 bits restantes contienen la dirección del sistema principal local; la dirección de subred ocupa los 8 primeros bits y la dirección del sistema principal ocupa los últimos 8 bits.

Existe flexibilidad al asignar direcciones de subred y direcciones de sistema principal. Los bits de la dirección local pueden dividirse según las necesidades y el crecimiento potencial de la organización y la estructura de la red. Las únicas restricciones son las siguientes:

- `network_address` es la dirección Internet de la red.
- `subnet_address` es un campo de anchura constante para una red en concreto.
- `host_address` es un campo con una anchura de 1 bit como mínimo.

Si la anchura del campo `subnet_address` es 0, la red no se organiza en subredes y el direccionamiento con la red se realiza utilizando la dirección de red Internet.

Los bits que identifican la subred se especifican mediante una máscara de bits y, por lo tanto, no es necesario adjuntarlos en la dirección. Sin embargo, suele ser aconsejable que los bits de subred sean contiguos y se localicen como los bits más significativos de la dirección local.

### Máscaras de subred

Cuando un sistema principal envía un mensaje a un destino, el sistema debe determinar si el destino se encuentra en la misma red que el origen o si es posible llegar al destino directamente a través de una de las interfaces locales. El sistema compara la dirección de destino con la dirección del sistema principal utilizando la *máscara de subred*.

Si el destino no es local, el sistema envía un mensaje a la pasarela. La pasarela realiza la misma comparación para ver si la dirección de destino se encuentra en una red a la que puede llegar localmente.

La máscara de subred indica al sistema cuál es el esquema de particionamiento de subred. Esta máscara de bits está formada por la parte de la dirección de red y la parte de la dirección de subred de la dirección Internet.

Dirección de red (8 bits)	Dirección host local (24 bits)			
Dirección de red	Dirección de subred		Dirección de host	
01111101	00001101	0100	1001	00001111

**Dirección de clase A con la correspondiente dirección de subred**

Dirección de red (8 bits)	Dirección host local (24 bits)			
Dirección de red	Dirección de subred		Dirección de host	
Máscara de subred	Dirección de host			
01111101	00001101	0100	1001	00001111

**Dirección de clase A con la correspondiente máscara de subred**

*Figura 20. Dirección de Clase A con la dirección de subred correspondiente*

Esta ilustración muestra una estructura típica de una dirección de Clase A. Los 8 primeros bits contienen la dirección de red (que siempre empezará por cero). Los 24 bits restantes contienen la dirección del sistema principal local; la dirección de subred ocupa los 8 primeros bits y la dirección del sistema principal ocupa los últimos 8 bits.

Por ejemplo, en la figura siguiente se muestra la máscara de subred de la dirección de Clase A con el esquema de particionamiento definido anteriormente.

La máscara de subred es un conjunto de 4 bytes, igual que la dirección Internet. La máscara de subred está formada por bits altos (1(unos)) correspondientes a las posiciones de los bits de la dirección de red y de subred y por bits bajos(0(ceros)) correspondientes a las posiciones de los bits de la dirección del sistema principal. Una máscara de subred de la dirección anterior sería como la de la figura siguiente.

Dirección de red (8 bits)	Dirección host local (24 bits)			
Dirección de red	Dirección de subred		Dirección de host	
11111111	11111111	1111	0000	00000000

*Figura 21. Ejemplo de máscara de subred*

Esta ilustración muestra un ejemplo de una estructura de máscara de subred. Los 8 primeros bits contienen la dirección de red. Los 24 bits restantes contienen la dirección del sistema principal local; la dirección de subred ocupa los 8 primeros bits y la dirección del sistema principal ocupa los últimos 8 bits.

#### **Comparación de direcciones**

La dirección de destino y la dirección de red local se comparan realizando el AND lógico o el OR exclusivo en la máscara de subred del sistema principal de origen.

El proceso de comparación se resalta a continuación:

1. Realice un AND lógico de la dirección de destino y la máscara de la dirección de subred local.
2. Realice un OR exclusivo en el resultado de la operación anterior y la dirección de red local de la interfaz local. Si el resultado es todo ceros, se asume que el destino puede alcanzarse directamente a través de una de las interfaces locales.
3. Si un sistema autónomo tiene más de una interfaz (por lo tanto, más de una dirección Internet), el proceso de comparación se repite para cada interfaz local.

Por ejemplo, supongamos que hay definidas dos interfaces locales para la red del sistema principal T125. La dirección Internet y las representaciones binarias de estas direcciones se muestran en el ejemplo siguiente:

```
CLASE A 73.1.5.2 = 01001001 00000001 00000101 00000010
```

```
CLASE B 145.21.6.3 = 10010001 00010101 00000110 00000011
```

Las máscaras de subred correspondientes de las interfaces de red locales se muestran en el ejemplo siguiente:

```
CLASE A 73.1.5.2 = 11111111 11111111 11100000 00000000
```

```
CLASE B 145.21.6.3 = 11111111 11111111 11111111 11000000
```

Si se solicita a la red de origen, T125, que envíe un mensaje a una red de destino con la dirección de sistema principal 114.16.23.8 (representada en binario como:01110010 00010000 00010111 00001000), el sistema comprueba si es posible llegar al destino a través de una interfaz local.

**Nota:** La palabra clave **subnetmask** debe establecerse en la base de datos de configuración de todos los sistemas principales que deban proporcionar soporte a las subredes. Antes de poder utilizar las posibilidades de una subred, todos los sistemas principales de la subred deben proporcionarle soporte. Establezca la máscara de subred permanentemente en la base de datos de configuración utilizando el menú Selección de interfaz de red en SMIT. La máscara de subred también puede establecerse en el sistema que se ejecute utilizando el mandato **ifconfig**. Si se utiliza el mandato **ifconfig** para establecer la máscara de subred, el cambio no es permanente.

### Direcciones de difusión

TCP/IP puede enviar datos a todos los sistemas principales de una red local o a todos los sistemas principales de todas las redes conectadas directamente. Dichas transmisiones se denominan *mensajes de difusión*.

Por ejemplo, el daemon de direccionamiento **routed** utiliza los mensajes de difusión para consultar y responder a las consultas de direccionamiento.

Para que los datos se difundan a todos los sistemas principales de todas las redes conectadas directamente, se utilizan UDP (User Datagram Protocol) e IP (Internet Protocol) para enviar los datos y en la dirección de destino del sistema principal de la cabecera de IP todos los bits están establecidos en 1. Para que los datos se difundan a todos los sistemas principales de una red en concreto, todos los bits de parte de la dirección local de la dirección IP están establecidos en 0. Ninguno de los mandatos del usuario utiliza la posibilidad de difusión, aunque dichos mandatos, o programas, pueden desarrollarse.

La dirección de difusión puede modificarse temporalmente cambiando el parámetro *broadcast* del mandato **ifconfig**. Para cambiar la dirección de difusión de forma permanente, debe utilizarse la vía de acceso rápida de SMIT smit chinet. La modificación de la dirección de difusión puede resultar útil si requiere compatibilidad con versiones de software anteriores que utilicen una dirección de difusión distinta; por ejemplo, todos los ID del sistema principal están establecidos en 0.

### Direcciones de bucle de retorno locales

IP (Internet Protocol) define la dirección de red especial, 127.0.0.1, como una dirección de bucle de retorno local.

Los sistemas principales utilizan las direcciones de bucle de retorno locales para enviarse mensajes a sí mismo. La dirección de bucle de retorno local la establece el gestor de la configuración durante el proceso de arranque del sistema. El bucle de retorno local se implementa en el kernel y también puede establecerse con el mandato **ifconfig**. El bucle de retorno se invoca cuando se inicia el sistema.

## Resolución de nombres TCP/IP

Aunque las direcciones de Internet de 32 bits proporcionan a las máquinas un medio eficiente de identificar el origen y el destino de los datagramas enviados entre redes, los usuarios prefieren nombres significados que se puedan recordar fácilmente. **Transmission Control Protocol/Internet Protocol**

**(TCP/IP)** proporciona un sistema de denominación que soporta las organizaciones de redes jerárquicas y planas.

La denominación en redes planas es muy simple. Los nombres de sistema principal constan de un solo conjunto de caracteres y generalmente se administran localmente. En redes **TCP/IP** planas, cada máquina de la red tiene un archivo (`/etc/hosts`) que contiene la información de correlación de nombre con dirección de Internet para cada sistema principal de la red. La carga administrativa de mantener cada archivo de denominación de máquina actualizado aumenta a medida que aumenta el tamaño de la red **TCP/IP**. Cuando las redes **TCP/IP** llegan a tener un tamaño muy grande, como en Internet, la denominación se divide jerárquicamente. Normalmente las divisiones siguen la organización de red. En **TCP/IP**, la denominación jerárquica se conoce como *Sistema de nombres de dominio* (DNS) y utiliza el protocolo DOMAIN. El protocolo DOMAIN lo implementa el daemon **named** en **TCP/IP**.

Como en la denominación para las redes planas, la jerarquía de nombres de dominio asigna a las redes y los sistemas principales nombres simbólicos que son significativos y fáciles de recordar para los usuarios. Sin embargo, en lugar de que cada máquina de la red mantenga un archivo que contenga la correlación de nombre con dirección para todos los demás sistemas principales de la red, se seleccionan uno o más sistemas principales para que funcionen como *servidores de nombres*. Los servidores de nombres convierten (resuelven) los nombres simbólicos asignados a las redes y los sistemas principales en las direcciones eficientes de Internet utilizadas por las máquinas. Un servidor de nombres tiene información completa sobre alguna parte del dominio, conocida como *zona* y tiene *autorización* para la zona.

### Autorización de denominación

En una red plana, todos los sistemas principales de la red están administrados por una autoridad central. Esta forma de red necesita que todos los sistemas principales de la red tengan nombres de sistema principal exclusivos. En una red grande, este requisito crea un gran peso administrativo en la autoridad central.

En una red de dominio, los grupos de sistemas principales se administran por separado en una jerarquía de dominios y subdominios con estructura de árbol. En este caso, los nombres de sistema principal sólo necesitan ser exclusivos en el dominio local y la autoridad central sólo administra el *dominio raíz*. Esta estructura permite que los subdominios se administren localmente y reduce el peso en la autoridad central. Por ejemplo, el dominio raíz de Internet consta de dominios como com (organizaciones comerciales), edu (organizaciones de enseñanza), gov (organizaciones gubernamentales) y mil (grupos militares). Sólo la autoridad central puede añadir dominios de nivel superior nuevos. La denominación en el segundo nivel se delega a agentes designados de los respectivos dominios. Por ejemplo, en la figura siguiente, com tiene autorización de denominación para todos los subdominios de organización comercial que están por debajo de él. De forma similar, la denominación en el tercer nivel se delega a los agentes de ese nivel (y así sucesivamente). Por ejemplo en la figura de estructura de dominio de Internet, Century tiene autorización de denominación para los subdominios Austin, Hopkins y Charlotte.

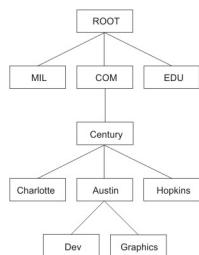


Figura 22. Estructura de dominios de Internet

Esta figura ilustra la estructura jerárquica de internet. Empieza en la parte superior con la raíz y las ramas en el siguiente nivel que contiene los dominios mil, com y edu. Bajo el dominio com, hay otro nivel que contiene Charlotte, Austin y Hopkins. Bajo Austin, están Dev y Graphics.

El subdominio Austin de Century también se puede dividir en zonas, por ejemplo Dev y Graphics. En este caso, la zona `austin.century.com` tiene todos los datos contenidos en el dominio `austin.century.com`, excepto los que se han delegado a Dev y Graphics. La zona `dev.century.com` sólo contendrá los datos delegados a Dev; no sabrá nada de Graphics, por ejemplo. La zona

`austin.century.com` (contrariamente al dominio del mismo nombre) sólo contendrá los datos no delegados a otras zonas.

### **Convenios de denominación**

En el sistema de nombres de dominio jerárquico, los nombres constan de una secuencia de subnombres no sensibles a las mayúsculas y minúsculas separados por puntos sin blancos intercalados.

El protocolo DOMAIN especifica que un nombre de dominio local debe tener menos de 64 caracteres y que un nombre de sistema principal debe tener menos de 32 caracteres de longitud. Primero se proporciona el nombre de sistema principal, una serie de nombres de dominios locales separados por puntos y finalmente el dominio raíz. Un nombre de dominio totalmente especificado para un sistema principal, incluidos los puntos, debe tener menos de 255 caracteres de longitud y debe tener el formato siguiente:

`sistemappal.subdominio1.[subdominio2 . . . subdominio].dominioraíz`

Dado que los nombres de sistema principal deben ser exclusivos en un dominio, puede utilizar un nombre abreviado al enviar mensajes a un sistema principal del mismo dominio. Por ejemplo, en lugar de enviar un mensaje a `smith.eng.1su.edu`, un sistema principal del dominio eng puede enviar un mensaje a `smith`. Adicionalmente, cada sistema principal puede tener varios alias que otros sistemas principales pueden utilizar al enviar mensajes.

### **Denominación de los sistemas principales de la red**

La finalidad de la utilización de nombres para los sistemas principales es proporcionar un procedimiento rápido, fácil y no ambiguo para hacer referencia a los sistemas de la red. Los administradores de sistema de Internet han descubierto que hay opciones correctas así como opciones no satisfactorias para los nombres de sistema principal. Estas sugerencias pretenden ayudarle a evitar peligros comunes en la elección de nombres de sistema principal.

A continuación, se proporcionan algunas sugerencias para elegir nombres de sistema principal no ambiguos y fáciles de recordar:

- Términos que se utilizan raramente, por ejemplo `sphinx` o `eclipse`.
- Nombres de tema, por ejemplo colores, elementos (por ejemplo `helio`, `argo`, o `zinc`), flores, peces y otros.
- Palabras reales (en lugar de series aleatorias de caracteres).

A continuación se muestran algunos ejemplos de elecciones no acertadas. En general, éstas opciones no son acertadas porque son difíciles de recordar o son confusas (para las personas o los sistemas):

- Términos que ya son de uso común, por ejemplo `arriba`, `abajo` o `colgar`.
- Nombres que sólo contienen números.
- Nombres que contienen signos de puntuación.
- Nombres que se basan en la distinción de mayúsculas y minúsculas, por ejemplo `Naranja` y `naranja`.
- El nombre o las iniciales del usuario principal del sistema.
- Nombres que tienen más de 8 caracteres.
- Palabras inusuales o escritas incorrectamente a propósito, por ejemplo `checq`, que se puede confundir con "cheque" o "checo".
- Nombres que son o se parecen a nombres de dominio, por ejemplo `yale.edu`.

### **Servidores de nombres**

En un espacio de nombres plano, todos los nombres se deben conservar en el archivo `/etc/hosts` de cada sistema principal de la red. Si la red es muy grande, esto puede convertirse en una carga en los recursos de cada máquina. En una red jerárquica, determinados sistemas principales designados como *servidores de nombres* resuelven los nombres en direcciones de Internet para otros sistemas principales.

Esto tiene dos ventajas respecto al espacio de nombres plano. Impide que los recursos de cada sistema principal de la red se queden inmovilizados resolviendo nombres y evita que la persona que gestiona el

sistema tenga que mantener los archivos de resolución de nombres en cada máquina de la red. El conjunto de nombres gestionados por un solo servidor de nombres se conoce como *zona de autorización*.

**Nota:** Aunque la máquina de sistema principal que realiza la función de resolución de nombres para una zona de autorización se conoce comúnmente como sistema principal de *servidor de nombres*, el proceso que controla la función, el daemon **named**, es el proceso de servidor de nombres real.

Para reducir adicionalmente la actividad de red innecesaria, todos los servidores de nombres *almacenan en antememoria* (almacenan durante un periodo de tiempo) las correlaciones de nombre con dirección. Cuando un cliente solicita a un servidor que resuelva un nombre, el servidor comprueba primero la antememoria para ver si el nombre se ha resuelto recientemente. Puesto que los nombres de dominio y de sistema principal cambian, cada elemento permanece en la antememoria durante un tiempo limitado especificado por el TTL del registro. De este modo, las autoridades pueden especificar cuánto tiempo esperan que la resolución de nombres sea precisa.

Dentro de cualquier sistema autónomo, puede haber varios servidores de nombres. Normalmente, los servidores de nombres se organizan jerárquicamente y corresponden a la organización de red. Si se toma como referencia la figura de "Estructura de dominio de Internet", cada dominio puede tener un servidor de nombres responsable de todos los subdominios del dominio. Cada servidor de nombres de subdominio se comunica con el servidor de nombres del dominio que está por encima de él (denominado servidor de nombres *padre*), así como con los servidores de nombres de otros subdominios.

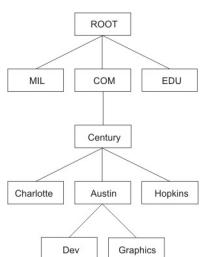


Figura 23. Estructura de dominios de Internet

Esta figura ilustra la estructura jerárquica de internet. Empieza en la parte superior con la raíz y las ramas en el siguiente nivel que contiene los dominios mil, com y edu. Bajo el dominio com, hay otro nivel que contiene Charlotte, Austin y Hopkins. Bajo Austin, están Dev y Graphics.

Por ejemplo, en la figura "Estructura de dominio de Internet", Austin, Hopkins y Charlotte son subdominios del dominio Century. Si se sigue la jerarquía de árbol en el diseño de red, el servidor de nombres de Austin se comunica con los servidores de nombres de Charlotte y Hopkins así como con el servidor de nombres padre Century. El servidor de nombres Austin también se comunica con los servidores de nombres responsables de los subdominios.

Existen varios tipos de servidores de nombres:

Item	Descripción
<b>Servidor de nombres maestro</b>	Carga los datos de un archivo o disco y puede delegar la autorización a otros servidores del dominio.

<b>Item</b>	<b>Descripción</b>
<b>Servidor de nombres esclavo</b>	Recibe la información en el arranque del sistema para una zona de autorización proporcionada de un servidor de nombres maestro y, a continuación, solicita periódicamente al servidor maestro que actualice la información. Cuando caduca el valor de renovación en el registro de recurso de inicio de autorización (SOA) en un servidor de nombres esclavo o cuando se recibe un mensaje de notificación de un servidor de nombres maestro, el esclavo vuelve a cargar la base de datos del maestro si el número de serie de la base de datos del maestro es mayor que el número de serie de la base de datos actual en el esclavo. Si llega a ser necesario forzar una nueva transferencia de zona del maestro, simplemente elimine las bases de datos esclavas existentes y renueve el daemon <b>named</b> en el servidor de nombres esclavo.
<b>Servidor de nombres de apéndice</b>	Aunque el método de duplicación de base de datos es similar al del servidor de nombres esclavo, el servidor de nombres de apéndice sólo replica los registros de servidor de nombres de la base de datos maestra en lugar de replicar la base de datos entera.
<b>Servidor intermedio</b>	Indica un servidor de nombres que sólo se basa en las sugerencias que ha creado a partir de consultas anteriores a otros servidores de nombres. El servidor de nombres intermedio responde a las consultas solicitando a otros servidores que tienen autorización para proporcionar la información necesaria si un servidor de nombres intermedio no tiene una correlación de nombre con dirección en la antememoria.
<b>Servidor de cliente o reenviador</b>	Reenvía las consultas que no puede satisfacer localmente a una lista fija de servidores de reenvío. Los servidores de sólo reenvío (un reenviador que obtiene información y la pasa a otros clientes, pero que realmente no es un servidor) no interactúa con los servidores de nombres maestros para el dominio raíz y otros dominios. Las consultas a los servidores de reenvío son repetitivas. Puede haber uno o más servidores de reenvío, que se prueban uno a uno hasta agotar la lista. Normalmente se utiliza una configuración de cliente o reenviador cuando no se desea que todos los servidores de un sitio determinado interactúen con el resto de los servidores de Internet o cuando se desea crear una antememoria grande en un número seleccionado de servidores de nombres.
<b>Servidor remoto</b>	Ejecuta todos los programas de red que utilizan el servidor de nombres sin que el proceso de servidor de nombres se ejecute en el sistema principal local. Todas las consultas las atiende un servidor de nombres que se ejecuta en otra máquina de la red.

Un sistema principal de servidor de nombres puede funcionar en diferentes capacidades para diferentes zonas de autorización. Por ejemplo, un solo sistema principal de servidor de nombres puede ser un servidor de nombres maestro para una zona y un servidor de nombres esclavo para otra zona.

## Resolución de nombres

El proceso de obtención de una dirección de Internet a partir de un nombre de sistema principal se conoce como resolución de nombres y lo realiza la subrutina `gethostbyname`.

El proceso de conversión de una dirección de Internet en un nombre de sistema principal se conoce como resolución de nombres inversa y lo realiza la subrutina `gethostbyaddr`. Estas rutinas son esencialmente accesorios en una biblioteca de rutinas de conversión de nombres que se conocen como *rutinas de resolución*.

Normalmente las rutinas de resolución de sistemas principales que ejecutan **TCP/IP** intentan resolver los nombres utilizando estas fuentes siguientes:

1. BIND/DNS (named)
2. NIS (Network Information Service - Servicio de información de red)
3. Archivo /etc/hosts local

Para resolver un nombre en una red de dominio, la rutina de resolución consulta primero la base de datos de servidores de nombres de dominio, que puede ser local si el sistema principal es un servidor de nombres de dominio o un sistema principal externo. Los servidores de nombres convierten los nombres de dominio en direcciones de Internet. El grupo de nombres del que es responsable un servidor de nombres es la zona de autorización. Si la rutina de resolución utiliza un servidor de nombres remoto, la rutina utiliza el protocolo de nombres de dominio (DOMAIN) para consultar la correlación. Para resolver un nombre de una red plana, la rutina de resolución busca una entrada en el archivo /etc/hosts local. Cuando se utiliza NIS, se busca en el archivo /etc/hosts del servidor maestro.

De forma predeterminada, las rutinas de resolución intentan resolver los nombres utilizando los recursos indicados más arriba. Primero se prueba BIND/DNS. Si el archivo /etc/resolv.conf no existe o si BIND/DNS no ha podido encontrar el nombre, se consulta NIS si está en ejecución. NIS tiene autoridad sobre el archivo /etc/hosts local, de modo que la búsqueda finaliza aquí si se está ejecutando. Si NIS no está en ejecución, se buscan en el archivo /etc/hosts local. Si ninguno de estos servicios puede encontrar el nombre, las rutinas de resolución devuelven `HOST_NOT_FOUND`. Si ninguno de los servicios está disponible, las rutinas de resolución devuelven `SERVICE_UNAVAILABLE`.

El orden predeterminado descrito anteriormente se puede sobrescribir creando el archivo de configuración /etc/irs.conf y especificando el orden deseado. Asimismo, se puede sobrescribir el orden predeterminado y el orden de /etc/irs.conf con la variable de entorno **NSORDER**. Si se define el archivo /etc/irs.conf o la variable de entorno **NSORDER**, se debe especificar como mínimo un valor junto con la opción.

Para especificar el orden de sistema principal con el archivo /etc/irs.conf:

```
hosts valor [ continue ]
```

El orden se especifica con cada método indicado en una línea él solo. El *valor* es uno de los métodos listados y la palabra clave *continue* indica que sigue otro método de resolución en la siguiente línea.

Para especificar el orden de sistema principal con la variable de entorno **NSORDER**:

```
NSORDER=valor,valor,valor
```

El orden se especifica en una línea con valores separados por comas. Están permitidos espacios en blanco entre las comas y el signo igual.

Por ejemplo, si la red local está organizada como una red plana, sólo se necesita el archivo /etc/hosts. En este ejemplo, el archivo /etc/irs.conf contiene la línea siguiente:

```
hosts local
```

Alternativamente, la variable de entorno **NSORDER** se puede establecer como:

```
NSORDER=local
```

Si la red local es una red de dominio que utiliza un servidor de nombres para la resolución de nombres un archivo /etc/hosts para la copia de seguridad, se deben especificar ambos servicios. En este ejemplo, el archivo /etc/irs.conf contiene las líneas siguientes:

```
hosts dns continue  
hosts local
```

La variable de entorno **NSORDER** se establece como:

```
NSORDER=bind,local
```

**Nota:** Los valores listados deben estar en minúsculas.

Al seguir cualquier orden de resolución definido o predeterminado, el algoritmo de búsqueda continua de una resolución a la siguiente sólo si:

- El servicio actual no está en ejecución, por consiguiente no está disponible.
- El servicio actual no puede encontrar el nombre y no tiene autoridad.

Si el archivo /etc/resolv.conf no existe, se considera que BIND/DNS no está configurado ni en ejecución y, por consiguiente, no está disponible. Si las subrutinas getdomainname y yp\_bind fallan, se considera que el servicio NIS no está configurado ni en ejecución y, por consiguiente, no está disponible. Si no se han podido abrir el archivo /etc/hosts, la búsqueda local es imposible y, por lo tanto, el archivo y el servicio no están disponibles.

Cuando un servicio de lista como *con autoridad*, significa que este servicio es el experto de los sucesores y tiene todos los nombres y las direcciones pertinentes. Las rutinas de resolución no intentan los servicios sucesores, porque es posible que los sucesores sólo contengan un subconjunto de la información del servicio con autoridad. La resolución de nombres finaliza en el servicio listado como servicio con autoridad, incluso si no encuentra el nombre (en cuyo caso, la rutina de resolución devuelve HOST\_NOT\_FOUND). Si el servicio con autoridad no está disponible, se consulta el siguiente servicio especificado.

Un origen con autoridad se especifica con la serie =auth directamente después de un valor. Se puede escribir la palabra entera, authoritative, pero sólo se utiliza la serie auth. Por ejemplo, si la variable de entorno **NSORDER** contiene lo siguiente:

```
hosts = nis=auth,dns,local
```

La búsqueda final después de la consulta NIS (si NIS se está ejecutando), independientemente de que se haya encontrado el nombre. Si NIS no se está ejecutando, se consulta el siguiente origen, que es DNS.

Los servidores de nombres **TCP/IP** utilizan el almacenamiento en antememoria para reducir el coste de la búsqueda de nombres sistemas principales en redes remotas. En lugar de buscar un nombre de nombre de sistema principal cada vez que se realiza una petición, un servidor de nombres busca primero en la antememoria para ver si se ha resuelto recientemente el nombre de sistema principal. Puesto que los nombres de dominio y de sistema principal cambian, cada elemento permanece en la antememoria durante un tiempo limitado especificado por el valor de tiempo de vida (TTL) del registro. De este modo, los servidores de nombres pueden especificar cuánto tiempo esperan que las respuestas se consideren como respuestas con autoridad.

#### **Potencial conflicto de nombres de sistema principal entre el servidor de nombres y sendmail**

En un entorno DNS, un nombre de sistema principal que se establece utilizando el mandato **hostname** desde la línea de mandatos o en el formato de archivo **rc.net** debe ser el nombre oficial del sistema principal tal como lo devuelve el servidor de nombres.

En general, este nombre es el nombre de dominio completo del sistema principal con el formato:

```
sistpral.subdominio.subdominio.dominioroot
```

**Nota:** Las rutinas de resolución necesitan que se establezca el dominio predeterminado. Si no se establece el dominio predeterminado en el mandato **hostname**, se debe establecer en el archivo /etc/resolv.conf.

Si el nombre de sistema principal no se configura como un nombre de dominio totalmente calificado y el sistema se ha configurado para utilizar el servidor de nombres de dominio junto con el programa **sendmail**, se debe editar el archivo de configuración **sendmail** (/etc/sendmail.cf) para reflejar este nombre de sistema principal oficial. Además, se deben establecer las macros de nombre de dominio de este archivo de configuración para que el programa **sendmail** funcione correctamente.

**Nota:** El dominio especificado en el archivo /etc/sendmail.cf tiene prioridad sobre el dominio establecido por el mandato **hostname** para todas las funciones **sendmail**.

#### **Potencial conflicto de nombre de dominio entre el servidor de nombres y sendmail**

Los nombres de dominio local y los servidores de nombre de dominio se especifican en diferentes archivos, en función de si el sistema principal es un servidor de nombres DOMAIN.

Para un sistema principal que está en una red DOMAIN pero que no es un servidor de nombres, el nombre de dominio local y el servidor de nombres de dominio se especifican en el archivo /etc/resolv.conf. En un sistema principal de servidor de nombres DOMAIN, el dominio local y otros servidores de nombres se definen en archivos leídos por el daemon **named** cuando éste se inicia.

#### **Protocolo de resolución de direcciones inversa**

El **RARP (Reverse Address Resolution Protocol - Protocolo de resolución de direcciones inversa)** convierte direcciones de hardware exclusivas en direcciones de Internet en el adaptador de red de área local (LAN) de Ethernet (sólo protocolo Ethernet).

Se soporta el protocolo Ethernet estándar con las restricciones siguientes:

- El servidor sólo responde a las peticiones **RARP**.
- El servidor sólo utiliza entradas de tabla **ARP** permanentes.
- El servidor no utiliza entradas de tabla **ARP** dinámicas.
- El servidor no responde automáticamente por sí solo.

El administrador del sistema debe crear y mantener manualmente una tabla de entradas **ARP** permanentes utilizando el mandato **arp**. Se debe añadir una entrada de tabla **ARP** específica en el servidor para cada sistema principal que necesite respuestas de **RARP** de un origen de autorización.

#### **Tareas de resolución de nombres (/etc/hosts) locales**

Configure el archivo /etc/hosts si la red es pequeña y está utilizando un esquema de denominación plano.

Incluso si está utilizando un esquema de denominación (o dominio) jerárquico con servidores de nombres, es posible que desee configurar el archivo /etc/hosts para identificar sistemas principales que los servidores de nombres no conocen.

Configure el sistema para la resolución de sistema principal local utilizando System Management Interface Tool (SMIT) o mandatos. Si elige el método de mandatos, asegúrese de conservar el formato del archivo /etc/hosts, tal como se describe en Hosts File Format for TCP/IP en la publicación *Referencia de archivos*.

Tabla 62. Tareas de resolución de nombres locales		
Tarea	Vía rápida de SMIT	Mandato o archivo
Listar todos los sistemas principales	<b>smit lshostent</b>	Utilice el mandato <b>hostent</b> o <b>view</b> /etc/hosts
Añadir un sistema principal	<b>smit mkhostent</b>	Utilice el mandato <b>hostent</b> o <b>edit</b> /etc/hosts
Cambiar/Mostrar características de un sistema principal	<b>smit chhostent</b>	Utilice el mandato <b>hostent</b> o <b>edit</b> /etc/hosts

Tabla 62. Tareas de resolución de nombres locales (continuación)

Tarea	Vía rápida de SMIT	Mandato o archivo
Eliminar un sistema principal	<b>smit rmhostent</b>	Utilice el mandato <b>hostent</b> o <b>edit</b> /etc/hosts

### Planificación de la resolución de nombres DOMAIN

Estas sugerencias pueden ayudarle a planificar su propio sistema de resolución de nombres DOMAIN.

Si forma parte de una red más grande, coordine la configuración del dominio y de los servidores de nombres con la autorización central.

- Debido a las amplias posibilidades de la arquitectura y configuración, familiarícese con **TCP/IP**, DNS y BIND antes de solidificar cualquier plan. Si piensa utilizar un servicio de información de red, familiarícese también con NFS y NIS. Los manuales sobre estos temas están ampliamente disponibles.
- Realice la planificación de antemano.

El cambio de un nombre es *mucho* más difícil que la configuración del nombre inicial. Obtenga el consenso de la organización respecto a la red, la pasarela, el servidor de nombres y los nombres de sistemas principales antes de configurar los archivos.

- Configure servidores de nombres redundantes.

Si no puede configurar servidores de nombres redundantes, asegúrese de configurar servidores de nombres esclavos e intermedios para tener algún tipo de copia de seguridad.

- Al seleccionar los servidores de nombres, tenga presente lo siguiente:

- Elija las máquinas que estén físicamente más cerca de los sistemas exteriores.
- Los servidores de nombres deben ser lo más independientes posible. Pruebe diferentes fuentes de alimentación y cableado independiente.
- Busque otra red para hacer una copia de seguridad del servidor de resolución de nombres y realice lo mismo para otras redes.

- Pruebe los servidores.

- Pruebe la resolución de nombres normal y la inversa.
- Pruebe la transferencia de zona de los servidores de nombre maestro a esclavo.
- Pruebe cada servidor de nombres después de que un sistema se haya colgado o haya rearrancado.

- Envíe peticiones de resolución de nombres a servidores de reenvío antes de que vayan a los servidores de nombres exteriores. Esto permite que los servidores de nombres compartan memoria caché y mejoren el rendimiento reduciendo la carga en los servidores de nombres maestros.

```
objectclass container
    requires
        objectclass,
        cn
objectclass hosts
    requires
        objectclass,
        hname
    allows
        addr
        halias,
        comment
```

### Resolución de servidor de nombres

En una red jerárquica, determinados sistemas principales se designan como *servidores de nombres*. Estos sistemas principales resuelven los nombres en direcciones IP para otros sistemas principales.

El daemon **named** controla la función de servidor de nombres y, por consiguiente, se debe ejecutar en un sistema principal de servidor de nombres.

Antes de configurar un servidor de nombres, decida qué tipo o tipos se ajustan mejor a la red que sirve. Existen varios tipos de servidores de nombres.

Un *servidor de nombres maestro* almacena realmente la base de datos que contiene la información de correlación de nombre a dirección. Carga los datos de un archivo o disco y puede delegar la autorización a otros servidores del dominio. Un *servidor de nombres esclavo* o un *servidor de nombres de apéndice* recibe su información en el arranque del sistema para una zona de autorización determinada desde un servidor de nombres maestro y, a continuación, solicita periódicamente al servidor maestro que actualice la información. Un *servidor de nombres intermedio* responde a las peticiones de resolver nombres consultando otros servidores que tienen autorización para proporcionar la información necesaria.

**Nota:** Las generaciones anteriores del servidor de nombres **named** especificaban el servidor de nombres maestro como el servidor de nombres primario, el servidor de nombres esclavo como el servidor de nombres secundario y el servidor de nombres intermedio como el servidor de nombres de almacenamiento en antememoria sólo.

Tenga presente que un servidor de nombres puede funcionar en diferentes capacidades para diferentes zonas de autorización. Por ejemplo, un sistema principal de servidor de nombres puede ser un servidor de nombres maestro para una zona y un servidor de nombres esclavo para otra zona. Si el sistema tiene instalado NIS, estos servicios también pueden proporcionar resolución de nombres.

Existen varios archivos implicados en la configuración de servidores de nombres.

Item	Descripción
conf	Este archivo se lee cuando se inicia el daemon <b>named</b> . Los registros del archivo conf indican al daemon <b>named</b> qué tipo de servidor es, sobre qué dominios tiene autorización (las zonas de autorización) y dónde debe obtener los datos para configurar inicialmente la base de datos. El nombre predeterminado es este archivo es /etc/named.conf. Sin embargo, puede cambiar el nombre de este archivo especificando el nombre y la vía de acceso del archivo en la línea de mandatos cuando se inicia el daemon <b>named</b> . Si tiene la intención de utilizar /etc/named.conf como el archivo conf y éste no existe, se genera un mensaje en el archivo syslog y <b>named</b> termina. Sin embargo, si se especifica un archivo conf alternativo, y el archivo alternativo no existe, no se genera un mensaje de error, y <b>named</b> continúa.
cache	Contiene información sobre la antememoria local. El archivo de antememoria local contiene los nombres y las direcciones de los servidores de nombres de autorización más alta de la red. El archivo de antememoria utiliza el Formato de registro de recursos estándar. El nombre del archivo de antememoria se establece en el archivo conf.

Item	Descripción
domain data	Existen tres archivos de datos de dominio típicos, también conocidos como los archivos de datos <b>named</b> . El archivo <b>named local</b> contiene la información de resolución de direcciones para el bucle de retorno local. El archivo <b>named de datos</b> contiene los datos de resolución de direcciones para todas las máquinas de la zona de autorización del servidor de nombres. El archivo <b>named de datos inversos</b> contiene la información de resolución de direcciones inversa para todas las máquinas de la zona de autorización del servidor de nombres. Los archivos de datos de dominio utilizan el Formato de registro de recursos estándar. Los nombres de archivo son definibles por el usuario y se establecen en el archivo <b>conf</b> . Por convenio, los nombres de estos archivos incluyen generalmente el nombre del daemon ( <b>named</b> ) y el tipo de archivo y el nombre del dominio se proporcionan en la extensión. Por ejemplo, el servidor de nombres para el dominio abc puede tener los archivos siguientes:

```
named.abc.data
named.abc.rev
named.abc.local
```

Al modificar los archivos de datos **named**, el número de serie del Registro de recursos SOA se debe incrementar para los servidores de nombres esclavos a fin de realizar correctamente los nuevos cambios de zona.

resolv.conf	<p>La presencia de este archivo indica a un sistema principal que vaya a un servidor de nombres para resolver primero un nombre. Si el archivo <b>resolv.conf</b> no existe, el sistema principal busca en el archivo <b>/etc/hosts</b> la resolución de nombres. En un servidor de nombres, el archivo <b>resolv.conf</b> debe existir y puede contener la dirección de sistema principal local, la dirección de bucle de retorno (127.0.0.1) o puede estar vacío.</p> <p><b>Nota:</b> Las rutinas de resolución requieren que se establezca el dominio predeterminado. Si el dominio predeterminado no se establece en el archivo <b>/etc/resolv.conf</b>, se debe establecer en <b>hostname</b></p>
-------------	--

El tiempo de vida (TTL) se especifica en registros de recursos. Si el TTL no se especifica en un registro, la duración de este periodo de tiempo toma de forma predeterminada el campo mínimo definido en el registro de inicio de autorización (SOA) de dicha zona. TTL se utiliza cuando se almacenan datos fuera de una zona (en una antememoria) para asegurar que los datos no se retienen de forma indefinida.

#### **Configuración de servidores de nombres de dominio**

En este caso, se configurarán un servidor de nombres maestro, un servidor de nombres esclavo y un servidor de nombres intermedio para realizar la resolución de nombres. Cada nombre estará en una máquina distinta y cada una de ellas tendrá configurado un archivo **/etc/named.conf**, aunque la información que contiene cada uno de ellos será diferente. El archivo **/etc/named.conf** se lee cada vez que se inicie el daemon **named** y especifica de qué tipo de servidor se trata (maestro, esclavo o intermedio) y dónde obtendrá los datos de resolución de nombres. Cada uno de estos servidores de nombres ejecutará BIND 8.

El servidor de nombres de maestro se configurará para proporcionar la resolución de nombres para la zona **abc.aus.century.com**. En este caso, la dirección IP del servidor de nombres maestro es **192.9.201.1** y el nombre de sistema principal es **venus.abc.aus.century.com**. Proporcionará la resolución de nombres para los nombres de sistema principal **venus**, **earth**, **mars** y **jupiter**. El archivo **/etc/named.conf** se configurará para especificar que el daemon **named** debe buscar en el directorio **/usr/local/domain** los archivos de datos. Los archivos de datos que se configurarán para el servidor de nombres maestro son **named.ca**, **named.abc.local**, **named.abc.data** y **named.abc.rev**.

A continuación, se configurará un servidor de nombres esclavo. El nombre de sistema principal del servidor de nombres esclavo será **earth.abc.aus.century.com** y la dirección IP será **192.9.201.5**.

En el archivo `/etc/named.conf` del servidor de nombres esclavo, especificaremos la dirección del servidor de nombres maestro para que el servidor de nombres esclavo pueda duplicar los archivos `named.abc.data` y `named.abc.rev` del servidor de nombres maestro. Además, se configurarán los archivos de datos `named.ca` y `named.abc.local` para este servidor.

A continuación, se configurará un servidor de nombres intermedio. El servidor de nombres intermedio guardará un almacenamiento intermedio local del nombre de sistema principal y las correlaciones de direcciones. Si una dirección solicitada o un nombre de sistema principal no están en el almacenamiento intermedio, el servidor intermedio contactará con el servidor de nombres maestro, obtendrá la información de resolución y la añadirá al almacenamiento intermedio. Además, se configurarán los archivos de datos `named.ca` y `named.abc.local` para este servidor.

Toda la información contenida en los archivos de datos named (no en el archivo `/etc/named.conf`) en los servidores de nombres debe estar en el Formato de registro de recurso estándar. Si desea obtener explicaciones acerca de la información sobre los archivos de datos named, consulte el apartado Standard Resource Record Format for TCP/IP en la publicación *Referencia de archivos*.

El administrador de cada uno de los servidores de nombre será `gail.zeus.abc.aus.century.com`. Se especifica en los archivos de datos locales de cada uno de los servidores de nombres. Además, en este caso, el servidor de nombres raíz es `relay.century.com` y la dirección IP es `129.114.1.2`.

Al final de este caso, se proporcionará la resolución de nombres para los sistemas principales venus, earth, mars y jupiter. Además, también se proporcionará la resolución de nombres inversa (dirección IP para nombre de sistema principal). Cuando se reciba una solicitud que no se pueda resolver, el servidor de nombres maestro se pondrá en contacto con `relay.century.com` para encontrar la información necesaria.

### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

### Paso 1. Configurar el servidor de nombres maestro

1. En el servidor de nombres maestro, abra el archivo `/etc/named.conf`. Si no hay ningún archivo `/etc/named.conf` en el directorio `/etc` cree uno ejecutando el siguiente mandato:

```
touch /etc/named.conf
```

Realice las acciones siguientes para configurar el archivo `/etc/named.conf`:

- a. Especifique una cláusula de directorio en la stanza de opciones. Esto permitirá que los archivos de datos named utilicen vías de acceso relativas al directorio `/usr/local/domain`. En este caso, se ha añadido lo siguiente:

```
options {  
    directory "/usr/local/domain";  
};
```

Si decide no especificar aquí un directorio, se buscará en el directorio `/etc` los archivos de datos necesarios.

- b. Para que los datos de registro se puedan colocar en el almacenamiento intermedio fuera de las zonas definidas, especifique el nombre del archivo de zona intermedio. En este caso, se ha añadido lo siguiente:

```
zone "." IN {  
    type hint;  
    file "named.ca";  
};
```

- c. Añada las stanzas siguientes para especificar cada zona, el tipo del servidor de nombres que va a configurar y el archivo de datos del dominio del servidor de nombres. En este caso, el servidor maestro para las zonas hacia delante e inversa es el siguiente:

```

zone "abc.aus.century.com" in {
    type master;
    file "named.abc.data";
};

zone "201.9.192.in-addr.arpa" in {
    type master;
    file "named.abc.rev";
};

```

d. Defina el nombre del archivo local named. Por ejemplo:

```

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "named.abc.local";
};

```

Cuando haya editado el archivo, guárdelo y ciérrelo.

2. Abra el archivo /usr/local/domain/named.ca. Añada las direcciones de los servidores de nombres raíz para el dominio. En este caso, se ha añadido lo siguiente:

```

; root name servers.
.           IN      NS      relay.century.com.
relay.century.com.   3600000  IN      A       129.114.1.2

```

Cuando haya editado el archivo, guárdelo y ciérrelo.

3. Abra el archivo /usr/local/domain/named.abc.local. Añada la siguiente información:

- Información sobre el inicio de autorización (SOA) de la zona y sobre el tiempo de vida por omisión. En este caso, se ha añadido lo siguiente:

```

$TTL 3h      ;3 hour

@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
    1          ;serial
    3600       ;refresh
    600        ;retry
    3600000   ;expire
    3600       ;negative caching TTL
)

```

- El registro del servidor de nombres (NS). Inserte un espacio de tabulador al principio de la línea; el daemon **named** sustituirá el espacio de tabulador por el nombre de zona:

```
<tab>    IN      NS      venus.abc.aus.century.com.
```

- El registro del puntero (PTR).

```
1      IN      PTR      localhost.
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

4. Abra el archivo /usr/local/domain/named.abc.data. Añada la siguiente información:

- Información sobre el inicio de autorización de la zona y sobre el tiempo de vida por omisión para la zona. Este registro designa el inicio de una zona. Sólo se permite un inicio de registro de autorizaciones por zona. En este caso, se ha añadido lo siguiente:

```

$TTL 3h      ;3 hour

@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
    1          ;serial
    3600       ;refresh
    600        ;retry
    3600000   ;expire
    3600       ;negative caching TTL
)

```

- El servidor de nombres registra todos los servidores de nombres maestros de la zona. Inserte un espacio de tabulador al principio de la línea; el daemon **named** sustituirá el espacio de tabulador por el nombre de zona:

```
<tab> IN NS venus.abc.aus.century.com.
```

- La información de resolución de nombre con dirección en todos los sistemas principales de la zona de autorización del servidor de nombres:

```
venus IN A 192.9.201.1
earth IN A 192.9.201.5
mars IN A 192.9.201.3
jupiter IN A 192.9.201.7
```

Incluya otros tipos de entrada, como, por ejemplo, registros de nombres canónicos y registros del intercambiador de correo cuando sea necesario.

Cuando haya editado el archivo, guárdelo y ciérrelo.

#### 5. Abra el archivo /usr/local/domain/named.abc.rev. Añada la siguiente información:

- Información sobre el inicio de autorización de la zona y sobre el tiempo de vida por omisión. Este registro designa el inicio de una zona. Sólo se permite un registro de autorizaciones por zona:

```
$TTL 3h ;3 hour
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
    1 ;serial
    3600 ;refresh
    600 ;retry
    3600000 ;expire
    3600 ;negative caching TTL
)
```

- Otros tipos de entradas, como, por ejemplo, registros de servidores de nombres. Si va a incluir estos registros, inserte un espacio de tabulador al principio de la línea; el daemon **named** sustituirá el espacio de tabulador por el nombre de zona. En este caso, se ha añadido lo siguiente:

```
<tab> IN NS venus.abc.aus.century.com.
```

- La información de resolución de dirección con nombre en todos los sistemas principales para que estén en la zona de autorización del servidor de nombres.

```
1 IN PTR venus.abc.aus.century.com.
5 IN PTR earth.abc.aus.century.com.
3 IN PTR mars.abc.aus.century.com.
7 IN PTR jupiter.abc.aus.century.com.
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

#### 6. Cree un archivo /etc/resolv.conf ejecutando el mandato siguiente:

```
touch /etc/resolv.conf
```

La presencia de este archivo indica que el sistema principal debe utilizar un servidor de nombres para la resolución de nombres.

#### 7. Añada la siguiente entrada en el archivo /etc/resolv.conf:

```
nameserver 127.0.0.1
```

La dirección 127.0.0.1 es la dirección de bucle de retorno, que hace que el sistema principal acceda a sí mismo como el servidor de nombres. El archivo /etc/resolv.conf también puede contener una entrada similar a la siguiente:

```
domain abc.aus.century.com
```

En este caso, abc.aus.century.com es el nombre de dominio.

Cuando haya editado el archivo, guárdelo y ciérrelo.

8. Utilice la vía de acceso rápida de la SMIT: smit stnamed para habilitar el daemon **named**. El daemon se inicializará con cada arranque del sistema. Indique si desea iniciar el daemon **named** ahora, durante el siguiente reinicio del sistema o en ambos casos.

## Paso 2. Configurar el servidor de nombres esclavo

Para configurar un servidor de nombres esclavo, utilice el siguiente procedimiento. Editará una serie de archivos y a continuación, utilizará la SMIT para iniciar el daemon **named**.

1. En el servidor de nombres esclavo, abra el archivo /etc/named.conf. Si no hay ningún archivo /etc/named.conf en el directorio /etc, cree uno ejecutando el siguiente mandato:

```
touch /etc/named.conf
```

Realice las acciones siguientes para configurar el archivo /etc/named.conf:

- a. Especifique una cláusula de directorio en la stanza de opciones. Esto permitirá que los archivos de datos named utilicen vías de acceso relativas al directorio /usr/local/domain. En este caso, se ha añadido lo siguiente:

```
options {  
    directory "/usr/local/domain";  
};
```

Si decide no especificar aquí un directorio, el daemon **named** buscará en el directorio /etc los archivos de datos necesarios.

- b. Para que los datos de registro se puedan colocan en el almacenamiento intermedio fuera de las zonas definidas, especifique el nombre del archivo de zona intermedio para el servidor de nombres:

```
zone "." IN {  
    type hint;  
    file "named.ca";  
};
```

- c. Especifique las cláusulas de la zona esclava. Cada stanza incluye el tipo de zona, un nombre de archivo con el cual el servidor de nombres puede realizar una copia de seguridad de los datos y la dirección IP del servidor de nombres maestro del cual el servidor de nombres esclavo duplicará los archivos de datos. En este caso, hemos añadido las siguientes cláusulas de zona esclava:

```
zone "abc.aus.century.com" IN {  
    type slave;  
    file "named.abc.data.bak";  
    masters { 192.9.201.1; };  
};  
  
zone "201.9.192.in-addr.arpa" IN {  
    type slave;  
    file "named.abc.rev.bak";  
    masters { 192.9.201.1; };  
};
```

- d. Para dar soporte a la dirección de red de bucle de retorno, especifique una zona de tipo *maestro* con un origen de named.abc.local, así como el dominio del cual el servidor de nombres es responsable.

```
zone "0.0.127.in-addr.arpa" in {  
    type master;  
    file "named.abc.local";  
};
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

2. Edite el archivo /usr/local/domain/named.ca.

Este archivo contiene el servidor de direcciones que es el servidor de dominio raíz de la red. En este caso, se ha añadido lo siguiente:

```
; root name servers.  
.           IN      NS      relay.century.com.  
relay.century.com. 3600000  IN      A      129.114.1.2
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

3. Abra el archivo /usr/local/domain/named.abc.local. En este caso, se ha añadido lo siguiente:

- Información sobre el inicio de autorización (SOA) de la zona y sobre el tiempo de vida por omisión:

```
$TTL 3h      ;3 hour  
  
@ IN SOA earth.abc.aus.century.com. gail.zeus.abc.aus.century.com. (  
    1          ;serial  
    3600       ;refresh  
    600        ;retry  
    3600000   ;expire  
    3600       ;negative caching TTL  
)
```

- El registro del servidor de nombres (NS). Inserte un espacio de tabulador al principio de la línea; el daemon **named** sustituirá el espacio de tabulador por el nombre de zona. Por ejemplo:

```
<tab>    IN      NS      earth.abc.aus.century.com.
```

- El registro del puntero (PTR).

```
1      IN      PTR      localhost.
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

4. Cree un archivo /etc/resolv.conf ejecutando el mandato siguiente:

```
touch /etc/resolv.conf
```

5. Añada la siguiente entrada a ese archivo:

```
nameserver 127.0.0.1domain abc.aus.century.com
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

6. Utilice la vía de acceso rápida de la SMIT: smit stnamed para habilitar el daemon **named**. El daemon se inicializará con cada arranque del sistema. Indique si desea iniciar el daemon **named** ahora, durante el siguiente reinicio del sistema o en ambos casos.

### Paso 3. Configurar el servidor de nombres intermedio

Para configurar un servidor de nombres intermedio o sólo de *almacenamiento intermedio*, utilice el siguiente procedimiento, que edita una serie de archivos y a continuación utiliza SMIT o la línea de mandatos para iniciar el daemon **named**.

1. En el servidor de nombres intermedio, edite el archivo /etc/named.conf. Si no hay ningún archivo /etc/named.conf en el directorio /etc cree uno ejecutando el siguiente mandato:

```
touch /etc/named.conf
```

Realice las acciones siguientes para configurar el archivo /etc/named.conf:

- a. Especifique una cláusula de directorio en la ztanza de opciones. Esto permitirá que los archivos de datos named utilicen vías de acceso relativas al directorio /usr/local/domain. En este caso, se ha añadido lo siguiente:

```
options {
    directory "/usr/local/domain";
};
```

- b. Para dar soporte a la dirección de red de bucle de retorno, especifique una zona de tipo *maestro* con un origen de named.abc.local, así como el dominio del cual el servidor de nombres es responsable. En este ejemplo, se ha especificado la palabra clave del directorio de opciones en el archivo /etc/named.conf.

```
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.abc.local";
};
```

- c. Especifique el nombre del archivo de zona de almacenamiento intermedio. Por ejemplo:

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

## 2. Edite el archivo /usr/local/domain/named.ca.

Este archivo contiene las direcciones de los servidores que son servidores de nombres con autorización sobre el dominio root de la red. Por ejemplo:

```
; root name servers.
.           IN      NS      relay.century.com.
relay.century.com.   3600000  IN      A      129.114.1.2
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

## 3. Edite el archivo /usr/local/domain/named.local. En este caso, se ha añadido la siguiente información a este archivo:

- Información sobre el inicio de autorización (SOA) de la zona y sobre el tiempo de vida por omisión:

```
$TTL 3h      ;3 hour
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
    1          ;serial
    3600       ;refresh
    600        ;retry
    36000000  ;expire
    3600       ;negative caching TTL
)
```

- El registro del servidor de nombres (NS). Inserte un espacio de tabulador al principio de la línea; el daemon **named** sustituirá el espacio de tabulador por el nombre de zona:

```
<tab>   IN      NS      venus.abc.aus.century.com.
```

- El registro del puntero (PTR).

```
1      IN      PTR      localhost.
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

## 4. Cree un archivo /etc/resolv.conf ejecutando el mandato siguiente:

```
touch /etc/resolv.conf
```

## 5. Añada la siguiente entrada a ese archivo:

```
nameserver 127.0.0.1domain abc.aus.century.com
```

Cuando haya editado el archivo, guárdelo y ciérrelo.

6. Utilice la vía de acceso rápida de la SMIT: smit stnamed para habilitar el daemon **named**. El daemon se inicializará con cada arranque del sistema. Indique si desea iniciar el daemon **named** ahora, durante el siguiente reinicio del sistema o en ambos casos.

Cuando vuelva a arrancar el sistema, se habrá realizado la configuración de IPv6. Repita este proceso para cada sistema principal.

### **Configuración de un servidor de correo de dominio**

La configuración de un servidor de correo de dominio proporciona a los usuarios externos a su organización un método sencillo para dirigir correo a sus usuarios. Es decir, sin un servidor de correo de dominio, la dirección de correo debe especificar un sistema principal determinado de su organización.

Por ejemplo, sam@orange.widget.com, donde widget.com es el nombre de dominio de su organización y orange es el sistema principal que sam utiliza. Sin embargo, con un servidor de correo de dominio, los usuarios externos a su organización puede especificar simplemente el nombre de usuario y el nombre de dominio, sin necesidad de conocer el sistema principal que los usuarios utilizan como, por ejemplo, sam@widget.com.

Para configurar un servidor de correo de dominio, utilice procedimiento siguiente:

1. Cree un registro del intercambiador de correo (MX) y un registro de dirección (A) para el servidor de correo black.widget.com:

```
widget.com      IN    MX      10 black.widget.com
widget.com      IN    A       192.10.143.9
black.widget.com IN    A       192.10.143.9
```

2. Edite sendmail.cf en el servidor de correo (black.widget.com) para añadir el alias de dominio (la clase **w**):

```
Cw $w $?D$w.$D$. widget.com
```

3. Los clientes de correo deben saber dónde enviar el correo que no sea local, así que edite sendmail.cf en cada cliente para que apunte al servidor de correo (la macro **S**):

```
DRblack.widget.com
```

4. Utilice la opción **NameServOpt** para configurar el daemon **sendmail** para que todo el mundo pueda utilizar los registros MX definidos en el servidor de nombres brown.widget.com.
5. Añada alias para los usuarios del dominio que no tengan cuentas en el servidor de correo utilizando el archivo de alias como, por ejemplo:

```
sam:sam@orange.widget.com
david:david@green.widget.com
judy:judy@red.widget.com
```

**Nota:** Los registros de buzón de correo (MB) pueden servir para la misma función.

6. El número de serie del registro de recursos SOA debe aumentarse, porque la base de datos se ha modificado.
7. Renueve la base de datos del servidor de nombres emitiendo el mandato refresh -s named.
8. En los clientes, ejecute el mandato refresh -s sendmail para que los cambios entren en vigor.

Existen otros métodos para configurar un servidor de correo de dominio. Estos procedimientos implican la utilización de registros de buzón de correo (MB), renombrado de correo (MR) y grupo de correo (MG).

### *Configuración de un servidor de correo de dominio utilizando registros de buzón de correo*

Siga el procedimiento siguiente para configurar un servidor de correo de dominio utilizando registros de buzón de correo.

1. Defina un registro de buzón de correo (MB) para cada usuario del dominio. Añada entradas como, por ejemplo:

```
sam IN MB orange.widget.com.
```

al archivo /usr/local/domain/named.abc.data del sistema principal brown.widget.com. Estas entradas identifican el servidor de correo black.widget.com al que enviar el correo para todos los usuarios del dominio.

2. Configure el daemon **sendmail** en el servidor de correo black.widget.com para que utilice los registros MB definidos en el servidor de nombres brown.widget.com.  
Utilice la opción **NameServOpt**.
3. Aumente el número de serie del registro de recursos de SOA, porque la base de datos se ha modificado.
4. Renueve la base de datos del servidor de nombres ejecutando el mandato **refresh -s named**.
5. Escriba el mandato **refresh -s sendmail** para que los cambios entren en vigor.

*Definición de un registro de redenominación de correo para un usuario*

Utilice el procedimiento siguiente para definir un registro de redenominación de correo.

1. Edite el archivo /usr/local/domain/named.abc.data en el servidor de nombres de dominio.
2. Añada un registro de redenominación de correo (MR) para cada alias.

Por ejemplo, si un usuario sam tiene un alias sammy, el Registro de redenominación será el siguiente:

```
sammy IN MR sam
```

Este registro hace que todo el correo dirigido a sammy se entregue a sam. Cada registro MR debe entrarse en una línea solo.

3. El número de serie del registro de recursos de SOA debe aumentarse, porque la base de datos se ha modificado.
4. Renueve la base de datos del servidor de nombres escribiendo el mandato **refresh -s named**.
5. Escriba el mandato **refresh -s sendmail** para que los cambios entren en vigor.

*Definición de los registros de los miembros del grupo de correo*

Utilice el procedimiento siguiente para definir los registros de los miembros del grupo de correo.

1. Edite el archivo /usr/local/domain/named.abc.data en el servidor de nombres de dominio.
2. Añada registros MG para cada grupo de correo (MG). Los registros MG funcionan como el archivo /etc/aliases, manteniendo los alias en el servidor de nombres. Por ejemplo:

```
users IN HINFO users-request widget.com
users IN MG sam
users IN MG david
users IN MG judy
```

Este ejemplo hace que todo el correo dirigido a users@widget.com se entregue a sam, david, y judy. Escriba cada registro MG en una línea independiente.

**Nota:** Los usuarios sam, david y judy deben tener definidos registros MB.

3. El número de serie del registro de recursos de SOA debe aumentarse, porque la base de datos se ha modificado.
4. Renueve la base de datos del servidor de nombres escribiendo el mandato **refresh -s named**.
5. Escriba el mandato **refresh -s sendmail** para que los cambios entren en vigor.

*Definición de los registros del intercambiador de correo*

Siga el procedimiento siguiente para definir los registros del intercambiador de correo.

1. Edite el archivo /usr/local/domain/named.abc.data en el servidor de nombres de dominio.

2. Añada los registros del intercambiador de correo (MX) para cada máquina a la que desee reenviar correo que no esté conectada directamente a la red.

Por ejemplo, si el correo dirigido a los usuarios de purple.widget.com debe reenviarse a post.office.widget, el registro MX tendrá un aspecto similar al siguiente:

```
purple.widget.com IN MX 0 post.office.widget.
```

Debe especificar tanto el nombre del sistema principal como el de la máquina cuando utilice registros MX. Escriba cada registro MG en una línea independiente. Puede utilizar comodines como, por ejemplo:

```
*.widget.com IN MX 0 post.office.widget.
```

Este ejemplo hace que el correo dirigido a un sistema principal desconocido(un sistema principal sin un registro MX explícito) del dominio widget.com se reenvíe a post.office.widget.

**Nota:** Los registros MX con comodines no son adecuados para su utilización en Internet.

3. El número de serie del registro de recursos SOA debe aumentarse, porque la base de datos se ha modificado.
4. Renueve la base de datos del servidor de nombres escribiendo el mandato `refresh -s named`.
5. Escriba el mandato `refresh -s sendmail` para que los cambios entren en vigor.

### Configuración de un reenviador

Para configurar un servidor de reenviadores, utilice el procedimiento siguiente, que edita una serie de archivos y, a continuación, utiliza SMIT o la línea de mandatos para iniciar el **denominado** daemon.

1. Edite el archivo `/etc/named.conf`.

Si no hay ningún archivo `named.conf` en el directorio `/etc`, copie el archivo de ejemplo `/usr/samples/tcpip/named.conf` en el directorio `/etc` y edítelo. Consulte el apartado "[named.conf File Format for TCP/IP](#)" de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado del archivo `conf`.

- Especifique una línea de reenviadores en la stanza de opciones del archivo `/etc/named.conf` que muestra las direcciones IP de los servidores de nombres que deben recibir las peticiones reenviadas. Por ejemplo:

```
options {  
    ...  
    directory "/usr/local/domain";  
    forwarders { 192.100.61.1; 129.35.128.222; };  
    ...  
};
```

- Especifique la zona de bucle de retorno. Por ejemplo:

```
zone "0.0.127.in-addr.arpa" in {  
    type master;  
    file "named.abc.local";  
};
```

- Especifique la zona intermedia. Por ejemplo:

```
zone "." IN {  
    type hint;  
    file "named.ca";  
};
```

2. Edite el archivo `/usr/local/domain/named.ca`. Consulte el apartado "[DOMAIN Cache File Format for TCP/IP](#)" de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado del archivo de antememoria.

Este archivo contiene las direcciones de los servidores que son servidores de nombres con autorización sobre el dominio root de la red. Por ejemplo:

```
; root name servers.  
.           IN      NS      relay.century.com.  
relay.century.com.    3600000   IN      A      129.114.1.2
```

**Nota:** Todas las líneas de este archivo deben estar en formato de registro de recursos estándar.

3. Edite el archivo /usr/local/domain/named.abc.local.

Consulte el apartado DOMAIN Local Data File Format for TCP/IP de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado del archivo de datos local.

- Especifique el inicio de autoridad (SOA) de la zona y la información de tiempo de vida por omisión. Por ejemplo:

```
$TTL 3h      ;3 hour  
  
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (  
    1          ;serial  
    3600       ;refresh  
    600        ;retry  
    3600000   ;expire  
    86400      ;negative caching TTL  
)
```

- Especifique el registro del servidor de nombres (NS). Por ejemplo:

```
<tab>    IN      NS      venus.abc.aus.century.com.
```

- Especifique el registro del puntero (PTR).

```
1      IN      PTR      localhost.
```

**Nota:** Todas las líneas de este archivo deben estar en formato de registro de recursos estándar.

4. Cree un archivo /etc/resolv.conf escribiendo el mandato siguiente:

```
touch /etc/resolv.conf
```

La presencia de este archivo indica que el sistema principal debe utilizar un servidor de nombres en lugar del archivo /etc/hosts para la resolución de nombres.

De modo alternativo, el archivo /etc/resolv.conf podría contener la entrada siguiente:

```
nameserver 127.0.0.1
```

La dirección 127.0.0.1 es la dirección de bucle de retorno, que hace que el sistema principal acceda a sí mismo como el servidor de nombres. El archivo /etc/resolv.conf también puede contener una entrada similar a la siguiente:

```
domain nombre_dominio
```

En el ejemplo anterior, el valor *nombre\_dominio* es austin.century.com.

5. Realice uno de los pasos siguientes:

- Habilite el daemon **named** utilizando la vía rápida de SMIT smit stnamed. El daemon se inicializará con cada arranque del sistema. Indique si desea iniciar el daemon **named** ahora, durante el siguiente reinicio del sistema o en ambos casos.
- Edite el archivo /etc/rc.tcpip. Descomente la línea del daemon **named** eliminando el símbolo de comentario (#) de la línea siguiente:

```
#start /etc/named "$src_running"
```

El daemon se inicializará con cada arranque del sistema.

6. Si opta por no inicializar el daemon named utilizando SMIT, inicie el daemon para esta sesión escribiendo el mandato siguiente:

```
startsrv -s named
```

## Configuración de un servidor de nombres de sólo reenvío

Para configurar un servidor de nombres de sólo reenvío, utilice el procedimiento siguiente, que edita una serie de archivos y, a continuación, utiliza SMIT o la línea de mandatos para iniciar el **denominado** daemon.

**Nota:** Puede conseguirse una configuración similar sin ejecutar un servidor de nombres de sólo reenvío. En lugar de ello, cree un archivo /etc/resolv.conf que contenga las líneas del servidor de nombres que hagan referencia a los reenviadores que deseé utilizar.

### 1. Edite el archivo /etc/named.conf.

Si no hay ningún archivo named.conf en el directorio /etc, copie el archivo de ejemplo /usr/samples/tcpip/named.conf en el directorio /etc y edítelo. Consulte el apartado named.conf File Format for TCP/IP de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado de un archivo conf.

- Especifique los reenviadores y reenvíe sólo las líneas de la stanza de opciones del archivo /etc/named.conf que muestren las direcciones IP de los servidores de nombres que reciban peticiones reenviadas. Por ejemplo:

```
options {  
    ...  
    directory "/usr/local/domain";  
    forwarders { 192.168.61.1; 129.35.128.222; };  
    forward only;  
    ...  
};
```

- Especifique la zona de bucle de retorno. Por ejemplo:

```
zone "0.0.127.in-addr.arpa" in {  
    type master;  
    file "named.abc.local";  
};
```

- Especifique la zona intermedia. Por ejemplo:

```
zone "." IN {  
    type hint;  
    file "named.ca";  
};
```

### 2. Edite el archivo /usr/local/domain/named.ca. Por ejemplo:

Consulte el apartado DOMAIN Cache File Format for TCP/IP de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado del archivo de antememoria. Este archivo contiene las direcciones de los servidores que son servidores de nombres con autorización sobre el dominio root de la red.

```
; root name servers.  
.           IN      NS      relay.century.com.  
relay.century.com. 3600000  IN      A      129.114.1.2
```

**Nota:** Todas las líneas de este archivo deben estar en formato de registro de recursos estándar.

### 3. Edite el archivo /usr/local/domain/named.abc.local. Consulte el apartado DOMAIN Local Data File Format for TCP/IP de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado del archivo de datos local.

- a) Especifique el inicio de autoridad (SOA) de la zona y la información de tiempo de vida por omisión. Por ejemplo:

```
$TTL 3h      ;3 hour  
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
```

```
        1      ;serial
        3600   ;refresh
        600    ;retry
        3600000 ;expire
        86400   ;negative caching TTL
    )
```

- b) Especifique el registro del servidor de nombres (NS). Por ejemplo:

```
<tab>  IN  NS  venus.abc.aus.century.com.
```

- c) Especifique el registro del puntero (PTR).

```
1  IN  PTR  localhost.
```

**Nota:** Todas las líneas de este archivo deben estar en formato de registro de recursos estándar.

4. Cree un archivo /etc/resolv.conf escribiendo el mandato siguiente:

```
touch /etc/resolv.conf
```

La presencia de este archivo indica que el sistema principal debe utilizar un servidor de nombres en lugar del archivo /etc/hosts para la resolución de nombres.

De modo alternativo, el archivo /etc/resolv.conf podría contener la entrada siguiente:

```
nameserver 127.0.0.1
```

La dirección 127.0.0.1 es la dirección de bucle de retorno, que hace que el sistema principal acceda a sí mismo como el servidor de nombres. El archivo /etc/resolv.conf también puede contener una entrada similar a la siguiente:

```
domain nombre_dominio
```

En el ejemplo anterior, el valor *nombre\_dominio* es austin.century.com.

5. Realice uno de los pasos siguientes:

- Habilite el daemon **named** utilizando la vía rápida de SMIT smit stnamed. El daemon se inicializará con cada arranque del sistema. Indique si desea iniciar el daemon **named** ahora, durante el siguiente reinicio del sistema o en ambos casos.
- Edite el archivo /etc/rc.tcpip. Descomente la línea del daemon **named** eliminando el símbolo de comentario (#) de la línea siguiente:

```
#start /etc/named "$src_running"
```

El daemon se inicializará con cada arranque del sistema.

6. Si opta por no inicializar el daemon **named** utilizando SMIT, inicie el daemon para esta sesión escribiendo el mandato siguiente:

```
starts src -s named
```

### Configuración de un sistema principal para que utilice un servidor de nombres

Para configurar un sistema principal para que utilice un servidor de nombres, utilice este procedimiento.

1. Cree un archivo /etc/resolv.conf ejecutando el mandato siguiente:

```
touch /etc/resolv.conf
```

2. En la primera línea del archivo /etc/resolv.conf, escriba la palabra domain seguida del nombre completo del dominio en el que se encuentra este sistema principal. Por ejemplo:

```
domain abc.aus.century.com
```

3. En cualquier línea en blanco por debajo de la línea domain, escriba la palabra nameserver, seguida por lo menos de un espacio, seguido de la dirección Internet decimal con puntos del servidor de nombres que deba utilizar este sistema principal (el servidor de nombres debe prestar servicio al dominio indicado en la sentencia domain).

Puede haber hasta 3 entradas de servidores de nombres. Por ejemplo, el archivo /etc/resolv.conf podría incluir las entradas siguientes:

```
nameserver 192.9.201.1
nameserver 192.9.201.2
```

El sistema consulta los servidores de nombres en el orden en que aparecen.

```
search domainname_list
```

De forma alternativa, es posible utilizar la palabra clave search para especificar el orden en el que la resolución consultará la lista de dominios. En este caso, los valores de domainname\_list son abc.aus.century.com y aus.century.com. La lista de nombres de dominio domainname\_list puede tener un máximo de 1024 series de caracteres, separadas entre sí mediante un espacio.

4. Suponiendo que el servidor de nombres esté operativo, es posible probar la comunicación entre el sistema principal y el servidor de nombres escribiendo el mandato siguiente:

```
host nombre_sistema_principal
```

Utilice el nombre de un sistema principal que el servidor de nombres deba resolver para ver si funciona el proceso. La salida que reciba debería ser similar a la siguiente:

```
brown.abc.aus.century.com is 129.35.145.95
```

En la tabla siguiente se muestran otras tareas de configuración.

Tabla 63. Configuración de un sistema principal para que utilice las tareas del servidor de nombres		
Tarea	Vía rápida de SMIT	Mandato o archivo
Creación de un archivo /etc/resolv.conf	smit stnamerslv2	create y edit /etc/resolv.conf <sup>1</sup>
Listado de todos los servidores de nombres que un sistema principal utiliza	smit lsnamerslv	view /etc/resolv.conf
Adición de un servidor de nombres	smit mknamerslv	edit /etc/resolv.conf <sup>2</sup>
Eliminación de un servidor de nombres	smit rmnamerslv	edit /etc/resolv.conf
Inicio/Reinicio utilizando la resolución de nombres de dominio	smit stnamerslv	
Detención de la utilización de la resolución de nombres de dominio	smit spnamerslv	
Modificación/Visualización del dominio	smit mkdomain	edit /etc/resolv.conf
Eliminación del dominio	smit rmdomain	edit /etc/resolv.conf

## Información relacionada

archivo netsvc.conf

### Zonas dinámicas del servidor de nombres DNS

El mandato **named** permite actualizaciones dinámicas. Es necesario configurar los archivos de configuración y la base de datos con nombre para que las máquinas cliente puedan emitir actualizaciones. Una zona puede establecerse como dinámica o estática. La zona por omisión es estática.

Para hacer una zona sea dinámica, es necesario añadir la palabra clave `allow-update` en la stanza de dicha zona del archivo `/etc/named.conf`. La palabra clave `allow-update` especifica una lista de coincidencias de una dirección Internet que define los sistemas principales que pueden someter actualizaciones. Consulte el apartado [named.conf File Format for TCP/IP](#) de la publicación *Referencia de archivos* para obtener más información y un ejemplo detallado de un archivo `conf`. En el ejemplo siguiente, todos los sistemas principales pueden actualizar la zona dinámica:

```
zone "abc.aus.century.com" IN {  
    type master;  
    file "named.abc.data";  
    allow-update { any; };  
};
```

Una vez una zona se ha marcado como dinámica, pueden iniciarse tres modalidades de seguridad:

Item	Descripción
<b>No segura</b>	Permite que cualquier usuario pueda actualizar toda la información de la zona en cualquier momento.   <b>Atención:</b> No se recomienda la utilización de esta modalidad. Puede provocar pérdidas de datos, interceptación de datos y frustración de los usuarios. Por lo menos una zona no segura debe estar limitada exclusivamente para actualizaciones de direcciones Internet específicas.
<b>Controlada</b>	Permite la creación de información nueva y la sustitución de información existente. Probablemente se trata de la modalidad más fácil de utilizar para un entorno de transición seguro. Esta modalidad también requiere que todas las actualizaciones de entrada lleven la indicación de fecha y hora y tengan firmas de clave.
<b>Protegida</b>	Requiere que todas las actualizaciones de información existente se sustituyan por información similar. No permite la creación de información nueva. Esta modalidad también requiere que todas las actualizaciones de entrada lleven la indicación de fecha y hora y tengan firmas de clave.

El valor predeterminado de una zona dinámica es la modalidad no segura. Para utilizar una de las otras modalidades, escriba `controlled` (controlada) o `presecured` (protegida= después de la palabra clave `update-security` en la stanza sobre la zona del archivo `/etc/named.conf`). Esto indica al servidor **named** el nivel de seguridad que debe utilizarse con esta zona. Por ejemplo:

```
zone "abc.aus.century.com" IN {  
    type master;  
    file "named.abc.data";  
    allow-update { any; };  
    update-security controlled;  
};
```

Una vez se ha seleccionado una modalidad, es necesario modificar los archivos de datos en sí para el nivel de seguridad. En la modalidad no segura, los archivos de datos se utilizan "tal cual." Para la modalidad controlada o protegida, es necesario generar un conjunto de pares de claves de nombre de sistema principal/servidor maestro para cada nombre de la zona. Esto se realiza con el mandato **nsupdate** utilizando la opción **-g**. Este mandato genera el par de claves (una clave privada y una pública). Estas claves son necesarias para firmar las actualizaciones con autenticidad. Después de generar todas las claves para la lista de nombres de la zona, es necesario añadirlas al archivo de datos. El formato de KEY es el siguiente:

Índice	ttl	Clase	Tipo	DistintivosClave	Protocolo	Algoritmo	DatosClave
--------	-----	-------	------	------------------	-----------	-----------	------------

donde:

Item	Descripción
Índice	Especifica el nombre utilizado para hacer referencia a los datos de la zona.
ttl	Especifica el tiempo de vida (TTL) de estos datos. Se trata de un campo opcional.
Clase	Especifica la clase de los datos. Depende de la zona, pero suele definirse como IN.
Tipo	Indica el tipo del registro. En este caso, es KEY.
DistintivosClave	Proporciona información con nombre sobre la clave. 0x0000 define el registro de clave habitual que se utiliza para un sistema principal. 0x0100 define el registro de clave asociado con el nombre de la zona.
Protocolo	Especifica el protocolo que debe utilizarse. Actualmente, sólo hay uno, 0.
Algoritmo	Especifica el algoritmo de la clave. Actualmente, sólo hay uno, 1. Se trata del método de autentificación privada/pública MD5.
DatosClave	Indica la clave en representación base64. El mandato <b>nsupdate</b> genera tanto la clave pública como la privada en representación base64. La clave pública se lista en el archivo de salida.

Por ejemplo, para garantizar la seguridad a través de un nombre de sistema principal en una zona dinámica, debe añadirse al archivo de la zona una línea similar a la siguiente para la zona que contiene el nombre del sistema principal.

```
bears      4660      IN      KEY      0x0000      0      1      A00tg.....
```

El ejemplo anterior indica que `bears` tiene definido un registro KEY. Si alguien desea actualizar `bears`, debería firmar su actualización con la clave privada que coincida la clave pública en la base de datos. Para que el mandato **nsupdate** sea satisfactorio, la clave privada debe colocarse en el cliente en un archivo de claves (por omisión, en `/etc/keyfile`). Debería seguir el formato siguiente:

```
nombre_sistema_principal    nombre_maestro          clave de base64
```

Se requiere una entrada KEY similar en la sección de definición de zona. *Se requiere una clave de zona tanto para la modalidad protegida como para la controlada. En caso contrario, se considera que la modalidad no es segura.* Esto puede hacerse tal como se muestra en el ejemplo `bears` anterior, pero la clave privada se deja para que el administrador la utilice con la modalidad de administración del mandato **nsupdate**.

1. Para generar un par de claves utilizando el mandato **nsupdate**, escriba lo siguiente:

```
nsupdate -g -h nombre_zona -p nombre_servidor -k archivo:claves_admin
```

Se genera una clave para la zona. En este ejemplo, **nsupdate** se enlaza con **nsupdate4**, lo que puede hacerse escribiendo lo siguiente:

```
ln -fs /usr/sbin/nsupdate4 /usr/sbin/nsupdate
```

2. Coloque la última clave del par en la sección inicial de la zona, de la forma siguiente:

```
IN      KEY      0x0100      0      1      clave
```

La entrada para el archivo `named.abc.data` es la siguiente:

```
$TTL 3h      ;3 hour
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
                           1      ;serial
```

```

        3600    ;refresh
        600    ;retry
        3600000 ;expire
        86400   ;negative caching TTL
)
IN      NS      venus.abc.aus.century.com.
IN      KEY    0x0100  0 1 AQP1wHmI0eZzRk6Q/nQYhs3xwnhfTgF/
               8Y1BVzKSoKxVKPNLInnYW0mB7attTcfhHaZZcZr4u/
               vDNikKnhnZwgn/
venus  IN      A       192.9.201.1
earth   IN      A       192.9.201.5
mars    IN      A       192.9.201.3

```

3. La zona está ahora lista para su carga renovando el servidor de nombres. Coloque el archivo de claves de administración en el cliente o en el servidor DHCP que esté actualizando la zona. Es posible utilizar la clave de zona contenida en el archivo de claves de administración para aplicar actualizaciones y operaciones de mantenimiento en el servidor de nombres.

### Seguridad en BIND 9

BIND 9 ofrece Firmas de transacciones (TSIG) y Firmas (SIG) como medidas de seguridad para **named**.

El servidor de nombres con BIND 9, por omisión, no permite actualizaciones dinámicas en zonas autorizadas, de forma similar a lo que sucede en BIND 8.

BIND 9 proporciona soporte principalmente a las Firmas de transacciones (TSIG) para la comunicación de servidor a servidor. Esto incluye los mensajes de consulta recursiva, notificación y transferencia de zona. TSIG también resulta útil para las actualizaciones dinámicas. Un servidor primario para una zona dinámica debe utilizar control de acceso para controlar las actualizaciones pero el control de acceso basado en IP resulta insuficiente.

Al utilizar el cifrado base de claves en lugar del método actual de listas de control de acceso, TSIG puede utilizarse para restringir quién puede actualizar las zonas dinámicas. A diferencia del método ACL (Lista de control de acceso) de las actualizaciones dinámicas, la clave TSIG puede distribuirse a otros actualizadores sin necesidad de modificar los archivos de configuración en el servidor de nombres, lo que significa que no es necesario que el servidor de nombres vuelva a leer los archivos de configuración.

Resulta importante observar que BIND 9 no tiene todas las palabras clave implementadas en BIND 8. En este ejemplo, utilizamos la configuración maestra simple de BIND 8.

**Nota:** Para utilizar named 9, es necesario volver a enlazar el enlace simbólico con el daemon **named** con **named9** y **nsupdate** con **nsupdate9** ejecutando los mandatos siguientes:

1. ln -fs /usr/sbin/named9 /usr/sbin/named
2. ln -fs /usr/sbin/nsupdate9 /usr/sbin/nsupdate
3. Genere la clave utilizando el mandato **dnssec-keygen**:

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST keyname
```

- HMAC-MD5 es el algoritmo utilizado para el cifrado
- 128 es la longitud de la clave que debe utilizarse (o el número de bits)
- HOST: HOST es la palabra clave de TSIG utilizada para generar una clave de sistema principal para un cifrado de clave compartido.

El mandato

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST venus-batman.abc.aus.century.com
```

generaría dos archivos de claves, como se indica a continuación:

```
Kvenus-batman.abc.aus.century.com.+157+35215.key
Kvenus-batman.abc.aus.century.com.+157+35215.private
```

- 157 es el algoritmo utilizado (HMAC-MD5)
- 35215 es la huella, que resulta útil en DNNSEC porque se permiten varias claves por zona.

2. Añada la entrada a named.conf en el servidor de nombres maestro:

```
// TSIG Key
key venus-batman.abc.aus.century.com. {
    algorithm hmac-md5;
    secret "+UWSvbpHWFdNwEAdy1Ktw==";
};
```

Suponiendo que se utilice HMAC-MD5, ambos archivos de claves contendrán la clave compartida, que se almacena como la última entrada de los archivos. Halle una forma seguridad de copiar la clave secreta compartida en el cliente. No es necesario que copie el archivo de claves, simplemente la clave secreta compartida.

A continuación se muestra la entrada para el archivo Kvenus-batman.abc.aus.century.com.+157+35215.private:

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: +UWSvbpHWFdNwEAdy1Ktw==
```

A continuación se muestra un ejemplo del archivo named.conf para el servidor de nombres maestro. La zona abc.aus.century.com sólo permite la transferencia de zona y las actualizaciones dinámicas a los servidores con la clave venus-batman.abc.aus.century.com. Realice lo mismo con la zona inversa, que requiere que los actualizadores tengan la clave compartida.

```
// TSIG Key
key venus-batman.abc.aus.century.com. {
    algorithm hmac-md5;
    secret "+UWSvbpHWFdNwEAdy1Ktw==";
};

options {
    directory "/usr/local/domain";
};

zone "abc.aus.century.com" in {
    type master;
    file "named.abc.data";
    allow-transfer { key venus-batman.abc.aus.century.com.; };
    allow-update{ key venus-batman.abc.aus.century.com.; };
};
```

Como las transferencias de zonas están ahora restringidas a aquellos que tengan una clave, el archivo del servidor de nombres esclavo named.conf también debe editarse. Todas las peticiones a 192.9.201.1 (venus.abc.aus.century.com) están firmadas mediante una clave. Observe que el nombre de la clave (venus-batman.abc.aus.century.com.) debe coincidir con la de los servidores que la utilizan.

A continuación se muestra un ejemplo del archivo named.conf en el servidor de nombres esclavo:

```
// TSIG Key
key venus-batman.abc.aus.century.com. {
    algorithm hmac-md5;
    secret "+UWSvbpHWFdNwEAdy1Ktw==";
};

server 192.9.201.1{
    keys { venus-batman.abc.aus.century.com.; };
};

options {
    directory "/usr/local/domain";
};

zone "abc.aus.century.com" IN {
    type slave;
    file "named.abc.data.bak";
    masters { 192.9.201.1; };
};
```

## Firmas de transacciones en BIND 9

BIND 9 proporciona soporte principalmente a las Firmas de transacciones (TSIG) para la comunicación de servidor a servidor.

Esto incluye los mensajes de consulta recursiva, notificación y transferencia de zona. TSIG también resulta útil para las actualizaciones dinámicas. Un servidor primario para una zona dinámica debe utilizar control de acceso para controlar las actualizaciones pero el control de acceso basado en IP resulta insuficiente.

Al utilizar el cifrado base de claves en lugar del método actual de listas de control de acceso, TSIG puede utilizarse para restringir quién puede actualizar las zonas dinámicas. A diferencia del método ACL (Lista de control de acceso) de las actualizaciones dinámicas, la clave TSIG puede distribuirse a otros actualizadores sin necesidad de modificar los archivos de configuración en el servidor de nombres, lo que significa que no es necesario que el servidor de nombres vuelva a leer los archivos de configuración.

Resulta importante observar que BIND 9 no tiene todas las palabras clave implementadas en BIND 8. En este ejemplo, utilizamos la configuración maestra simple de BIND 8.

**Nota:** Para utilizar named 9, es necesario volver a enlazar el enlace simbólico con el daemon **named** con **named9** y **nsupdate** con **nsupdate9** ejecutando los mandatos siguientes:

1. ln -fs /usr/sbin/named9 /usr/sbin/named
2. ln -fs /usr/sbin/nsupdate9 /usr/sbin/nsupdate
3. Genere la clave utilizando el mandato **dnssec-keygen**:

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST keyname
```

- HMAC-MD5 es el algoritmo utilizado para el cifrado
- 128 es la longitud de la clave que debe utilizarse (o el número de bits)
- HOST: HOST es la palabra clave de TSIG utilizada para generar una clave de sistema principal para un cifrado de clave compartido.

El mandato

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST venus-batman.abc.aus.century.com
```

generaría dos archivos de claves, como se indica a continuación:

```
Kvenus-batman.abc.aus.century.com.+157+35215.key  
Kvenus-batman.abc.aus.century.com.+157+35215.private
```

- 157 es el algoritmo utilizado (HMAC-MD5)
- 35215 es la huella, que resulta útil en DNNSEC porque se permiten varias claves por zona.

2. Añada la entrada a named.conf en el servidor de nombres maestro:

```
// TSIG Key  
key venus-batman.abc.aus.century.com. {  
    algorithm hmac-md5;  
    secret "+UWSvbpXHWFdNwEAdy1Ktw==";  
};
```

Suponiendo que se utilice HMAC-MD5, ambos archivos de claves contendrán la clave compartida, que se almacena como la última entrada de los archivos. Halle una forma seguridad de copiar la clave secreta compartida en el cliente. No es necesario que copie el archivo de claves, simplemente la clave secreta compartida.

A continuación se muestra la entrada para el archivo Kvenus-batman.abc.aus.century.com.+157+35215.private:

```
Private-key-format: v1.2  
Algorithm: 157 (HMAC_MD5)  
Key: +UWSvbpXHWFdNwEAdy1Ktw==
```

Lo que sigue es un ejemplo del archivo named.conf para el servidor de nombres maestro. La zona abc.aus.century.com sólo permite la transferencia de zona y las actualizaciones dinámicas a los servidores con la clave venus-batman.abc.aus.century.com. Realice lo mismo con la zona inversa, que requiere que los actualizadores tengan la clave compartida.

```
// TSIG Key
key venus-batman.abc.aus.century.com. {
    algorithm hmac-md5;
    secret "+UWSvbxHWFdNwEAdy1Ktw==";
};

options {
    directory "/usr/local/domain";
};
zone "abc.aus.century.com" in {
    type master;
    file "named.abc.data";
    allow-transfer { key venus-batman.abc.aus.century.com.; };
    allow-update{ key venus-batman.abc.aus.century.com.; };
};
```

Como las transferencias de zonas están ahora restringidas a aquellos que tengan una clave, el archivo del servidor de nombres esclavo named.conf también debe editarse. Todas las peticiones a 192.9.201.1 (venus.abc.aus.century.com) están firmadas mediante una clave. Observe que el nombre de la clave(venus-batman.abc.aus.century.com.) debe coincidir con la de los servidores que la utilizan.

A continuación se muestra un ejemplo del archivo named.conf en el servidor de nombres esclavo:

```
// TSIG Key
key venus-batman.abc.aus.century.com. {
    algorithm hmac-md5;
    secret "+UWSvbxHWFdNwEAdy1Ktw==";
};

server 192.9.201.1{
    keys { venus-batman.abc.aus.century.com.; };
};

options {
    directory "/usr/local/domain";
};

zone "abc.aus.century.com" IN {
    type slave;
    file "named.abc.data.bak";
    masters { 192.9.201.1; };
};
```

### Firmas en BIND 9

BIND 9 proporciona soporte parcial a las firmas de transacciones DNSSEC SIG tal como se especifica en RFC 2535.

SIG utiliza claves públicas y privadas para autenticar los mensajes.

Los registros de SIG permiten a los administradores firmar los datos de su zona, afirmando con ello que son auténticos.

#### Seguridad de la zona root

Cuando se utilizan estos pasos para asegurar la zona root, se supone que otros servidores de nombres de Internet no utilizan BIND 9 y que desea asegurar los datos de la zona y permitir que otros servidores verifiquen los datos de la zona.

Desea indicar que la zona (en nuestro caso aus.century.com) es una zona root segura y validará los datos de cualquier zona segura por debajo de la misma.

#### 1. Genere las claves utilizando el mandato dnssec-keygen:

```
dnssec-keygen -a RSA -b 512 -r /usr/sbin/named -n ZONE aus.century.com.
```

**Nota:** Si OpenSSL está instalado, es posible el cifrado RSA como el algoritmo para generar la clave, aunque primero debe volver a enlazar la biblioteca DNS con una biblioteca DNS segura ejecutando el mandato siguiente:

```
ln -fs /usr/lib/libdns_secure.a /usr/lib/libdns.a
```

- ZONE: ZONE es la palabra clave de DNSSEC utilizada para generar claves de zona para el cifrado de claves privadas/públicas.
- El distintivo `r` especifica un dispositivo aleatorio.

## 2. Añada la entrada de clave pública similar al archivo named.conf.

La entrada utilizada en nuestro caso se muestra a continuación. Más abajo aparece el contenido del archivo de claves Kaus.century.com.+001+03254.key.

```
abc.aus.century.com. IN KEY 256 3 1
AQ0nfGEAg0xpzSdNRe7KePq3Dl4NqQiq7HkwK16TygUfaw6vz6ldmauB4UQFcGK0yL68/
Zv5ZnEvyB1fMTAaDLYz
```

La clave pública está incluida en el archivo Kzonename.+algor.+fingerprint.key o, en nuestro caso, Kaus.century.com.+001+03254.key. Debe eliminar la clase IN y el tipo KEY, así como escribir la clave entre comillas. Una vez añada esta entrada al archivo /etc/named.conf y renueve el servidor de nombres, la zona aus.century.com será una zona root segura.

```
trusted-keys {
    aus.century.com. 256 3 1 "AQ0nfGEAg0xpzSdNRe7KePq3Dl4NqQiq7HkwK16Tyg
    Ufaw6vz6ldmauB4UQFcGK0yL68/Zv5ZnEvyB1fMTAaDLYz";
};
options {
    directory "/usr/local/domain";
};

zone "abc.aus.century.com" in {
    type master;
    file "named.abc.data.signed";
    allow-update{192.9.201.1;};
};
```

### Aplicación de la cadena de confianza

Una vez conseguida una raíz segura, es posible asegurar esto de las zonas hijo. En este caso, estamos trabajando para asegurar la zona abc.aus.century.com.

Siga estos pasos para asegurar el resto de las zonas hijo:

#### 1. Genere pares de claves utilizando el mandato dnssec-keygen:

```
dnssec-keygen -a RSA -b 512 -r /usr/sbin/named -n ZONE abc.aus.century.com.
```

El distintivo `r` especifica un archivo de entrada aleatorio.

#### 2. Genere un conjunto de claves ejecutando el mandato dnssec-makekeyset:

```
dnssec-makekeyset -t 172800 Kabc.aus.century.com.+001+11515.key
```

donde Kabc.aus.century.com.+001+11515.key es su propia clave pública.

Se crea un archivo de conjunto de claves denominado keyset-abc.aus.century.com.

#### 3. Envíe este archivo de conjunto de claves a la zona padre para su firma. En este caso, nuestra zona padre es la zona root segura aus.century.com.

#### 4. El padre debe firmar la clave utilizando la clave privada.

```
dnssec-signkey keyset-abc.aus.century.com. Kaus.century.com.+001+03254.private
```

Se generará un archivo denominado signedkey-abc.aus.century.com y el padre deberá enviar este archivo de vuelta a la zona hijo.

5. En un servidor de nombres hijo para la zona abc.aus.century.com, añada \$INCLUDE Kabc.aus.century.com.+001+11515.key al archivo de zona plano named.abc.data. Recuerde colocar el archivo signedkey-abc.aus.century.com en la misma ubicación que el archivo de zona named.abc.data. Cuando se firme la zona en el paso siguiente, el programa sabrá incluir signedkey-abc.aus.century.com, que se habrá recibido del padre.

```
$TTL 3h      ;3 hour
@ IN SOA venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
    1           ;serial
    3600        ;refresh
    600         ;retry
    3600000    ;expire
    86400       ;negative caching TTL
)
$INCLUDE Kabc.aus.century.com.+001+03254.key
```

6. Firme la zona utilizando el mandato **dnssec-signzone**:

```
dnssec-signzone -o abc.aus.century.com. named.abc.data
```

7. Modifique el archivo **named.conf** de la zona hijo abc.aus.century.com para que utilice el archivo de zona que acaba de firmarse (named.abc.data.signed). Por ejemplo:

```
options {
    directory "/usr/local/domain";
};

zone "abc.aus.century.com" in {
    type master;
    file "named.abc.data.signed";
    allow-update{192.9.201.1;};
};
```

8. Renueve el servidor de nombres.

Para obtener información sobre la resolución de problemas, consulte el apartado “[Problemas de resolución de nombres](#)” en la página 498.

## Planificación y configuración para la resolución de nombres de LDAP (esquema de IBM SecureWay Directory)

**LDAP (Lightweight Directory Access Protocol)** es un estándar abierto de la industria que define un método para acceder y actualizar información en un directorio.

Un esquema **LDAP** define las normas para ordenar datos. La clase de objeto **ibm-HostTable**, parte del esquema de IBM SecureWay Directory, se puede utilizar para almacenar la información de correlación de nombre con dirección de Internet para cada sistema principal de la red.

La clase de objeto **ibm-HostTable** se define del modo siguiente:

Nombre de clase de objeto:	ibm-HostTable
Descripción:	Entrada de tabla del sistema principal que tiene una colección de correlaciones de direcciones IP.
OID:	TBD
RDN:	ipAddress
Clase objeto superior:	top
Atributos necesarios:	host, ipAddress
Atributos opcionales:	ibm-hostAlias, ipAddressType, description

A continuación se proporcionan las definiciones de atributo:

Nombre de atributo:	ipAddress
Descripción:	Dirección IP del nombre de sistema principal de la tabla de sistema principal
OID:	TBD
Sintaxis:	caseIgnoreString
Longitud:	256
Un solo valor:	Yes
Nombre de atributo:	ibm-hostAlias
Descripción:	Alias del nombre de sistema principal de la tabla de sistema principal

```

OID: TBD
Sintaxis: caseIgnoreString
Longitud: 256
Un solo valor: Multi-valued
Nombre de atributo: ipAddressType
Descripción: Familia de direcciones de la dirección IP (1=IPv4, 2=IPv6)
OID: TBD
Sintaxis: Integer
Longitud: 11
Un solo valor: Yes
Nombre de atributo: host
Descripción: Nombre de sistema principal de un sistema informático.
OID: 1.13.18.0.2.4.486
Sintaxis: caseIgnoreString
Longitud: 256
Un solo valor: Multi-valued
Nombre de atributo: description
Descripción: Comentarios que proporcionan una descripción de una
entrada de objeto de directorio.
OID: 2.5.4.13
Sintaxis: caseIgnoreString
Longitud: 1024
Un solo valor: Multi-valued

```

Utilice el procedimiento siguiente para configurar el servidor **LDAP** que cumpla con los estándares del esquema de IBM SecureWay Directory, con el fin de almacenar la información de sistema principal de correlación de nombre con dirección de Internet.

1. Añada un sufijo al servidor **LDAP**.

El sufijo es el punto de partida de la base de datos de sistemas principales. Por ejemplo "cn=hosts". Esto se puede realizar utilizando la herramienta de administración IBM SecureWay Directory Server basada en la web.

2. Cree un archivo LDIF (LDAP Data Interchange Format - Formato de intercambio de datos LDAP).

Esto se puede realizar manualmente o con el mandato **hosts2ldif**, que crea un archivo LDIF desde el directorio /etc/hosts. Consulte el [Mandato hosts2ldif](#) para obtener más información. A continuación, se muestra un archivo LDIF de ejemplo:

```

dn: cn=hosts
objectclass: top
objectclass: container
cn: hosts
dn: ipAddress=1.1.1.1, cn=hosts
host: test
ipAddress: 1.1.1.1
objectclass: ibm-HostTable
ipAddressType: 1
ibm-hostAlias: e-test
ibm-hostAlias: test.austin.ibm.com
description: primera interfaz ethernet
dn: ipAddress=fe80::dead, cn=hosts
host: test
ipAddress: fe80::dead
objectclass: ibm-HostTable
ipAddressType: 2
ibm-hostAlias: test-ll
ibm-hostAlias: test-ll.austin.ibm.com
description: interfaz de nivel de enlace de v6

```

3. Importe los datos del directorio hosts del archivo LDIF en el servidor **LDAP**.

Esto se puede realizar con el mandato **ldif2db** o mediante la herramienta de administración IBM SecureWay Directory Server basada en la web.

Si desea configurar el cliente para que acceda a la base de datos de sistemas principales del servidor LDAP, utilizando el mecanismo de **LDAP**, siga estos pasos:

1. Cree el archivo /etc/resolv.ldap. Consulte el [Formato de archivo resolv.ldap para TCP/IP](#) en la publicación *Referencia de archivos* si desea más información y un ejemplo detallado de un archivo resolv.ldap.
2. Cambie la resolución de nombres predeterminada mediante la variable de entorno NSORDER, el archivo /etc/netsvc.conf o el archivo /etc/irs.conf. Consulte el [Formato de archivo](#)

netsvc.conf para TCP/IP o el Formato de archivo irs.conf para TCP/IP en la publicación *Referencia de archivos* para obtener más información.

Aunque aún se soporta, la utilización del mecanismo `ldap` está en desuso. Este mecanismo existente `ldap` funciona con IBM SecureWay Directory Schema, mientras que `nis_ldap` (NIS\_LDAP) funciona con el esquema RFC 2307. Se recomienda utilizar el mecanismo `nis_ldap` en lugar del mecanismo `ldap`. Para obtener información sobre la resolución de nombres `nis_ldap`, consulte el apartado “[Planificación y configuración de la resolución de nombres NIS\\_LDAP \(esquema RFC 2307\)](#)” en la página 217.

## Planificación y configuración de la resolución de nombres NIS\_LDAP (esquema RFC 2307)

AIX 5.2 ofrece un nuevo mecanismo de denominación llamado NIS\_LDAP.

La diferencia entre el mecanismo LDAP existente y el nuevo mecanismo NIS\_LDAP está en el esquema de LDAP (el conjunto de atributos y clases de objeto que determinan cómo se agrupan los atributos para describir una entidad). El mecanismo LDAP existente funciona con el servidor LDAP que se ajusta a los estándares del esquema de IBM SecureWay Directory y sólo soporta el servicio de nombres de sistema principal. El mecanismo NIS\_LDAP funciona con el servidor LDAP que se ajusta a los estándares del esquema RFC 2307 y soporta todos los servicios: usuarios y grupos, sistemas principales, servicios, protocolos, redes y grupo de redes. RFC 2307 define un conjunto de atributos y clases de objetos que se pueden utilizar para describir servicios de información de red, incluidos usuarios y grupos.

- Para configurar el servidor LDAP, necesitará definir el servidor LDAP y migrar los datos necesarios al servidor.
  - a) Utilice el mandato **`mksecldap`** para configurar un servidor.

El mecanismo `nis_ldap` sólo funciona con el esquema RFC 2307. Al configurar el servidor LDAP, se deberá invocar el mandato **`mksecldap`** con la opción `-S rfc2307` o `-S rfc2307aix` (pero no la opción `-S aix`, que especifica el esquema de IBM SecureWay Directory). De forma predeterminada, el mandato **`mksecldap`** migra los usuarios y los grupos definidos en el sistema local al servidor LDAP. Si desea inhabilitar esta migración, utilice la opción `-u NONE`.

```
mksecldap -s -a cn=admin -p adminpwd -S rfc2307aix
```

Esto configura un servidor LDAP, en el que el DN de administrador es `cn=admin` y la contraseña es `adminpwd`. El sufijo predeterminado, `cn=aixdata`, también se añade al archivo `/etc/slapd32.conf`, el archivo de configuración de servidor LDAP.

De forma predeterminada, el mandato **`mksecldap`** migra los usuarios y los grupos definidos en el sistema local al servidor LDAP. Si desea inhabilitar esta migración, utilice la opción `-u NONE`, que impide la migración de usuarios y grupos locales al servidor LDAP, para que sólo pueda añadir usuarios y grupos NIS posteriormente.

```
mksecldap -s -a cn=admin -p adminpwd -u NONE
```

- b) Migré los datos NIS. Utilice el mandato **`nistoldif`** desde el servidor NIS para migrar las correlaciones NIS al servidor LDAP. El mandato **`nistoldif`** también se puede utilizar para migrar datos de archivos planos.

Ejecute el mandato **`nistoldif`** en un sistema que contenga los datos NIS que es necesario migrar al servidor LDAP.

```
nistoldif -h server1.ibm.com -a cn=admin -p adminpwd -d cn=aixdata
```

Esto migra las correlaciones NIS del sistema local al servidor LDAP, `server1.ibm.com`. Los datos NIS se ponen bajo el DN `cn=aixdata`. También puede ejecutar el mandato **`nistoldif`** para migrar datos de archivos planos de cualquier sistema al servidor LDAP. Los archivos planos se utilizarán para las correlaciones que falten en el servidor NIS.

**Nota:** Los nombres se representan mediante el atributo `cn` del servidor LDAP. El atributo `cn` definido por RFC 2307 no es sensible a las mayúsculas y minúsculas. Los nombres que sólo difieren por las mayúsculas y minúsculas se fusionarán en el servidor. Las coincidencias tampoco

son sensibles a las mayúsculas y minúsculas. Las búsquedas de TCP, tcp o Tcp devolverán todas las entradas de protocolo para TCP.

- Para configurar que el cliente LDAP acceda a nombres del servidor LDAP, ejecute el mandato **mksecldap** con las opciones de configuración de cliente.
  - a) El mandato **mksecldap** guarda el nombre, el puerto, el DNadmin, la contraseña y el DNbase del servidor LDAP en el archivo `/etc/security/ldap/ldap.cfg`, que el daemon **secldapclntd** lee en el arranque. El mandato **mksecldap** inicia el daemon **secldapclntd** automáticamente, si la configuración es satisfactoria.

Consulte el archivo `/etc/security/ldap/ldap.cfg` en *Files Reference* y el daemon **secldapclntd** en *Commands Reference, Volume 5* para obtener más información.
  - b) El mandato **mksecldap** añade el mecanismo `nis_ldap` al archivo `/etc/netsvc.conf` y al archivo `/etc/irs.conf` para que la resolución de nombres se pueda dirigir a LDAP. También puede establecer manualmente la variable de entorno `NSORDER` en `nis_ldap` para utilizar la resolución de nombres NIS\_LDAP.

```
mksecldap -c -a cn=admin -p adminpwd -h server1.ibm.com
```

Esto configura el sistema local para que utilice el servidor LDAP `server1.ibm.com`. Se deben proporcionar el DN y la contraseña de administrador de servidor LDAP para que este cliente se autentique en el servidor. Los archivos `/etc/netsvc.conf` y `/etc/irs.conf` se actualizan de forma que la resolución de nombres se resuelve mediante NIS\_LDAP.

Para obtener más información, consulte el formato de archivo `/etc/netsvc.conf` para TCP/IP o el formato de archivo `/etc/irs.conf` para TCP/IP en la publicación *Referencia de archivos*.

- c) La resolución de nombres para usuarios y grupos no la controlan los archivos `/etc/netsvc.conf` o `/etc/irs.conf`. En su lugar, se realiza mediante el archivo `/etc/security/user`. Para permitir que un usuario LDAP inicie la sesión en un sistema AIX, establezca las variables `SYSTEM` y `registry` del usuario en LDAP en el archivo `/etc/security/user` de ese sistema cliente.

Para ello, puede ejecutar el mandato **chuser**.

```
chuser -R LDAP SYSTEM=LDAP registry=LDAP foo
```

Puede configurar el sistema para permitir que todos los usuarios LDAP inicien la sesión en un sistema. Para ello, edite el archivo `/etc/security/user`. Añada `registry = files` a la stanza de root. A continuación, añada `SYSTEM = LDAP` y `registry = LDAP` a la stanza predeterminada.

Para obtener más información sobre la autenticación de usuario, consulte [Light Directory Access Protocol](#) en la publicación *Security*.

## Información relacionada

[Migración de NIS a servicios LDAP conforme a RFC 2307](#)

## Asignación de direcciones y parámetros TCP/IP - Protocolo de configuración dinámica de sistemas principales

**TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet)** permite las comunicaciones entre máquinas con direcciones configuradas. Parte del peso con el que se debe enfrentar un administrador de red es la asignación de direcciones y la distribución de parámetros para todas las máquinas de la red. Normalmente, se trata de un proceso en el que el administrador de red impone la configuración a cada usuario, permitiendo al usuario configurar su propia máquina. Sin embargo, las configuraciones incorrectas o los malentendidos pueden generar llamadas de servicio que el administrador debe tratar individualmente. El **DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de sistemas principales)** proporciona al administrador de red un método para eliminar el usuario final de este problema de configuración y mantener la configuración de red en una ubicación centralizada.

**DHCP** es un protocolo de capa de aplicación que permite a un máquina cliente de la red obtener una dirección IP y otros parámetros de configuración del servidor. Obtiene la información intercambiando

paquetes entre un daemon en el cliente y otro en el servidor. Ahora la mayoría de los sistemas operativos proporcionan un cliente **DHCP** en el paquete base.

Para obtener una dirección, el daemon de cliente **DHCP** (**dhcpcd**) difunde un mensaje de descubrimiento **DHCP** que el servidor recibe y procesa. (Se pueden configurar varios servidores en la red para redundancia). Si hay una dirección libre disponible para dicho cliente, se crea un mensaje de oferta **DHCP**. Este mensaje contiene una dirección IP y otras opciones que son apropiadas para dicho cliente. El cliente recibe la oferta **DHCP** del servidor y la almacena mientras espera otras ofertas. Cuando el cliente elige la mejor oferta, difunde una petición **DHCP** que especifica qué oferta de servidor desea.

Todos los servidores **DHCP** configurados reciben la petición. Cada uno comprueba si es el servidor solicitado. Si no lo es, el servidor libera la dirección asignada a dicho cliente. El servidor solicitado marca la dirección como asignada y devuelve un reconocimiento **DHCP**, momento en el cual termina la transacción. El cliente tiene una dirección durante el periodo de tiempo (alquiler) designado por el servidor.

Cuando ha transcurrido la mitad de este tiempo de alquiler, el cliente envía al servidor un paquete de *renovación* para ampliar el tiempo de alquiler. Si el servidor desea renovarlo, envía un reconocimiento **DHCP**. Si el cliente no obtiene una respuesta del servidor que es propietario de la dirección actual, difunde un paquete de revinculación **DHCP** para alcanzar el servidor, si, por ejemplo, el servidor se ha movido de una red a otra. Si el cliente no ha renovado la dirección después del tiempo de alquiler completo, la interfaz se desactiva y el proceso vuelve a empezar. Este ciclo evita que se asigne la misma dirección a varios clientes de una red.

El servidor **DHCP** asigna direcciones basándose en claves. Cuatro claves comunes son network (red), class (clase), vendor (proveedor) y client ID (ID de cliente). El servidor utiliza estas claves para obtener una dirección y un conjunto de opciones de configuración a devolver al cliente.

#### **red**

Identifica de qué segmento de red procede el paquete. La clave de red permite al servidor comprobar la base de datos de direcciones y asignar una dirección por segmento de red.

#### **class**

Es totalmente configurable por el cliente. Puede especificar una dirección y opciones. Esta clave se puede utilizar para indicar la función de máquina en la red o para describir cómo se agrupan las máquinas para fines administrativos. Por ejemplo, es posible que el administrador de red desee crear una clase netbios que contenga opciones para clientes NetBIOS o una clase contabilidad que represente las máquinas del departamento de contabilidad que necesitan acceso a una impresora específica.

#### **vendor**

Ayuda a identificar el cliente por la plataforma de software/hardware (por ejemplo un cliente Microsoft Windows 95 o un cliente OS/2 Warp).

#### **client ID**

Identifica el cliente a través del nombre de sistema principal de máquina o de la dirección de capa de control de accesos al medio (MAC). El ID de cliente se especifica en el archivo de configuración del daemon **dhcpcd**. Asimismo, el servidor puede utilizar el ID de cliente para pasar opciones a un cliente específico o prohibir a un cliente determinado recibir cualquier parámetro.

La configuración puede utilizar estas claves de forma individual o en combinaciones. Si el cliente proporciona varias claves y se pueden asignar varias direcciones, sólo se elige una y el conjunto de opciones se deriva de la clave elegida en primer lugar. Para obtener información más detallada sobre la selección de claves y direcciones, consulte el apartado “Configuración de DHCP” en la página 222.

Se necesita un agente de relé para que las difusiones iniciales del cliente puedan salir de la red local. Este agente se denomina agente de relé BOOTP. Los agentes de relé actúan como agentes de reenvío para paquetes **DHCP** y **BOOTP**.

### **Servidores DHCP**

En el sistema operativo AIX, el servidor **DHCP** se ha segmentado en tres partes principales.

Los componentes principales del servidor **DHCP** son una base de datos, un motor de protocolo y un conjunto de hebras de servicio, cada uno con su propia información de configuración.

### **Base de datos DHCP**

La base de datos db\_file.dhcpo se utiliza para hacer el seguimiento de clientes y direcciones y para el control de acceso (por ejemplo, permitir a determinados clientes en algunas redes pero no otras o inhabilitar los clientes **BOOTP** en una red determinada).

Las opciones también se almacenan en la base de datos para recuperarlas y entregarlas a los clientes. La base de datos se implementa como un objeto cargable dinámicamente, que permite la actualización y el mantenimiento fáciles del servidor.

Si se utiliza la información en el archivo de configuración, la base de datos se prepara y se verifica la coherencia. Un conjunto de archivos de punto de comprobación maneja las actualizaciones en la base de datos y reduce la sobrecarga de las grabaciones en el archivo de almacenamiento principal. La base de datos también contiene las agrupaciones de direcciones y opciones, pero éstas son estáticas y se describen en “Configuración de DHCP” en la página 222.

El archivo de almacenamiento principal y la copia de seguridad son archivos ASCII planos que se pueden editar. El formato de los archivos de almacenamiento principal de base de datos es:

```
DF01
"ID CLIENTE" "0.0.0.0" Estado InicioTiempoAlquiler DuraciónTiempoAlquiler FinTiempoAlquiler
  "Dirección IP servidor" "ID clase" "ID proveedor" "Nombre sistpral" "Nombre dominio"
"ID CLIENTE" "0.0.0.0" Estado InicioTiempoAlquiler DuraciónTiempoAlquiler FinTiempoAlquiler
  "Dirección IP servidor" "ID clase" "ID proveedor" "Nombre sistpral" "Nombre dominio"
...
...
```

La primera línea es un identificador de versión para el archivo: DF01c. Las líneas siguientes son líneas de definición de registro de cliente. El servidor lee desde la segunda línea hasta el final del archivo. (Los parámetros entre comillas deben estar entre comillas.)

#### **"ID CLIENTE"**

ID que el cliente utiliza para representarse a sí mismo en el servidor.

#### **"0.0.0.0"**

es la dirección IP asignada actualmente al servidor **DHCP**. Si no se ha asignado ninguna dirección, es "0.0.0.0".

#### **Estado**

Estado actual del cliente. El motor de protocolo **DHCP** contiene el conjunto permitido y los estados se mantienen en la base de datos **DHCP**. El número junto a *Estado* representa el valor. Los estados pueden ser:

##### **(1) FREE**

Representa direcciones que están disponibles para utilizarse. En general, los clientes no tienen este estado a menos que no tengan asignada ninguna dirección. **dadmin** y la salida de **lssrc** informan de este estado como Free.

##### **(2) BOUND**

Indica que el cliente y la dirección están unidos y que se ha asignado al cliente esta dirección durante algún tiempo. **dadmin** y la salida de **lssrc** informan de este estado como Leased.

##### **(3) EXPIRED**

Indica que el cliente y la dirección están unidos, pero sólo a título informativo, de un modo similar a direcciones liberadas. Sin embargo, el estado caducado representa a clientes que dejan que caduquen los alquileres. Una dirección caducada está disponible para utilizarse y se reasigna después de que todas las direcciones libres dejen de estar disponibles y antes de que se reasignen las direcciones liberadas. **dadmin** y la salida de **lssrc** informan de este estado como Expired.

##### **(4) RELEASED**

Indica que el cliente y la dirección están unidos sólo a título informativo. El protocolo **DHCP** sugiere que los servidores **DHCP** mantengan información sobre los clientes que han servido para futuras referencias (principalmente para intentar proporcionar la misma dirección a ese cliente al que se ha asignado esa dirección en el pasado). Este estado indica que el cliente ha liberado la dirección. La dirección está libre para que la utilicen otros clientes, si no hay otras direcciones disponibles. **dadmin** y la salida de **lssrc** informan de este estado como Released.

## (5) RESERVED

Indica que el cliente y la dirección están unidos, pero de forma flexible. El cliente ha emitido un mensaje de descubrimiento **DHCP** y el servidor **DHCP** ha respondido, pero el cliente aún no ha respondido con una petición **DHCP** de dicha dirección. **dadmin** y la salida de **lssrc** informan de este estado como Reserved.

## (6) BAD

Representa una dirección que está en uso en la red pero que el servidor **DHCP** no ha distribuido. Este estado también representa direcciones que los clientes han rechazado. Este estado no se aplica a los clientes. **dadmin** y la salida de **lssrc** informan de este estado como Used y Bad, respectivamente.

### *LeaseTimeStart*

Es el inicio del tiempo de alquiler actual (en el número de segundos desde el 1 de enero de 1970).

### *LeaseTimeDuration*

Representa la duración del alquiler (en segundos).

### *LeaseTimeEnd*

Utiliza el mismo formato que *LeaseTimeStart*, pero representa el final del alquiler. Algunas opciones de configuración utilizan valores diferentes para el inicio y el final de un alquiler y estos valores se pueden alterar temporalmente mediante opciones de archivo de configuración. Consulte el apartado “[Sintaxis de archivo de servidor DHCP para la base de datos db\\_file](#)” en la página 246.

### **“Dirección IP servidor”**

Es la dirección IP del servidor DHCP que es propietario de este registro.

### **“ID clase” “ID proveedor” “Nombre sistpral” “Nombre dominio”**

Valores que el servidor utiliza para determinar qué opciones se envían al servidor (almacenadas como series entrecomillada). Estos parámetros aumentan el rendimiento porque se pueden generar previamente listas de opciones para estos clientes cuando arranca el servidor **DHCP**.

### *Archivos de punto de comprobación de DHCP*

La sintaxis para los archivos de punto de comprobación no se especifica.

Si el servidor se cuelga o si tiene que cerrar el sistema y no puede realizar un cierre normal de la base de datos, el servidor puede procesar los archivos de punto de comprobación y de copia de seguridad para reconstruir una base de datos válida. El cliente que se está grabando en el archivo de punto de comprobación cuando el servidor se cuelga se pierde. Los valores predeterminados son:

#### **/etc/db\_file.cr**

operación de base de datos normal

#### **/etc/db\_file.crbk**

copias de seguridad para la base de datos

#### **/etc/db\_file.chkpt y /etc/db\_file.chkpt2**

archivos de punto de comprobación de rotación

El servidor **DHCP** tiene hebras. Para mantener un rendimiento alto, las operaciones de base de datos (incluidas las operaciones de guardar) son eficientes con las hebras. Cuando se solicita una operación de guardar, el archivo de punto de comprobación existente rota al siguiente archivo de punto de comprobación, el archivo de base de datos existente se copia en el archivo de copia de seguridad y se crea el nuevo archivo de guardar. Entonces se anota cada registro de cliente y se commuta un bit para indicar que el cliente debe utilizar el nuevo archivo de punto de comprobación para el registro. Cuando se registran todos los registros de cliente, el archivo de guardar se cierra y los archivos de punto de comprobación antiguos y de copia de seguridad se suprimen. Los clientes aún se pueden procesar y, en función de si se ha guardado el registro de cliente o no, los cambios de base de datos entran en un nuevo archivo de guardar o en un nuevo archivo de punto de comprobación.

### **Motor de protocolo DHCP**

El motor de protocolo **DHCP** da soporte a RFC 2131 y aún es compatible con RFC 1541. (El servidor también puede procesar las opciones definidas en RFC 2132). El motor de protocolo utiliza la base de datos para determinar qué información se devuelve al cliente.

La configuración de las agrupaciones de direcciones tiene algunas opciones de configuración que afectan al estado de cada máquina. Por ejemplo, el servidor **DHCP** ejecuta ping en las direcciones antes de distribuirlos. Ahora la cantidad de tiempo que el servidor espera una respuesta es configurable para cada agrupación de direcciones.

### Operaciones con hebra DHCP

La última parte del servidor **DHCP** es en realidad un conjunto de operaciones que se utilizan para mantener todos los elementos en ejecución. Dado que el servidor **DHCP** tiene hebras, estas operaciones se configuran realmente como hebras que en ocasiones realizan acciones para asegurarse de que todo está correcto.

La primera hebra, la hebra main, maneja las peticiones SRC (por ejemplo startsrc, stopsrc, lssrc, traceson y refresh). Esta hebra también coordina todas las operaciones que afectan a todas las hebras y maneja las señales. Por ejemplo,

- A SIGHUP (-1) produce una renovación de todas las bases de datos en el archivo de configuración.
- A SIGTERM (-15) hará que el servidor se detenga de forma ordenada.

La siguiente hebra, la hebra dadmin, intercambia información con el programa cliente dadmin y el servidor **DHCP**. Se puede utilizar la herramienta dadmin para obtener el estado así como para modificar la base de datos a fin de editar los archivos de base de datos manualmente. Las versiones anteriores del servidor **DHCP** impedían que los clientes obtuvieran direcciones si se estaba ejecutando una petición de estado. Con la adición de las hebras dadmin y src, el servidor puede manejar peticiones de servicio y seguir manejando peticiones de cliente.

La siguiente hebra es la hebra garbage, que ejecuta temporizadores que limpian periódicamente la base de datos, guardan la base de datos, depuran los clientes que no tienen direcciones y eliminan direcciones reservadas que han estado en estado de reserva durante demasiado tiempo. Todos estos temporizadores son configurables (consulte “Configuración de DHCP” en la página 222). Las demás hebras son procesadores de paquetes. El número de éstos es configurable; el valor predeterminado es 10. Cada uno de ellos puede manejar una petición de un cliente **DHCP**. El número de procesadores de paquetes necesarios depende de la carga y de la máquina. Si la máquina se utiliza para servicios distintos de **DHCP**, no es sensato arrancar 500 hebras.

### Planificación de DHCP

Para utilizar este protocolo, el administrador de red necesita configurar un servidor **DHCP** y configurar agentes de relé BOOTP en enlaces que no tienen un servidor **DHCP**. La planificación avanzada puede reducir la carga de **DHCP** en la red.

Por ejemplo, se puede configurar un servidor para manejar todos los clientes, pero todos los paquetes deben pasar por él. Si tiene un direccionador individual entre dos redes grandes, es más sensato poner dos servidores en la red, uno en cada enlace.

Otro aspecto a tener en cuenta es que **DHCP** implica un patrón de tráfico. Por ejemplo, si establece el tiempo de alquiler predeterminado en menos de dos días y las máquinas se desenchufan durante el fin de semana, el lunes por la mañana se convierte en un periodo de tráfico **DHCP** alto. Aunque el tráfico **DHCP** no produce una enorme sobrecarga para la red, es necesario tenerlo en cuenta cuando se decide dónde poner los servidores **DHCP** en una red y cuántos hay que utilizar.

Después de habilitar **DHCP** para obtener el cliente en la red, un cliente no tiene requisitos para entrar cualquier elemento. El cliente **DHCP**, dhcpcd, lee el archivo dhcpcd.ini, que contiene información sobre el registro cronológico y otros parámetros necesarios para empezar a ejecutar. Después de la instalación, decida qué método utilizar para la configuración de **TCP/IP**: configuración mínima o **DHCP**. Si se selecciona **DHCP**, elija una interfaz y especifique algunos parámetros opcionales. Para elegir la interfaz, seleccione la palabra clave any, que indica a dhcpcd que busque la primera interfaz que funcione y la utilice. Este método minimiza la cantidad de entrada en el lado del cliente.

### Configuración de DHCP

De forma predeterminada, el servidor **DHCP** se configura leyendo el archivo /etc/dhcpsd.cnf, que especifica la base de datos inicial de opciones y direcciones.

El servidor se inicia en el archivo `/etc/rc.tcpip`. También se puede iniciar desde SMIT o mediante mandatos de SRC. El cliente **DHCP** puede configurarse ejecutando la herramienta System Management Interface Tool (SMIT) o editando un archivo ASCII plano.

La configuración del servidor **DHCP** es generalmente la parte más difícil de la utilización de **DHCP** en la red. En primer lugar, decida en qué redes desea tener los clientes **DHCP**. Cada subred de la red representa una agrupación de direcciones que el servidor **DHCP** debe añadir a la base de datos. Por ejemplo:

```
database db_file
{
    subnet 9.3.149.0 255.255.255.0
        { option 3 9.3.149.1 # La pasarela predeterminada que los clientes de
          # esta red deben utilizar
          option 6 9.3.149.2 # El servidor de nombres que los clientes de esta
          # red deben utilizar
        }
    ...
}
```

El ejemplo anterior muestra una subred, 9.3.149.0, con una máscara de subred 255.255.255.0. Todas las direcciones de esta subred, 9.3.149.1 a 9.3.149.254, están en la agrupación. Opcionalmente, se puede especificar un rango al final de la línea o se puede incluir una sentencia de exclusión o rango en el contenedor de subred. Consulte el apartado “[Opciones conocidas del archivo de servidor DHCP](#)” en la página 231 para conocer las definiciones y los métodos de configuración comunes.

La cláusula de base de datos con `db_file` indica qué método de base de datos se debe utilizar para procesar esta parte del archivo de configuración. Los comentarios empiezan con un # (signo de almohadilla). El servidor **DHCP** ignora el texto desde la # inicial hasta el final de la línea. El servidor utiliza cada línea `option` para indicar al cliente qué debe hacer. “[Opciones conocidas del archivo de servidor DHCP](#)” en la página 231 describe las opciones conocidas y soportadas actualmente. Consulte el apartado “[Sintaxis de archivo de servidor DHCP para la operación de servidor general](#)” en la página 237 si desea conocer procedimientos para especificar opciones que el servidor no conoce.

Si el servidor no sabe cómo analizar una opción, utiliza los métodos predeterminados para enviar la opción al cliente. Esto también permite al servidor **DHCP** enviar opciones específicas de sitio que no están definidas por RFC, pero que determinados clientes o configuraciones de cliente pueden utilizar.

### **Archivo de configuración DHCP**

El archivo de configuración tiene una sección de dirección y una sección de definición de opciones. Estas secciones utilizan contenedores para incluir opciones, modificadores y, potencialmente, otros contenedores.

Un *contenedor* (básicamente, un método para agrupar opciones) utiliza un identificador para clasificar los clientes en grupos. Los tipos de contenedor son subred, clase, proveedor y cliente. Actualmente, no hay ningún contenedor genérico que pueda definir el usuario. El identificador define de forma exclusiva el cliente para que se pueda realizar el seguimiento del cliente si, por ejemplo, se mueve entre subredes. Se puede utilizar más de un tipo de contenedor para definir el acceso de cliente.

Las *opciones* son identificadores que se devuelven al cliente, por ejemplo dirección de DNS y pasarela predeterminada.

Los *modificadores* son sentencias individuales que modifican algún aspecto de un contenedor, por ejemplo el valor predeterminado de tiempo de alquiler.

### *Contenedores DHCP*

Cuando el servidor **DHCP** recibe una petición, el paquete se analiza y las claves de identificación determinan qué contenedores, opciones y direcciones se extraen.

El ejemplo del apartado “[Configuración de DHCP](#)” en la página 222 muestra un contenedor de subred. La clave de identificación es la posición del cliente en la red. Si el cliente es de esa red, se clasifica en ese contenedor.

Cada tipo de contenedor utiliza una opción diferente para identificar un cliente:

- El contenedor de subred utiliza el campo **giaddr** o la dirección de la interfaz de recepción para determinar de qué subred procede el cliente.
- El contenedor de clase utiliza el valor de la opción 77 (Identificador de clase de sitio de usuario).
- El proveedor utiliza el valor de la opción 60 (Identificador de clase de proveedor).
- El contenedor de cliente utiliza la opción 61 (Identificador de cliente) para clientes **DHCP** y el campo **chaddr** en el paquete **BOOTP** para los clientes **BOOTP**.

Excepto para las subredes, cada contenedor permite la especificación del valor que coincide con él, incluida la coincidencia de expresiones regulares.

También existe un contenedor implícito, el contenedor *global*. Las opciones y los modificadores se colocan en el contenedor global a menos que se alteren temporalmente o se rechacen. La mayoría de los contenedores se pueden poner dentro de otros contenedores lo que implica un ámbito de visibilidad. Los contenedores pueden tener o no tener asociados a ellos rangos de direcciones. Las subredes, por naturaleza, tienen rangos asociados a ellas.

Las normas básicas para los contenedores y subcontenedores son:

- Todos los contenedores son válidos a nivel global.
- No se pueden poner subredes dentro de otros contenedores.
- Los contenedores restringidos no pueden contener contenedores regulares del mismo tipo. (Por ejemplo, un contenedor con una opción que sólo permite una clase de Contabilidad no puede incluir un contenedor con una opción que permite todas las clases que empiezan con la letra "a". Esto no está permitido.)
- Los contenedores de cliente restringidos no pueden tener subcontenedores.

Según las normas anteriores, puede generar una jerarquía de contenedores que segmente las opciones en grupos para clientes o conjuntos de clientes específicos.

Si un cliente coincide con varios contenedores, ¿cómo se manejan las opciones y las direcciones? El servidor **DHCP** recibe mensajes, pasa la petición a la base de datos (archivo\_bd en este caso) y se genera una lista de contenedores. La lista se presenta en orden de profundidad y prioridad. La prioridad se define como una jerarquía implícita en los contenedores. Los contenedores estrictos tienen una prioridad más alta que los contenedores normales. Los clientes, las clases, los proveedores y finalmente las subredes se clasifican, en ese orden, y dentro del tipo de contenedor por profundidad. Esto genera una lista ordenada del más específico al menos específico. Por ejemplo:

```
Subnet 1
--Class 1
--Client 1
Subnet 2
--Class 1
---Vendor 1
----Client 1
--Client 1
```

El ejemplo muestra dos subredes, Subnet 1 y Subnet 2. Hay un nombre de clase, Class 1, un nombre de proveedor, Vendor 1 y un nombre de cliente, Client 1. Class 1 y Client 1 se definen en varios lugares. Dado que están en contenedores diferentes, los nombres pueden ser iguales pero los valores que contienen pueden ser diferentes. Si Client 1 envía un mensaje al servidor **DHCP** de Subnet 1 especificando Class 1 en la lista de opciones, el servidor **DHCP** generará la siguiente vía de acceso de contenedor:

```
Subnet 1, Class 1, Client 1
```

El contenedor más específico se lista en último lugar. Para obtener una dirección, la lista se examina en jerarquía inversa para encontrar la primera dirección disponible. A continuación, la lista se examina avanzando en la jerarquía para obtener las opciones. Las opciones alteran temporalmente los valores anteriores a menos que exista un rechazo (**deny**) de opción en el contenedor. Asimismo, dado que Class 1 y Client 1 están en Subnet 1, se ordenan de acuerdo con la prioridad de contenedor. Si el mismo cliente está en Subnet 2 y envía el mismo mensaje, la lista de contenedores generada es:

**Subnet 2, Class 1, Client 1** (a nivel de Subnet 2), **Client 1** (a nivel de Class 1)

Subnet 2 se lista en primer lugar, a continuación Class 1, y Client 1 en el nivel Subnet 2 (porque esta sentencia de cliente sólo está un nivel por debajo en la jerarquía). La jerarquía implica que un cliente que coincide con la primera sentencia de cliente es menos específico que el cliente que coincide con Client 1 de Class 1 en Subnet 2.

La prioridad seleccionada por profundidad en la jerarquía no se reemplaza por la prioridad de los propios contenedores. Por ejemplo, si el mismo cliente emite el mismo mensaje y especifica un identificador de proveedor, la lista de contenedores es:

**Subnet 2, Class 1, Vendor 1, Client 1** (a nivel de Subnet 2), **Client 1** (a nivel de Class 1)

La prioridad de contenedor mejora el rendimiento de búsqueda porque sigue un concepto general según el cual los contenedores de cliente son el modo más específico de definir uno o varios clientes. El contenedor de clase contiene direcciones menos específicas que un contenedor de cliente, el contenedor de proveedor es incluso menos específico y el contenedor de subred es el menos específico.

#### *Direcciones y rangos de direcciones de DHCP*

Cualquier tipo de contenedor puede tener rangos de direcciones asociados; las subredes deben tener rangos de direcciones asociados. Cada rango dentro de un contenedor debe ser un subconjunto del rango y no se debe solapar con rangos de otros contenedores.

Por ejemplo, si se define una clase dentro de una subred y la clase tiene un rango, el rango debe ser un subconjunto del rango de subredes. Asimismo, el rango dentro de ese contenedor de clases no se puede solapar con ningún otro rango que esté a su nivel.

Los rangos se pueden expresar en la línea de contenedor y modificar mediante sentencias de exclusión y rango para permitir separar conjuntos de direcciones asociadas con un contenedor. Si tiene disponibles las diez direcciones superiores y las segundas diez direcciones de una subred, la subred puede especificar estas direcciones por rango en la cláusula de subred para reducir el uso de memoria y la posibilidad de colisión de direcciones con otros clientes que no están en los rangos especificados.

Cuando se ha seleccionado una dirección, cualquier contenedor subsiguiente de la lista que contiene rangos de direcciones se elimina de la lista junto con los hijos. Las opciones específicas de red de contenedores eliminados no son válidas si no se utiliza una dirección de ese contenedor.

#### *Opciones de archivo de configuración DHCP*

Después de que se haya seleccionado la lista para determinar las direcciones, se genera un conjunto de operaciones para el cliente.

En este proceso de selección, las opciones se graban encima de las opciones seleccionadas anteriormente a menos que se encuentre un **deny** (rechazo), en cuyo caso la opción rechazada se elimina de la lista que se está enviando al cliente. Este método permite la herencia de los contenedores padre para reducir la cantidad de datos que se deben especificar.

#### *Modificadores DHCP*

Los modificadores son elementos que cambian algún aspecto de un contenedor determinado, por ejemplo el acceso o el tiempo de alquiler.

Defina las agrupaciones de dirección y opción antes de modificar el contenedor. Los modificadores más comunes son **leasetimedefault**, **supportBootp** y **supportUnlistedclients**.

##### **leasetimedefault**

Define la cantidad de tiempo que se va a alquilar una dirección a un cliente.

##### **supportBootp**

Define si el servidor responde a los clientes **BOOTP** o no.

##### **supportUnlistedclients**

Indica si los clientes se deben definir explícitamente mediante una sentencia de cliente para recibir direcciones. El valor para **supportUnlistedClients** puede ser **none**, **dhcp**, **bootp** o **both**. Esto le permite restringir el acceso al cliente bootp y permitir a todos los clientes DHCP obtener direcciones.

Otros modificadores se listan en el apartado “[Sintaxis de archivo de servidor DHCP para la base de datos db\\_file](#)” en la página 246.

#### *Registro cronológico de DHCP*

Después de seleccionar los modificadores, el siguiente elemento que se debe configurar es el registro cronológico.

Los parámetros de registro cronológico se especifican en un contenedor como la base de datos, pero la palabra clave de contenedor es **logging\_info**. Cuando se aprende a configurar **DHCP**, es aconsejable activar el registro cronológico al nivel más alto. También es mejor especificar la configuración de registro cronológico antes de otros datos de archivo de configuración para asegurar que los errores de configuración se registran después de que se haya inicializado el subsistema de registro cronológico. Utilice la palabra clave **logitem** para activar el nivel de registro cronológico o elimine la palabra clave **logitem** para inhabilitar un nivel de registro cronológico. Otras palabras clave del registro cronológico permiten especificar el nombre de archivo de registro cronológico, el tamaño de archivo y el número de archivos de registro cronológico en rotación.

#### *Opciones específicas de servidor DHCP*

El último conjunto de parámetros a especificar son opciones específicas de servidor que permiten al usuario controlar el número de procesadores de paquete, la frecuencia con la que se ejecutan las hebras de recolección de basura, etc.

Por ejemplo, dos opciones específicas de servidor son:

##### **reservedTime**

Indica el periodo de tiempo durante el cual permanece una dirección en estado reservado después de enviar una oferta (OFFER) al cliente **DHCP**

##### **reservedTimeInterval**

Indica la frecuencia con la que el servidor **DHCP** examina las direcciones para ver si hay alguna que haya estado en estado reservado durante un periodo de tiempo más largo que **reservedTime**.

Estas opciones son útiles si tiene varios clientes que difunden mensajes de descubrimiento (DISCOVER) y no difunden el mensaje de petición (REQUEST) o el mensaje REQUEST se pierde en la red. La utilización de estos parámetros evita que las direcciones se reserven indefinidamente para un cliente que no cumple las normas.

Otra opción especialmente útil es **SaveInterval**, que indica con qué frecuencia se produce la operación de guardar. Todas las opciones específicas del servidor se listan en el apartado “[Sintaxis de archivo de servidor DHCP para la operación de servidor general](#)” en la página 237 con las palabras clave de registro cronológico.

#### *Consideraciones acerca del rendimiento de DHCP*

Es importante conocer que determinadas palabras clave de configuración y la estructura del archivo de configuración tienen un efecto en el uso de memoria y el rendimiento del servidor **DHCP**.

En primer lugar, se puede evitar el uso de memoria excesivo conociendo el modelo de opciones de herencia de los contenedores padre a hijo. En un entorno que no soporta clientes no listados, el administrador debe listar explícitamente cada cliente en el archivo. Cuando se listan opciones para cualquier cliente específico, el servidor utiliza más memoria almacenando ese árbol de configuración que cuando se heredan opciones de un contenedor padre (por ejemplo, los contenedores de subred, red o globales). Por consiguiente, el administrador debe verificar si se repiten opciones a nivel de cliente en el archivo de configuración y determinar si estas opciones se pueden especificar en el contenedor padre y compartir entre el conjunto de clientes en general.

Asimismo, al utilizar las entradas de **logItem** INFO y TRACE, se registran muchos mensajes durante el proceso de cada mensaje de cliente **DHCP**. La adición de una línea al archivo de registro puede ser una operación costosa; por consiguiente, si se limita la cantidad de registro, mejorará el rendimiento del servidor **DHCP**. Cuando se sospecha que hay un error en el servidor **DHCP**, se puede volver a habilitar dinámicamente el registro cronológico utilizando los mandatos de **traceson** o **dadmin** de SRC.

Finalmente, la selección de un valor **numprocessors** depende del tamaño de la red soportada por **DHCP**, del parámetro de configuración **pingTime db\_file** y del retardo de propagación típico en la red. Puesto

que cada hebra de procesador de paquete emite una petición de eco de ICMP para verificar el estado de una dirección que es propiedad de servidor antes de ofrecerla a un cliente, la cantidad de tiempo durante el cual se espera cualquier respuesta de eco afecta directamente a la cantidad de tiempo de proceso para un mensaje DISCOVER. Esencialmente, la hebra de procesador de paquete no puede hacer nada más que esperar cualquier respuesta o el tiempo de espera de **pingTime**. Si se reduce el valor de **numprocessors**, el tiempo de respuesta del servidor mejora reduciendo el número de retransmisiones de cliente, aunque manteniendo todavía la ventaja de ping del diseño de servidor.

Para un rendimiento óptimo, seleccione un **pingTime** basándose en el retardo de propagación de las redes remotas soportadas por el servidor **DHCP**. Asimismo, seleccione el valor **numprocessors** basándose en este valor de **pingTime** y en el tamaño de la red. La selección de un valor demasiado pequeño puede hacer que se detengan todas las hebras de proceso de paquetes. Entonces hace que el servidor espere cualquier respuesta de eco mientras los mensajes de cliente **DHCP** de entrada se ponen en cola en el puerto de servidor. Esto hace que el servidor maneje los mensajes de cliente en lotes en lugar de hacerlo en una corriente constante.

Un valor seleccionado que sea demasiado pequeño puede hacer que todas las hebras de proceso de paquetes se detengan en espera de respuestas de eco.

Para evitar esta situación, establezca el valor para **numprocessors** en un número más alto que el número estimado de mensajes DISCOVER que se pueden recibir en un intervalo de **pingTime** durante un periodo de mucha actividad de cliente **DHCP**. Sin embargo, no establezca **numprocessors** en un valor tan alto que pueda cargar el kernel con gestión de hebras.

Por ejemplo, los valores **numprocessors 5** y **pingTime 300** producen un rendimiento deficiente en un entorno con un potencial de 10 mensajes DISCOVER por segundo porque en la demanda máxima, sólo se manejan 5 mensajes cada 3 segundos. Configure este entorno con valores similares a **numprocessors 20** y **pingTime 80**.

#### **Personalización de archivo de configuración DHCP**

Hay varios factores implicados en la personalización del archivo de configuración **DHCP**.

Muchas redes incluyen varios tipos de cliente; por ejemplo, una red individual puede incluir sistemas que ejecuten diversos sistemas operativos, por ejemplo Windows, OS/2, el sistema operativo Java™ y UNIX. Cada uno de éstos necesita identificadores de proveedor exclusivos (el campo utilizado para identificar el tipo de máquina en el servidor DHCP). Las máquinas de clientes del sistema operativo Java y de cliente limitado de IBM pueden necesitar parámetros exclusivos, por ejemplo archivos de arranque, y opciones de configuración que es necesario adaptar específicamente para ellas. Los sistemas Windows 95 no manejan bien las opciones específicas de Java.

Las opciones específicas de máquina se pueden encapsular en contenedores de proveedor si el uso principal para determinadas máquinas se basa en el tipo de usuario para dichas máquinas. Por ejemplo, el personal de desarrollo puede utilizar los clientes de este sistema operativo para la programación, el personal de marketing puede utilizar los clientes de OS/2, el personal de ventas puede utilizar máquinas de clientes de sistema operativo Java y de clientes limitados de IBM y el personal de contabilidad puede utilizar las máquinas Windows 95. Cada una de estas familias de usuarios pueden necesitar diferentes opciones de configuración (diferentes impresoras, servidores de nombres o servidores web predeterminados, etc). En este caso, tales opciones pueden incluirse en el contenedor de proveedor, porque cada grupo utiliza un tipo de máquina diferente.

Si varios grupos utilizan el mismo tipo de máquina, la colocación de las opciones en un identificador de clase subordinado permitirá a los directores de marketing, por ejemplo, utilizar un conjunto específico de impresoras a las que otros empleados no pueden acceder.

**Nota:** El siguiente ejemplo ficticio representa parte de un archivo de configuración. Los comentarios van precedidos de un signo de almohadilla (#) y describen cómo define cada línea la instalación.

```
vendor "AIX_CLIENT"
{
# Ninguna opción específica, maneja los elementos basándose en la clase
}

vendor "OS/2 Client"
{
```

```

# Ninguna opción específica, maneja los elementos basándose en la clase
}

vendor "Windows 95"
{ option 44 9.3.150.3      # Servidor de nombres NetBIOS predeterminado
}

vendor "Java OS"
{ bootstrapserver 9.3.150.4    # Servidor TFTP predeterminado para recuadros de
    # sistema operativo Java
    option 67 "javaos.bin"     # Archivo de arranque del recuadro de sistema
    # operativo Java
}

vendor "IBM Thin Client"
{ bootstrapserver 9.3.150.5    # Servidor TFTP predeterminado para recuadros
    # de cliente limitado
    option 67 "thinos.bin"     # Archivo de arranque predeterminado para
    # recuadros de cliente limitado
}

subnet 9.3.149.0 255.255.255.0
{ option 3 9.3.149.1          # Pasarela predeterminada para la subred
    option 6 9.3.150.2          # Es el servidor de nombres para la subred
    class accounting 9.3.149.5-9.3.149.20
    {                         # La clase de contabilidad está limitada al rango de
        # direcciones 9.3.149.5-9.3.149.20
        # La impresora para este grupo también está en el rango, de modo
        # que se excluye.
        exclude 9.3.149.15
        option 9 9.3.149.15      # Servidor LPR (servidor de impresión)
        vendor "Windows 95"
        {
            option 9 deny          # La instalación de Windows 95 no soporta
            # esta impresora, de modo que la opción se rechaza.
        }
    }
    .
}

```

### **DHCP y el Sistema de nombres de dominio dinámico**

El servidor **DHCP** proporciona opciones que permite la operación en un entorno DDNS (Dynamic Domain Name System - Sistema de nombres de dominio dinámico).

Para utilizar **DHCP** en un entorno DDNS, debe establecer y utilizar una Zona dinámica en un servidor DNS.

Después de configurar el servidor DDNS, decida si el servidor **DHCP** va a realizar actualizaciones de registros A, actualizaciones de registros PTR, actualizaciones para ambos tipos de registro o ninguna actualización. Esta decisión depende de si una máquina cliente puede realizar parte de este trabajo o la totalidad del mismo.

- Si el cliente puede compartir la responsabilidad de actualización, configure el servidor para que realice las actualizaciones de registros PTR y configure el cliente para que realice las actualizaciones de registros A.
- Si el cliente puede realizar ambas actualizaciones, configure el servidor para que no haga ninguna.
- Si el cliente no puede realizar actualizaciones, configure el servidor para que haga las dos.

El servidor **DHCP** tiene un conjunto de palabras clave de configuración que permite especificar que se ejecute un mandato cuando se necesita una actualización. Éstas son:

#### **updatedns**

(En desuso.) Representa el mandato a emitir para que realice cualquier tipo de actualización. Se le llama para la actualización de registros PTR y de registros A.

#### **updatednsA**

Especifica al mandato que actualice el registro A.

#### **updatednsP**

Especifica al mandato que actualice el registro PTR.

Estas palabras clave especifican series ejecutables que el servidor **DHCP** ejecuta cuando se necesita una actualización. Las series de palabra clave deben contener cuatro %s (símbolo de porcentaje, letra s). El

primer %s es el nombre de sistema principal, el segundo es el nombre de dominio, el tercero es la dirección IP y el cuarto es el tiempo de alquiler. Se utilizan como los cuatro primeros parámetros para el mandato **dhcpaction**. Los dos parámetros restantes para el mandato **dhcpaction** indican el registro a actualizar (A, PTR, NONE o BOTH) y si se debe actualizar NIM (NIM o NONIM). Consulte “[Sugerencias para DHCP y la Gestión de instalación de red](#)” en la página 321 para obtener más información sobre la interacción de NIM y **DHCP**. Por ejemplo:

```
updatednsA "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' A NONIM"
           # Esto sólo ejecuta el mandato dhcpaction en el registro A
updatednsP "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' PTR NONIM"
           # Esto sólo ejecuta el mandato en el registro PTR
updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' BOTH NIM"
           # Esto ejecuta el mandato en ambos registros y actualiza NIM
```

El servidor **DHCP** también tiene un conjunto de palabras clave para eliminar las entradas DNS cuando se libera o caduca un alquiler. Las palabras clave son:

#### **releasednsA**

Elimina el registro A.

#### **releasednsP**

Elimina el registro PTR.

#### **removedns**

Elimina ambos tipos de registro.

Estas palabras clave especifican series ejecutables que el servidor **DHCP** ejecuta cuando se libera o caduca una dirección. El mandato **dhcpremove** funciona de forma similar a **dhcpaction**, pero sólo toma tres parámetros:

1. La dirección IP, especificada como %s en la serie de mandato
2. El registro que se debe eliminar (A, PTR, NONE o BOTH).
3. Determinar si NIM se debe actualizar (NIM o NONIM).

Por ejemplo:

```
releasednsA "/usr/sbin/dhcpremove '%s' A NONIM"
           # Esto sólo ejecuta mandato dhcpremove en el registro A
releasednsP "/usr/sbin/dhcpremove '%s' PTR NONIM"
           # Esto sólo ejecuta el mandato en el registro PTR
removedns "/usr/sbin/dhcpremove '%s' BOTH NIM"
           # Esto ejecuta el mandato en ambos registros y actualiza NIM
```

Los scripts **dhcpaction** y **dhcpremove** realizan una comprobación de parámetros, a continuación configuran una llamada a **nsupdate**, que se ha actualizado para funcionar con los servidores de este sistema operativo y con los servidores DDNS de OS/2. Consulte la descripción del mandato [nsupdate](#) para obtener más información.

Si la interacción de NIM NO es necesaria para la actualización de nombres, se puede configurar el servidor DHCP para que utilice una transferencia de socket entre el daemon DHCP y el mandato **nsupdate** a fin de mejorar el rendimiento y permitir recuperar las actualizaciones de DNS tras una anomalía. Para configurar esta opción, la palabra clave updateDNSA, updateDSP, releaseDNSA o releaseDSP debe especificar "nsupdate\_daemon" como primera palabra entrecomillada. Los parámetros y distintivos para esta actualización son idénticos a los que acepta el mandato **nsupdate**. Adicionalmente, se pueden utilizar los nombres de variable siguientes para sustituirlos:

Item	Descripción
\$hostname	Sustituye el nombre de sistema principal del cliente en la actualización de DNS o el nombre de sistema principal asociado anteriormente con el cliente para la eliminación de DNS.
\$domain	Sustituye el dominio DNS para la actualización o el dominio utilizado anteriormente del nombre de sistema principal de cliente para una eliminación de DNS.

Item	Descripción
<code>\$ipaddress</code>	Sustituye la dirección IP que se debe asociar o desasociar del nombre de cliente <b>DHCP</b> .
<code>\$leasetime</code>	Sustituye el tiempo de alquiler (en segundos).
<code>\$clientid</code>	Sustituye la representación de serie del identificador de cliente <b>DHCP</b> o la combinación de tipo de hardware y dirección de hardware para clientes <b>BOOTP</b> .

Por ejemplo:

```
updateDNSA "nsupdate_daemon -p 9.3.149.2 -h $hostname -d $domain
-s"d;a;*;a;a;$ipaddress;s;$leasetime;3110400"
updateDNSP "nsupdate_daemon -p 9.3.149.2 -r $ipaddress
-s"d;ptr;*;a;ptr;$hostname.$domain.;s;$leasetime;3110400"
releaseDNSA "nsupdate_daemon -p 9.3.149.2 -h $hostname -d $domain -s"d;a;*;s;1;3110400"
releaseDNSP "nsupdate_daemon -p 9.3.149.2 -r $ipaddress -s"d;ptr;*;s;1;3110400"
```

Consulte la descripción del mandato **nsupdate** para obtener más información.

Además, se han añadido políticas definidas por el administrador para intercambios de nombres de sistema principal entre el servidor y los clientes. De forma predeterminada, el nombre de sistema principal que se devuelve al cliente y se utiliza para una actualización de DDNS es la opción 12 (definida en el archivo de configuración de servidor). De forma alternativa, el nombre de sistema principal predeterminado puede ser el nombre de sistema principal sugerido por el cliente, mediante la opción 81 (opción DHCPDDNS) o mediante la opción 12 (opción HOSTNAME). Sin embargo, el administrador puede alterar temporalmente el nombre de sistema principal predeterminado utilizando las palabras clave de configuración hostnamepolicy, proxyarec y appenddomain. Estas opciones y sus parámetros se definen en el apartado “[Sintaxis de archivo de servidor DHCP para la base de datos db\\_file](#)” en la página [246](#).

### Compatibilidad de DHCP con versiones anteriores

El servidor **DHCP** reconoce la configuración de las versiones anteriores y los archivos de base de datos, `dhcps.ar` y `dhcps.cr`.

Analiza los archivos de configuración antiguos y genera nuevos archivos de base de datos en las ubicaciones anteriores. Las bases de datos antiguas se convierten automáticamente en el nuevo archivo. El propio archivo de configuración no se convierte.

El módulo de base de datos de servidor **DHCP**, `db_file`, puede leer el formato anterior. El servidor **DHCP** puede reconocer cuando un contenedor de base de datos no está en el archivo de configuración y trata el archivo entero como si configurara los parámetros de servidor, los parámetros de registro y los parámetros de base de datos `db_file`.

#### Nota:

- Parte de la sintaxis de archivo de configuración antigua ha quedado en desuso, pero aún se soporta. Los siguientes elementos también son elementos en desuso:
  - El contenedor de red está completamente en desuso. Para especificarlo correctamente, convierta la cláusula de red con un rango en un contenedor de subred válido con una dirección de subred, una máscara de subred y el rango. Si el contenedor de red tiene contenedores de subred, elimine la contraseña de contenedor de subred y las llaves y, a continuación, ponga la máscara de subred en el lugar apropiado de la línea. Para empezar a utilizar el contenedor de base de datos, agrupe todo lo que pertenece a las redes y al acceso de cliente en una contenedor de base de datos de tipo `db_file`.
  - Las palabras clave `updatedns` y `removedns` están en desuso y se han sustituido por la especificación de la acción para los registros A y PTR por separado.
  - Las palabras clave `clientrecorddb` y `addressrecorddb` se han sustituido por `clientrecorddb` y `backupfile`, respectivamente.

5. Las palabras clave `option sa` y `option ga` se han sustituido por las palabras clave `bootstrapserver` y `giaddrfield`, respectivamente. Consulte el apartado “[Sintaxis de archivo de servidor DHCP para la operación de servidor general](#)” en la página 237 y el apartado “[Sintaxis de archivo de servidor DHCP para la base de datos db\\_file](#)” en la página 246 para obtener más información.

### Opciones conocidas del archivo de servidor DHCP

Aquí se identifican las opciones conocidas del archivo de servidor **DHCP**.

**Nota:** Las opciones cuya especificación no está permitida (No en la columna ¿Se puede especificar?) que se muestran en esta tabla se pueden especificar en el archivo de configuración, pero el valor correcto se escribirá encima de las mismas. Para obtener una mejor definición de cada opción, consulte RFC 2132.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción/Utilización
0	Ninguno	No	El servidor rellena el campo de opción, si es necesario.
1	Doble palabra con puntos	No	La máscara de red de la subred de la que se ha extraído la dirección.
2	Entero de 32 bits	Sí	Especifica el desplazamiento de la subred de cliente, en segundos respecto a la Hora universal coordinada (UTC).
3	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de las pasarelas predeterminadas.
4	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor horario.
5	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor de nombres
6	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de DNS.
7	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor de registro cronológico.
8	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor de cookies
9	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor LPR.
10	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidores de impresión.
11	Una o más dobles palabras con puntos	Sí	Una lista de direcciones IP de servidor de ubicación de recursos.
12	Serie ASCII	Sí	Un nombre de sistema principal para que lo utilice el cliente.
13	Entero sin signo de 16 bits	Sí	El tamaño del archivo de arranque.
14	Serie ASCII	Sí	La vía de acceso para el archivo de vuelcos Merit.
15	Serie ASCII	Sí	El nombre de dominio DNS predeterminado.
16	Dirección IP	Sí	La dirección del servidor de intercambio.
17	Serie ASCII	Sí	La vía de acceso raíz predeterminada.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción/Utilización
18	Serie ASCII	Sí	La vía de acceso a las extensiones para el cliente.
19	Yes, No, True, False, 1, 0	Sí	Especificar si se debe activar el reenvío de IP.
20	Yes, No, True, False, 1, 0	Sí	Especificar si se debe utilizar el direccionamiento de origen no local.
21	Uno o más pares de dobles palabras con puntos, con el formato <i>DoblePuntos:DoblePuntos</i>	Sí	Las políticas de filtro para las direcciones IP.
22	Entero sin signo de 16 bits	Sí	El tamaño máximo que se debe permitir para los fragmentos de datagrama.
23	Entero sin signo de 8 bits	Sí	El tiempo de vida (TTL) de IP.
24	Entero sin signo de 32 bits	Sí	El número de segundos a utilizar en el tiempo de espera de duración de MTU de vía de acceso.
25	Lista de uno o varios enteros sin signo de 16 bits	Sí	La tabla de Plateau de MTU de vía de acceso. Especifica un conjunto de valores que representan los tamaños de MTU a utilizar cuando se utiliza el descubrimiento de MTU de vía de acceso.
26	Entero sin signo de 16 bits	Sí	Especifica el tamaño de MTU para la interfaz de recepción.
27	Yes, No, True, False, 1, 0	Sí	Especifica si todas las subredes son locales.
28	Dirección IP (doble palabra con puntos)	Sí	Especifica la dirección de difusión para la interfaz.
29	Yes, No, True, False, 1, 0	Sí	Especifica si se debe utilizar el descubrimiento de máscara de red de ICMP.
30	Yes, No, True, False, 1, 0	Sí	Especifica si el cliente se debe convertir en un proveedor de máscara de red de ICMP.
31	Yes, No, True, False, 1, 0	Sí	Especifica si se deben utilizar mensajes de descubrimiento de directorio de ICMP.
32	Dirección IP (doble palabra con puntos)	Sí	Especifica la dirección a utilizar para solicitud de directorio.
33	Uno o más pares de direcciones IP, con el formato <i>DoblePuntos:DoblePuntos</i>	Sí	Cada par de direcciones representa una ruta estática.
34	Yes/No, True/False, 1/0	Sí	Especifica si se debe utilizar la encapsulación de cola.
35	Entero sin signo de 32 bits	Sí	Valor de tiempo de espera de antememoria ARP.
36	Yes/No, True/False, 1/0	Sí	Especifica si se debe utilizar la encapsulación de Ethernet.
37	Entero sin signo de 8 bits	Sí	El tiempo de vida (TTL) de TCP.
38	Entero sin signo de 32 bits	Sí	El intervalo de mantenimiento de actividad de TCP.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción/Utilización
39	Yes/No, True/False, 1/0	Sí	Especifica si se debe utilizar el mantenimiento de actividad de TCP.
40	Serie ASCII	Sí	El dominio NIS predeterminado.
41	Una o más dobles palabras con puntos	Sí	Especifica las direcciones IP de los servidores NIS.
42	Una o más dobles palabras con puntos	Sí	Especifica las direcciones IP de los servidores NTP.
43	serie hexadecimal de dígitos, con el formato de hex " <i>dígitos</i> ", hex " <i>dígitos</i> " o 0xd <i>dígitos</i>	Sí, pero realmente sólo se especifica con contenedor de proveedor	Contenedor de opción encapsulado para el contenedor de proveedor.
44	Una o más dobles palabras con puntos	Sí	Especifica las direcciones IP de servidor de nombres de NetBIOS.
45	Una o más dobles palabras con puntos	Sí	Especifica direcciones IP de servidor de distribución de datagrama de NetBIOS.
46	Entero sin signo de 8 bits	Sí	Especifica el tipo de nodo de NetBIOS.
47	serie hexadecimal de dígitos, con el formato de hex " <i>dígitos</i> ", hex " <i>dígitos</i> " o 0xd <i>dígitos</i>	Sí	Ámbito de NetBIOS.
48	Una o más dobles palabras con puntos	Sí	Especifica las direcciones IP del servidor de fuentes de Windows X.
49	Una o más dobles palabras con puntos	Sí	Especifica el Gestor de pantalla X Windows.
50	Ninguno	No	Dirección IP solicitada, utilizada por el cliente para indicar la dirección que desea.
51	Entero sin signo de 32 bits	Sí	Tiempo de alquiler para la dirección devuelta. De forma predeterminada, el servidor <b>DHCP</b> utiliza la palabra clave <b>leasetimedefault</b> , pero la especificación directa de la opción 51 la altera temporalmente.
52	Ninguno	No	Sobrecarga de opción. El cliente la utiliza para indicar que los campos <b>sname</b> y <b>file</b> del paquete <b>BOOTP</b> pueden tener opciones.
53	Ninguno	No	El cliente o el servidor <b>DHCP</b> utiliza esta opción para indicar el tipo de mensaje <b>DHCP</b> .
54	Ninguno	No	El servidor o el cliente <b>DHCP</b> utiliza esta opción para indicar la dirección del servidor o el servidor al que va dirigido el mensaje.
55	Ninguno	No	El cliente <b>DHCP</b> la utiliza para indicar las opciones deseadas.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción/Utilización
56	Serie ASCII	Sí	Serie que el servidor <b>DHCP</b> envía al cliente. En general, la pueden utilizar el servidor y el cliente <b>DHCP</b> para indicar problemas.
57	No	No	El cliente <b>DHCP</b> utiliza esta opción para indicar al servidor <b>DHCP</b> el tamaño máximo de paquete <b>DHCP</b> que el cliente puede recibir.
58	Entero sin signo de 32 bits	Sí	Especifica el número de segundos hasta que el cliente debe enviar un paquete de renovación.
59	Entero sin signo de 32 bits	Sí	Especifica el número de segundos hasta que el cliente debe enviar un paquete de renvinculación.
60	Ninguno	No	El cliente <b>DHCP</b> utiliza esta opción para indicar el tipo de proveedor. El servidor <b>DHCP</b> utiliza este campo para comparar contenedores de proveedor.
61	Ninguno	No	El cliente <b>DHCP</b> la utiliza para identificarse a sí mismo de forma exclusiva. El servidor <b>DHCP</b> utiliza este campo para comparar contenedores de cliente.
66	Serie ASCII	Sí	Especifica el servidor de nombres <b>TFTP</b> . Es el nombre de sistema principal y se utiliza en lugar del campo <b>siaddr</b> si el cliente conoce esta opción.
67	Serie ASCII	Sí	Especifica el nombre de archivo de arranque. Se puede utilizar en lugar de la palabra clave <b>bootfile</b> , que pone el archivo en el campo <b>filename</b> del paquete.
68	Una o más dobles palabras con puntos o NONE	Sí	Especifica direcciones de agentes iniciales.
69	Una o más dobles palabras con puntos	Sí	Especifica los servidores SMTP predeterminados a utilizar.
70	Una o más dobles palabras con puntos	Sí	Especifica los servidores POP3 predeterminados a utilizar.
71	Una o más dobles palabras con puntos	Sí	Especifica los servidores NNTP predeterminados a utilizar.
72	Una o más dobles palabras con puntos	Sí	Especifica los servidores WWW predeterminados a utilizar.
73	Una o más dobles palabras con puntos	Sí	Especifica los servidores Finger predeterminados a utilizar.
74	Una o más dobles palabras con puntos	Sí	Especifica los servidores IRC predeterminados a utilizar.
75	Una o más dobles palabras con puntos	Sí	Especifica los servidores Street Talk predeterminados a utilizar.
76	Una o más dobles palabras con puntos	Sí	Especifica los servidores de asistencia de directorio de Street Talk predeterminados a utilizar.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción/Utilización						
77	Serie ASCII	Sí	Identificador de clase de sitio de usuario. El servidor <b>DHCP</b> utiliza este campo para comparar contenedores de clase.						
78	Byte obligatorio, una o más dobles palabras con puntos	Sí	La opción de agente de directorio de SLP especifica una lista de direcciones IP para Agentes de directorio						
79	Byte obligatorio y serie ASCII	Sí	La serie ASCII es una lista de ámbito, que es una lista delimitada por coma, que indica los ámbitos que utilizará un agente SLP porque así se ha configurado						
81	Serie ASCII más otros elementos	No	El cliente DHCP utiliza esta opción para definir la política que el servidor <b>DHCP</b> debe utilizar respecto a DDNS.						
85	Una o más dobles palabras con puntos	Sí	La opción de servidor NDS especifica uno o más servidores NDS que el cliente debe contactar para acceder a la base de datos DNS. Los servidores se deberá listar en orden de preferencia.						
86	Serie ASCII	Sí	La opción de nombre de árbol NDS especifica el nombre del árbol NDS con el que el cliente se pondrá en contacto.						
87	Serie ASCII	Sí	La opción de contexto NDS especifica el contexto NDS inicial que el cliente debe utilizar.						
93	Ninguno	No	El cliente DHCP utiliza esta opción para definir la arquitectura de sistema cliente.						
94	Ninguno	No	El cliente DHCP utiliza esta opción para definir el identificador de interfaz de red de cliente.						
117	Uno o más enteros sin signo de 16 bits	Sí	La opción de búsqueda de servicio de nombres proporciona el orden preferido de código de opción de entero para servicios de nombres. Por ejemplo:						
			<table> <tr> <td>Servicios de nombres</td> <td>valor</td> </tr> <tr> <td>Opción servidor nombres dominio</td> <td>6</td> </tr> <tr> <td>Opción NIS</td> <td>41</td> </tr> </table>	Servicios de nombres	valor	Opción servidor nombres dominio	6	Opción NIS	41
Servicios de nombres	valor								
Opción servidor nombres dominio	6								
Opción NIS	41								
118	Una doble palabra con puntos	No	La opción de selección de subred es una opción enviada por el cliente solicitando al servidor dhcp que asigne la dirección IP de la subred especificada.						
255	Ninguno	No	El servidor y el cliente DHCP utilizan esta opción para indicar el final de una lista de opciones.						

#### Subopción de contenedor de proveedor de entorno de ejecución previa al arranque

Cuando se soporta un cliente PXE (Entorno de ejecución previa al arranque), el servidor **DHCP** pasa al servidor BINLD la siguiente opción, que BINLD utiliza para configurarse.

Núm. opc.	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
7	una doble palabra con puntos	Sí	Dirección IP multidifusión. Dirección IP multidifusión de descubrimiento de servidor de arranque.

El ejemplo siguiente muestra cómo se puede utilizar esta opción:

```
pxeservertype proxy_on_dhcp_server
Vendor pxeserver
{
    option 7 9.3.4.68
```

En el ejemplo anterior, el servidor **DHCP** informa al cliente que el servidor proxy se ejecuta en la misma máquina pero está escuchando en el puerto 4011 para las peticiones de cliente. El contenedor de proveedor es necesario aquí porque el servidor BINLD difunde un mensaje INFORM/REQUEST en el puerto 67 con la opción 60 establecida en "PXEserver." En respuesta, el servidor **DHCP** envía la dirección IP multidifusión en la que BINLD tiene que escuchar la petición de PXEclient.

En el ejemplo siguiente, el servidor **dhcpsd** da el nombre de archivo de arranque al PXEclient o dirige a PXEclient al servidor BINLD enviando subopciones. La palabra clave **pxebootfile** se utiliza para crear una lista de archivos de arranque para una arquitectura de cliente determinada y versiones mayores y menores del sistema cliente.

```
pxeservertype dhcp_pxe_binld
subnet default
{
    vendor pxe
    {
        option 6 2 # Inhabilitar multidifusión
        option 8 5 4 10.10.10.1 12.1.1.15 12.5.5.5 12.6.6.6\
                    2 2 10.1.1.10 9.3.4.5 1 1 10.5.5.9\
                    1 1 9.3.149.15\
                    4 0
        option 9 5 "WorkSpace On Demand" 2 "Intel"\
                    1 "Microsoft Windows NT" 4 "NEC ESMPRO"
        option 10 2 "Press F8 to View Menu"
    }
    vendor pxeserver
    {
        option 7 239.0.0.239
    }
}

subnet 9.3.149.0 255.255.255.0
{
    option 3 9.3.149.1
    option 6 9.3.149.15

    vendor pxe
    {
        option 6 4 # archivo de arranque presente en el paquete de oferta
        pxebootfile 1 2 1 os2.one
        pxebootfile 2 2 1 aix.one
    }
}
```

El servidor utiliza cada línea de opción del contenedor PXE para indicar al cliente qué debe hacer. ["Subopciones de contenedor de proveedor PXE"](#) en la página 352 describe las subopciones de PXE conocidas y soportadas actualmente.

## Sintaxis de archivo de servidor DHCP para la operación de servidor general

Aquí se define la sintaxis de archivo **DHCP** para la operación de servidor general y los valores válidos para cada campo.

**Nota:** Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
database	database <i>tipo_bd</i>	Sí	Ninguno	El contenedor primario que contiene las definiciones para las agrupaciones de dirección, las opciones y las sentencias de acceso de cliente. <i>tipo_bd</i> es el nombre de un módulo que se carga para procesar esta parte del archivo. El único valor actualmente disponible es db_file.
logging_info	logging_info	Sí	Ninguno	El contenedor de registro cronológico primario que define los parámetros de registro.
logitem	logitem NONE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem SYSERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem OBJERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem PROTOCOL	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem PROTERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem WARN	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem WARNING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem CONFIG	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem EVENT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem PARSEERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem ACTION	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem ACNTING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem STAT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem TRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem RTRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem START	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
numLogFiles	numLogFiles <i>n</i>	No	0	Especifica el número de archivos de registro cronológico a crear. El registro cronológico rota cuando el primero se llena. <i>n</i> es el número de archivos que se deben crear.
logFileSize	logFileSize <i>n</i>	No	0	Especifica el tamaño de cada archivo de registro cronológico en unidades de 1024 bytes.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
logFileName	logFileName <i>vía_acceso</i>	No	Ninguno	Especifica la vía de acceso al primer archivo de registro cronológico. El archivo de registro cronológico original se denomina <i>nombre_archivo</i> o <i>nombre_arch.ext</i> . Cuando un archivo se rota, se redenomina empezando con el <i>nombre_archivo</i> base y, a continuación, añadiendo un número o sustituyendo la extensión por un número. Por ejemplo, si el nombre de archivo original es <i>file</i> , el nombre de archivo rotado se convierte en <i>file01</i> . Si el nombre de archivo original es <i>file.log</i> , se convierte en <i>file.01</i> .
CharFlag	charflag yes	No	true	No se aplica al servidor <b>DHCP</b> de este sistema operativo, pero el servidor OS/2 <b>DHCP</b> lo utiliza para producir ventanas de depuración.
CharFlag	charflag true	No	true	No se aplica al servidor <b>DHCP</b> de este sistema operativo, pero el servidor OS/2 <b>DHCP</b> lo utiliza para producir ventanas de depuración.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
CharFlag	charflag false	No	true	No se aplica al servidor <b>DHCP</b> de este sistema operativo, pero el servidor OS/2 <b>DHCP</b> lo utiliza para producir ventanas de depuración.
CharFlag	charflag no	No	true	No se aplica al servidor <b>DHCP</b> de este sistema operativo, pero el servidor OS/2 <b>DHCP</b> lo utiliza para producir ventanas de depuración.
StatisticSnapShot	StatisticSnapShot <i>n</i>	No	-1, never	Especifica, en segundos, la frecuencia con la que se graban estadísticas en el archivo de registro cronológico.
UsedIpAddressExpireInterval	UsedIpAddressExpireInterval <i>n unidades_tiempo</i>	No	-1, never	Especifica la frecuencia con la que las direcciones que están en estado BAD se recuperan y se comprueban para ver su validez.
leaseExpireInterval	leaseExpireInterval <i>n unidades_tiempo</i>	No	900 segundos	Especifica la frecuencia con la que las direcciones en estado BOUND se comprueban para ver si han caducado. Si la dirección ha caducado, el estado pasa a EXPIRED.
reservedTime	reservedTime <i>n unidades_tiempo</i>	No	-1, never	Especifica cuánto tiempo deben permanecer las direcciones en estado RESERVED antes de recuperar el estado FREE.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
reservedTimeInterval	reservedTimeInterval <i>n unidades_tiempo</i>	No	900 segundos	Especifica la frecuencia con la que las direcciones en estado RESERVE se comprueban para ver si deben recuperar el estado FREE.
saveInterval	saveInterval <i>n unidades_tiempo</i>	No	3600 segundos	Especifica la frecuencia con la que el servidor <b>DHCP</b> debe forzar una operación de guardar las bases de datos abiertas. Para servidores muy cargados, debe ser 60 o 120 segundos.
clientpruneintv	clientpruneintv <i>n unidades_tiempo</i>	No	3600 segundos	Especifica la frecuencia con la que el servidor <b>DHCP</b> hace que las bases de datos eliminen clientes que no están asociados con ninguna dirección (en estado UNKNOWN). Esto reduce el uso de memoria del servidor <b>DHCP</b> .
numprocessors	numprocessors <i>n</i>	No	10	Especifica el número de procesadores de paquetes que se deben crear. Un mínimo de uno.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
userObject	userObject <i>nombre_obj</i>	Sí	Ninguno	Indica que el servidor debe cargar un objeto compartido definido por el usuario y llamar a las rutinas en este objeto mediante cada interacción con los clientes <b>DHCP</b> . El objeto que se debe cargar está ubicado en el directorio /usr/sbin con el nombre <i>nombre_obj</i> .dhcpo. Consulte la API de extensión definida por el usuario del servidor DHCP para obtener más información.
pxeservertype	pxeservertype <i>tipo_servidor</i>	No	dhcp_only	<p>Indica el tipo de servidor <b>dhcpd</b> que es. <i>tipo_servidor</i> puede ser uno de los siguientes:</p> <p><b>dhcp_pxe_binld</b>  <b>DHCP</b> realiza las funciones <b>dhcpsd</b>, <b>pxed</b> y <b>bindl</b>.</p> <p><b>proxy_on_dhcp_server</b>  <b>DHCP</b> hace referencia al cliente PXE en el puerto de servidor proxy de la misma máquina.</p> <p>El valor predeterminado es <b>dhcp_only</b>, que significa que <b>dhcpsd</b> no soporta clientes PXE en modalidad predeterminado.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportsubnetselection	supportsubnetselection global supportsubnetselection subnetlevel supportsubnetselection no	No	Ninguno	Indica si el servidor dhcp va a soportar la opción 118 (opción de selección de subred) en el paquete DISCOVER o REQUEST de clientes.  global: todas las subredes del archivo de configuración soportarán la opción 118.  subnetlevel: las subredes que se han configurado para soportar esta opción mediante la palabra clave supportoption118 soportarán esta opción.  no: no soporta la opción 118.

#### Sintaxis de archivo de servidor DHCP para la base de datos db\_file

La sintaxis de archivo para la base de datos db\_file tiene las propiedades siguientes.

**Nota:**

1. Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.
2. Los elementos especificados en un contenedor se pueden alterar temporalmente en otro subcontenedor. Por ejemplo, puede definir globalmente clientes **BOOTP**, pero dentro de una subred determinada permitir clientes **BOOTP** especificando la palabra clave supportBootp en ambos contenedores.
3. Los contenedores de cliente, clase y proveedor permiten el soporte de expresiones regulares. Para clase y proveedor, una serie entrecomillada donde el primer carácter después de las comillas es un punto de exclamación (!) indica que se debe tratar el resto de la serie como una expresión regular. El contenedor de cliente permite expresiones regulares en los campos hwtype y hwaddr. Se utiliza una sola serie para representar ambos campos con el formato siguiente:

número\_decimal-datos

Si número\_decimal es cero, los datos son una serie ASCII. Si es cualquier otro número, los datos son dígitos hexadecimales.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
subred	subnet default	Sí	Ninguno	Especifica una subred sin ningún rango asociado. El servidor utiliza esta subred sólo cuando se responde a un paquete INFORM/ REQUEST de cliente desde el cliente y la dirección del cliente no tiene otro contenedor de subred coincidente.
subred	subnet <i>id subred</i> máscara de red	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
subred	subnet <i>id subred</i> <i>máscara de red rango</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
subred	subnet <i>id</i> subred <i>máscara de red</i> <i>etiqueta:prioridad</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
subred	subnet <i>id</i> subred <i>máscara de red rango</i> <i>etiqueta:prioridad</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
subred	subnet <i>id subred rango</i>	Sí	Ninguno	<p>Especifica una subred que va dentro de un contenedor de red. Define un rango de direcciones que es la subred entera a menos que se especifique la parte de rango opcional. La máscara de red asociada con la subred se toma del contenedor de red que la rodea.</p> <p><b>Nota:</b> Este método está en desuso y se ha sustituido por los demás formatos de subred.</p>
option	option <i>número datos ...</i>	No	Ninguno	<p>Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i>, <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i>. Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
option	option <i>númerodeny</i>	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
option	option * deny	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>número</i> deny sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), Ox <i>dígitoshex</i> , hex" <i>dígitoshex</i> " o hex " <i>dígitoshex</i> ". Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.
exclude	exclude <i>una dirección IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
exclude	exclude <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.
range	range <i>dirección_IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
range	range <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
client	client <i>tipohw dirhw</i> NONE	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>dirhw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
client	client <i>tipohw dirhw ANY</i>	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
client	client <i>tipohw dirhw doble_puntos</i>	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>dirhw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
client	client <i>tipohw dirhw rango</i>	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
class	class <i>serie</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
class	class <i>serie rango</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
red	network <i>id</i> red máscara <i>red</i>	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
red	network <i>id red</i>	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
red	network <i>id red rango</i>	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor_hex</i> ""	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor_hex</i> ""	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> 0xdata	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> ""	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> <i>rango</i>	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor rango hex</i> ""	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> <i>rango hex</i> ""	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> <i>rango</i> 0xdata	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> <i>rango</i> ""	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción.</p> <p><i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
inoption	inoption <i>número</i> <i>datos_opción</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
inoption	inoption <i>número</i> <i>datos_opción rango</i>	Sí	Ninguno	<p>Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo.</p> <p>Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
virtual	virtual fill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
virtual	virtual sfill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
virtual	virtual rotate <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
virtual	virtual srotate <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
inorder:	inorder: <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política de llenado, que significa utilizar todas las direcciones del contenedor antes de ir al siguiente contenedor. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.
balance:	balance: <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política de rotación, que significa utilizar la siguiente dirección del siguiente contenedor. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.
supportBootp	supportBootp true	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .
supportBootp	supportBootp 1	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .

Palabra clave	Formato	Subcontene- dores	Valor predeterminado	Significado
supportBootp	supportBootp yes	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .
supportBootp	supportBootp false	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .
supportBootp	supportBootp 0	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .
supportBootp	supportBootp no	No	Sí	Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .
supportBootp				Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes <b>BOOTP</b> .

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportUnlistedclients	supportUnlistedclients BOTH	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>
supportUnlistedclients	supportUnlistedclients DHCP	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportUnlistedclients	supportUnlistedclients BOOTP	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>
supportUnlistedclients	supportUnlistedclients NONE	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportUnlistedclients	supportUnlistedclients true	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>
supportUnlistedclients	supportUnlistedclients yes	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportUnlistedclients	supportUnlistedclients 1	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>
supportUnlistedclients	supportUnlistedclients false	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportUnlistedclients	supportUnlistedclients no	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>
supportUnlistedclients	supportUnlistedclients 0	No	Both	<p>Especifica si el contenedor actual y todos los que están bajo él (hasta que se alteren temporalmente) deben soportar clientes no listados. El valor indica si se debe permitir el acceso a todos los clientes sin sentencias de cliente específicas, sólo a los clientes <b>DHCP</b>, sólo a los clientes <b>BOOTP</b> o a ninguno.</p> <p><b>Nota:</b> Los valores true y false se soportan por compatibilidad con versiones anteriores y están en desuso. El valor true corresponde a BOTH y el valor false corresponde a NONE.</p>

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
addressrecorddb	addressrecrddb <i>vía de acceso</i>	No	Ninguno	<p>Si se especifica, funciona como la palabra clave <b>backupfile</b>. Sólo es válido en el nivel de contenedor global o de base de datos.</p> <p><b>Nota:</b> Este método está en desuso.</p>
backupfile	backupfile <i>vía de acceso</i>	No	/etc/db_file.crbk	Especifica el archivo a utilizar para las copias de seguridad de base de datos. Sólo es válido en el nivel de contenedor global o de base de datos.
checkpointfile	checkpointfile <i>vía de acceso</i>	No	/etc/db_file.chkpt	Especifica los archivos de punto de comprobación de base de datos. El primer archivo de punto de comprobación es <i>vía de acceso</i> . El segundo archivo de punto de comprobación es <i>vía de acceso</i> con el último carácter sustituido por un 2. Por consiguiente, el archivo de punto de comprobación no debe terminar en 2. Sólo es válido en el nivel de contenedor global o de base de datos.
clientrecorddb	clientrecorddb <i>vía de acceso</i>	No	/etc/db_file.cr	Especifica el archivo para guardar la base de datos. El archivo contiene todos los registros de cliente que el servidor <b>DHCP</b> ha atendido. Sólo es válido en el nivel de contenedor global o de base de datos.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
bootstrapserver	bootstrapserver <i>dirección IP</i>	No	Ninguno	Especifica el servidor que los clientes deben utilizar para realizar <b>TFTP</b> en los archivos después de recibir paquetes <b>BOOTP</b> o <b>DHCP</b> . Este valor rellena el campo <b>siaddr</b> del paquete. Es válido en cualquier nivel de contenedor.
giaddrfield	giaddrfield <i>dirección IP</i>	No	Ninguno	Especifica giaddrfield para los paquetes de respuesta.  <b>Nota:</b> Esta especificación no está permitida en los protocolos <b>BOOTP</b> y <b>DHCP</b> , pero algunos clientes necesitan que el campo <b>giaddr</b> sea la pasarela predeterminada para la red. Debido a este potencial conflicto, giaddrfield sólo se deberá utilizar en un contenedor cliente, aunque puede funcionar a cualquier nivel.
pingTime	pingTime <i>n unidad_tiempo</i>	No	3 segundos	Especifica la cantidad de tiempo a esperar una respuesta de ping antes de distribuir una dirección. La unidad de tiempo predeterminada son las centésimas de segundo. El valor de unidad de tiempo se define en la nota que precede a esta tabla. Es válido en cualquier nivel de contenedor. El parámetro <i>unidad_tiempo</i> es opcional.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
bootptime	bootptime <i>n unidad_tiempo</i>	No	-1, infinite	Especifica la cantidad de tiempo que se debe alquilar una dirección a un cliente <b>BOOTP</b> . El valor predeterminado es -1, que significa infinito. Están disponibles los valores de unidad de tiempo normales. El parámetro <i>unidad_tiempo</i> es opcional. Es válido en cualquier nivel de contenedor.
AllRoutesBroadcast	allroutesbroadcast no	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.
AllRoutesBroadcast	allroutesbroadcast false	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
AllRoutesBroadcast	allroutesbroadcast 0	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.
AllRoutesBroadcast	allroutesbroadcast yes	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.
AllRoutesBroadcast	allroutesbroadcast true	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
AllRoutesBroadcast	allroutesbroadcast 1	No	0	Especifica si las respuestas se deben difundir a todas las rutas, si se necesita una respuesta de difusión. Es válido en cualquier nivel de contenedor. Los servidores <b>DHCP</b> del sistema operativo lo ignoran porque la dirección MAC real del cliente, incluido RIF, se almacena para el paquete de retorno. Es válido en cualquier nivel de contenedor.
addressassigned	addressassigned "serie"	No	Ninguno	Especifica una serie entrecomillada a ejecutar cuando se asigna una dirección a un cliente. La serie debe tener dos %s. El primer %s es el id de cliente con el formato <i>tipo-serie</i> . El segundo %s es una dirección IP en formato de doble palabra con puntos. Es válido en cualquier nivel de contenedor.
addressreleased	addressreleased "serie"	No	Ninguno	Especifica una serie entrecomillada a ejecutar cuando un cliente libera una dirección. La serie debe tener un %. %s es la dirección IP que se está liberando en formato de doble palabra con puntos. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
appenddomain	appenddomain 0	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.
appenddomain	appenddomain no	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.
appenddomain	appenddomain false	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.
appenddomain	appenddomain 1	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
appenddomain	appenddomain yes	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.
appenddomain	appenddomain true	No	No	Especifica si se debe añadir el nombre de dominio de la opción 15 definida al nombre de sistema principal sugerido por el cliente en el caso de que el cliente no sugiera un nombre de dominio. Es válido en cualquier nivel de contenedor.
canonical	canonical 0	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.
canonical	canonical no	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.
canonical	canonical false	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.
canonical	canonical 1	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
canonical	canonical yes	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.
canonical	canonical true	No	0	Especifica que el id de cliente está en formato canónico. Esto sólo es válido en el contenedor de cliente.
leaseTimeDefault	leaseTimeDefault <i>n unidad_tiempo</i>	No	86400 segundos	Especifica el tiempo de alquiler predeterminado para los clientes. Es válido en cualquier nivel de contenedor. El parámetro <i>unidad_tiempo</i> es opcional.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
proxyarec	proxyarec never	No	usedhcpdnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpdns significa utilizar la opción 81 si el cliente la especifica. usedhcpdnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
proxyarec	proxyarec usedhcpddns	No	usedhcpdnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpdns significa utilizar la opción 81 si el cliente la especifica. usedhcpdnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
proxyarec	proxyarec usedhcpddnsplus	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpdns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
proxyarec	proxyarec always	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpddns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
proxyarec	proxyarec usedhcpddnsprotected	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpdns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
proxyarec	proxyarec usedhcpddnsplusprotect ed	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpddns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
proxyarec	proxyarec alwaysprotected	No	usedhcpdnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpdns significa utilizar la opción 81 si el cliente la especifica. usedhcpdnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontene- dores	Valor predeterminado	Significado
proxyarec	proxyarec standard	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpddns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
	proxyarec protected	No	usedhcpddnsplus	Especifica qué opciones y métodos se deben utilizar para las actualizaciones del registro A en el DNS. never significa no actualizar nunca el registro A. usedhcpddns significa utilizar la opción 81 si el cliente la especifica. usedhcpddnsplus significa utilizar la opción 81 o la opción 12 y 15, si se especifican. always significa realizar la actualización del registro A para todos los clientes. XXXXprotected modifica el mandato <b>nsupdate</b> para asegurarse de que se permite el cliente. standard es sinónimo de always. protected es sinónimo de alwaysprotected. Es válido en cualquier nivel de contenedor.
releasednsA	releasednsA "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se libera una dirección. La serie se utiliza para eliminar el registro A asociado con la dirección liberada. Es válido en cualquier nivel de contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
releasednsP	releasednsP "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se libera una dirección. La serie se utiliza para eliminar el registro PTR asociado con la dirección liberada. Es válido en cualquier nivel de contenedor.
removedns	removedns "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se libera una dirección. La serie se utiliza para eliminar los registros PTR y A asociados con la dirección liberada. Es válido en cualquier nivel de contenedor.  <b>Nota:</b> Esto está en desuso y se ha sustituido por las palabras clave releasednsA y releasednsP.
updatedns	updatedns "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se vincula una dirección. La serie se utiliza para actualizar los registros A y PTR asociados con la dirección. Es válido en cualquier nivel de contenedor.  <b>Nota:</b> Esto está en desuso y se ha sustituido por las palabras clave updatednsA y updatednsP.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
updatednsA	updatednsA "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se vincula una dirección. La serie se utiliza para actualizar el registro A asociado con la dirección. Es válido en cualquier nivel de contenedor.
updatednsP	updatednsP "serie"	No	Ninguno	Especifica la serie de ejecución a utilizar cuando se vincula una dirección. La serie se utiliza para actualizar el registro PTR asociado con la dirección. Es válido en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy suggested	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy resolved	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy always_resolved	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy defined	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy always_defined	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene- dores</b>	<b>Valor predetermina- do</b>	<b>Significado</b>
hostnamepolicy	hostnamepolicy default	No	por omisión	Especifica qué nombre de sistema principal se debe devolver al cliente. La política predeterminada es preferir el nombre de sistema principal y el nombre de dominio definidos a los nombres sugeridos. Otras políticas implican un seguimiento estricto (por ejemplo: defined devolverá el nombre definido o ninguno si no se define ningún nombre en la configuración). Asimismo, las políticas que utilizan el modificador always obligarán al servidor a devolver la opción de nombre de sistema principal independientemente de que el cliente la haya solicitado a través de la opción de lista de parámetros. Tenga en cuenta que la sugerencia de un nombre de sistema principal también implica solicitarlo y que los nombres de sistema principal se pueden sugerir a través de la opción 81 o a través de las opciones 12 y 15. Esta palabra clave es válida en cualquier nivel de contenedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
bootfilepolicy	bootfilepolicy suggested	No	suggested	Especifica la preferencia para devolver el nombre de archivo de arranque a un cliente. suggested prefiere el nombre de archivo de arranque sugerido por el cliente a cualquier nombre configurado por el servidor. merge añade el nombre sugerido por el cliente al directorio inicial configurado por el servidor. defined prefiere el nombre definido respecto a cualquier nombre de archivo de arranque sugerido. always devuelve el nombre definido independientemente de que el cliente solicite la opción de archivo de arranque a través de la opción de lista de parámetros.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predetermina-do</b>	<b>Significado</b>
bootfilepolicy	bootfilepolicy merge	No	suggested	Especifica la preferencia para devolver el nombre de archivo de arranque a un cliente. suggested prefiere el nombre de archivo de arranque sugerido por el cliente a cualquier nombre configurado por el servidor. merge añade el nombre sugerido por el cliente al directorio inicial configurado por el servidor. defined prefiere el nombre definido respecto a cualquier nombre de archivo de arranque sugerido. always devuelve el nombre definido independientemente de que el cliente solicite la opción de archivo de arranque a través de la opción de lista de parámetros.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontene-dores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
bootfilepolicy	bootfilepolicy defined	No	suggested	Especifica la preferencia para devolver el nombre de archivo de arranque a un cliente. suggested prefiere el nombre de archivo de arranque sugerido por el cliente a cualquier nombre configurado por el servidor. merge añade el nombre sugerido por el cliente al directorio inicial configurado por el servidor. defined prefiere el nombre definido respecto a cualquier nombre de archivo de arranque sugerido. always devuelve el nombre definido independientemente de que el cliente solicite la opción de archivo de arranque a través de la opción de lista de parámetros.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
bootfilepolicy	bootfilepolicy always	No	suggested	Especifica la preferencia para devolver el nombre de archivo de arranque a un cliente. suggested prefiere el nombre de archivo de arranque sugerido por el cliente a cualquier nombre configurado por el servidor. merge añade el nombre sugerido por el cliente al directorio inicial configurado por el servidor. defined prefiere el nombre definido respecto a cualquier nombre de archivo de arranque sugerido. always devuelve el nombre definido independientemente de que el cliente solicite la opción de archivo de arranque a través de la opción de lista de parámetros.
stealfromchildren	stealfromchildren true	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
stealfromchildren	stealfromchildren 1	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.
stealfromchildren	stealfromchildren yes	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
stealfromchildren	stealfromchildren false	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.
stealfromchildren	stealfromchildren 0	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
stealfromchildren	stealfromchildren no	No	No	Especifica si el contenedor padre debe "robar" de los contenedores hijo cuando se queda sin direcciones. Esto significa que si tiene una subred con la clase definida con un rango de direcciones, esas direcciones están reservadas para los clientes que especifiquen esa clase. Si stealfromchildren es verdadero (true), las direcciones se extraerán de un hijo para intentar satisfacer la petición. El valor predeterminado es no robar una dirección.
homedirectory	homedirectory <i>vía de acceso</i>	No	Ninguno	Especifica el directorio inicial a utilizar en la sección de archivo del paquete de respuesta. Se puede especificar a cualquier nivel de contenedor. La política de archivo de arranque (bootfile) define cómo interactúan los elementos especificados en la sección de archivo del paquete de entrada con el archivo de arranque y las sentencias de directorio inicial.

<b>Palabra clave</b>	<b>Formato</b>	<b>Subcontenedores</b>	<b>Valor predeterminado</b>	<b>Significado</b>
bootfile	bootfile <i>vía de acceso</i>	No	Ninguno	Especifica el archivo de arranque a utilizar en la sección de archivo del paquete de respuesta. Se puede especificar a cualquier nivel de contenedor. La política de archivo de arranque (bootfile) define cómo interactúan los elementos especificados en la sección de archivo del paquete de entrada con el archivo de arranque y las sentencias de directorio inicial.
pxebootfile	pxebootfile <i>arquitectura_sistema</i> <i>versión_principal</i> <i>versión_secundaria</i> <i>nombre_archivo_arranque</i>	No	Ninguno	Especifica el archivo de arranque que se debe proporcionar a un cliente. Sólo se utiliza cuando <b>dhcpsd</b> soporta clientes PXE (pxeservertype es dhcp_pxe_binld). El analizador de archivo de configuración genera un error si el número de parámetros después de pxebootfile es menor que cuatro e ignora cualquier parámetro adicional. pxebootfile sólo se puede utilizar en un contenedor.

Palabra clave	Formato	Subcontenedores	Valor predeterminado	Significado
supportoption118	supportoption118 no/ yes	No. Sólo se puede definir en el contenedor de subred.	Ninguno	Esta palabra clave especifica si este contenedor soporta la opción 118. Yes significa que se soporta y No significa que no se soporta. Para que esta opción entre en vigor, también tiene que utilizar la palabra clave supportsubnetselection.

### Sugerencias para DHCP y la Gestión de instalación de red

El concepto de asignación dinámica de direcciones de IP (Protocolo Internet) es bastante nuevo. Se proporcionan las siguientes sugerencias para ayudarle con la interacción de **DHCP** y NIM (Network Installation Management - Gestión de instalación de red).

1. Al configurar objetos en el entorno NIM, utilice nombres de sistema principal siempre que sea posible. Esto le permite utilizar un servidor de nombres dinámico que actualice las direcciones IP cuando el nombre de sistema principal se convierta en una dirección IP en el entorno NIM.
2. Coloque el maestro NIM y el servidor **DHCP** en el mismo sistema. El servidor **DHCP** tiene una opción en la serie DNS de actualización que, cuando se establece en NIM, intenta mantener los objetos NIM fuera de los estados que necesitan direcciones IP estáticas cuando dichas direcciones cambian.
3. Para los clientes NIM, establezca el tiempo de alquiler predeterminado en el doble de tiempo que se tarda en instalar un cliente. Esto permite que una dirección IP alquilada sea válida durante la instalación. Después de la instalación, reinicie el cliente. **DHCP** se iniciará o necesitará configurarse, en función del tipo de instalación.
4. El servidor dhcpsd debe ser responsable de PTR y de los registros A DNS. Cuando se vuelve a instalar NIM en la máquina, el archivo que contiene RSA se suprime y el cliente no puede actualizar el registro. El servidor actualiza los registros del sistema. Para ello, cambie la línea updatedns de /etc/dhcpcd.ini por:

```
updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' NONE NONIM"
```

En el archivo /etc/dhcpsd.cnf, cambie la línea updatedns por:

```
updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' BOTH NIM"
```

**Nota:** Cuando se pone un objeto NIM en estado pendiente de instalación de BOS, es posible que el servidor dhcpsd pase argumentos que son diferentes de los que se pretendía pasar originalmente. Minimice el tiempo que el cliente está en este estado pendiente para evitar esta situación.

Estas sugerencias permiten que el entorno NIM funcione con clientes dinámicos.

### Protocolo de configuración dinámica de sistemas principales (Dynamic Host Configuration Protocol) versión 6

El **DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de sistemas principales)** proporciona un método para mantener configuraciones de red en una ubicación centralizada. Este tema es específico de **DHCPv6**; todas las referencias a "dirección IP" se refieren a las direcciones IPv6, y todas las referencias a "**DHCP**" se refieren a **DHCPv6** (a menos que se indique lo contrario).

Un servidor **DHCPv4** puede coexistir en el mismo enlace con un servidor **DHCPv6**. Para obtener una explicación a fondo del protocolo, consulte la RFC 3315.

**DHCP** es un protocolo de capa de aplicación que permite a un máquina cliente de la red obtener direcciones IP y otros parámetros de configuración del servidor. Estos parámetros se definen en *opciones*. Las opciones se obtienen intercambiando paquetes entre un daemon en el cliente y otro en el servidor. Estos intercambios de mensajes son en formato de paquetes **UDP**. Un cliente utiliza una dirección local de enlace, a través del mandato **autoconf6** o de otros métodos, para identificar la dirección de origen en el servidor. El servidor escucha en una dirección de multidifusión de ámbito de enlace reservado. Un agente de relé permitirá al cliente y al servidor comunicarse si no están ubicados en el mismo enlace.

En este tema se explica el reconocimiento de intercambio de cuatro mensajes para una sola interfaz con un IA\_NA y una dirección para este IA\_NA. Para obtener una dirección IP, el daemon de cliente **DHCP** (**dhcpcd6**) envía un mensaje **SOLICIT** en la dirección **All\_DHCP\_Relay\_Agents\_and\_Servers**, recibido por el servidor y procesado. (Se pueden configurar varios servidores en la red para redundancia). Si una dirección libre está disponible para dicho cliente, se crea un mensaje **ADVERTISE** y se devuelve dicho mensaje al cliente. Este mensaje contiene una dirección IP y otras opciones que son apropiadas para dicho cliente. El cliente recibe el mensaje **DHCP ADVERTISE** de servidor y lo almacena mientras espera otros anuncios. Cuando el cliente ha elegido el mejor anuncio, envía un **DHCP REQUEST** a la dirección **All\_DHCP\_Relay\_Agents\_and\_Servers** que especifica qué anuncio de servidor desea.

Todos los servidores **DHCP** configurados reciben el mensaje **REQUEST**. Cada uno comprueba si es el servidor solicitado. El servidor no procesa ningún paquete con un DUID de servidor que no coincide con el propio. El servidor solicitado marca la dirección como asignada y devuelve **DHCP REPLY**, momento en el cual la transacción se ha completado. El cliente tiene una dirección durante el periodo de tiempo (**valid-lifetime**) designado por el servidor.

Cuando caduca el tiempo de vida preferido para la dirección, el cliente envía al servidor un paquete **RENEW** para ampliar el tiempo de alquiler. Si el servidor desea renovar la dirección, envía un **DHCP REPLY**. Si el cliente no obtiene una respuesta del servidor que es propietario de la dirección actual, difunde un paquete **DHCP REBIND** si, por ejemplo, el servidor se ha movido de una red a otra. Si el cliente no ha renovado la dirección después del tiempo de vida válido, se elimina la dirección de la interfaz y el proceso vuelve a empezar. Este ciclo evita que se asigne la misma dirección a varios clientes de una red.

Un cliente puede tener varias opciones IA\_NA y cada IA\_NA puede tener varias direcciones. Un cliente también puede tener varias opciones IA\_TA y cada una también puede tener varias direcciones:

- **Asociación de identidad para direcciones no temporales (IA\_NA):** Una IA que contiene direcciones asignadas que no son direcciones temporales
- **Asociación de identidad para direcciones temporales (IA\_TA):** Una IA que contiene direcciones temporales (consulte la RFC 3041).
- **DUID:** Identificador exclusivo de **DHCP** para un participante de **DHCP**; cada cliente y servidor **DHCP** tiene un DUID exclusivo que permanece igual de un rearranque a otro.

El servidor **DHCP** asigna direcciones basándose en claves. Cuatro claves comunes son **class**, **vendor**, **client ID** e **inoption**. El servidor utiliza estas claves para asignar una dirección y el conjunto de opciones de configuración a devolver al cliente.

#### **class**

La clave **class** es totalmente configurable por el cliente. Puede especificar una dirección y opciones. Esta clave se puede utilizar para indicar la función de máquina en la red o para describir cómo se agrupan las máquinas para fines administrativos. Por ejemplo, es posible que el administrador de red desee crear una clase NetBIOS que contenga opciones para clientes NetBIOS o una clase de contabilidad que represente máquinas del departamento de contabilidad que necesitan acceso a una impresora específica.

#### **vendor**

La clave **vendor** ayuda a identificar al cliente por el hardware y la plataforma de software.

### **client ID**

La clave **client ID** identifica el cliente por el DUID. El ID de cliente se especifica en el archivo `duid` del daemon **dhcpcd**. Asimismo, el servidor puede utilizar el ID de cliente para pasar opciones a un cliente específico o prohibir a un cliente determinado recibir cualquier parámetro.

### **Inoption**

La clave **inoption** identifica el cliente por la opción solicitada por el cliente.

Estas claves se pueden utilizar de forma individual o en combinaciones. Si el cliente proporciona varias claves y se pueden asignar varias direcciones, sólo se elige una y el conjunto de opciones se deriva de la clave elegida en primer lugar.

Se necesita un agente de relé para que la multidifusión inicial del cliente pueda salir de la red local. Los agentes de relé actúan como agentes de reenvío para los paquetes **DHCP**.

### **Servidor DHCPv6**

Existen tres componentes principales del servidor **DHCPv6**.

El servidor **DHCP** se ha segmentado en tres componentes principales: una base de datos, un motor de protocolo y un conjunto de hebras de servicio. Cada componente tiene su propia información de configuración.

#### **Base de datos DHCPv6**

La base de datos `db_filev6.dhcpo` se utiliza para realizar el seguimiento de clientes y direcciones y para el control de acceso.

Las opciones también se almacenan en la base de datos para recuperarlas y entregarlas a los clientes. La base de datos se implementa como un objeto cargable dinámicamente.

Si se utiliza la información en el archivo de configuración, la base de datos se prepara y se verifica la coherencia. La base de datos también contiene las agrupaciones de direcciones y opciones

El archivo de almacenamiento principal y la copia de seguridad son archivos ASCII. El formato de los archivos de almacenamiento principal de base de datos es el siguiente:

**Nota:** No edite estos archivos manualmente.

```
DB6-1.0
Client-Info {
    duid 1-0006085b68e20004ace491d3
    state 7
    authinfo {
        protocol 2
        algorithm 1
        rdm 0
        replay 1206567640
    }
    Interface 0 {
        Inoptions {
            interface-id "en1"
            policies 2
            maxopcode 16
            numiana 1
            Ianalist {
                option 3 40
                00000001000000320000005000050018deaddeadaaaaaaa00000000000000006000000064000000c8
            }
        }
        numiata 0
        Optiontable {
            option 6 10 00030004001700180237
            option 8 2 e659
            option 15 14 000369626d000373756e00026870
            option 16 18 000004d20007307831313131000369626d
        }
    }
    Ianarec {
        IAID 1
        t1 50
        t2 80
        Addrec {
            Address dead:dead:aaaa:aaaa::6
            state 3
            starttime 1087592918
        }
    }
}
```



### **(3) EXPIRED**

Indica que el cliente y la dirección están unidos, pero sólo a título informativo, de un modo similar a direcciones liberadas. Sin embargo, el estado caducado representa a clientes que dejan que caduquen los alquileres. Una dirección caducada está disponible para utilizarse y se reasigna después de que todas las direcciones libres dejen de estar disponibles y antes de que se reasignen las direcciones liberadas. Los mandatos **dadmin** y **lssrc** informan de este estado como Expired.

### **(4) RELEASED**

Indica que el cliente y la dirección están unidos sólo a título informativo. El protocolo **DHCP** sugiere que los servidores **DHCP** mantengan información sobre los clientes que han servido para futuras referencias (principalmente para intentar proporcionar la misma dirección a ese cliente al que se ha asignado esa dirección en el pasado). Este estado indica que el cliente ha liberado la dirección. La dirección está libre para que la utilicen otros clientes, si no hay otras direcciones disponibles. Los mandatos **dadmin** y **lssrc** informan de este estado como Released.

### **(5) RESERVED**

Indica que el cliente y la dirección están unidos, pero de forma flexible. El cliente ha emitido un mensaje de descubrimiento **DHCP** y el servidor **DHCP** ha respondido, pero el cliente aún no ha respondido con una petición **DHCP** de dicha dirección. Los mandatos **dadmin** y **lssrc** informan de este estado como Reserved.

### **(6) BAD**

Representa una dirección que está en uso en la red pero que el servidor **DHCP** no ha distribuido. Este estado también representa direcciones que los clientes han rechazado. Este estado no se aplica a los clientes. El mandato **dadmin** informa de este estado como Used y el mandato **lssrc** informa de este estado como Bad.

#### **Starttime**

Hora a la que se ha distribuido esta dirección, representada en segundos desde el 1 de enero de 2000.

#### **preferred-lifetime**

Número de segundos antes de que sea necesario renovar esta dirección.

#### **valid-lifetime**

Número de segundos antes de que esta dirección no sea válida y ya no se pueda utilizar.

#### **protocolo**

El protocolo de autentificación utilizado por el cliente:

##### **(1) DELAYED**

El cliente está utilizando la autentificación retardada.

##### **(2) RECONFIGURE KEY**

El cliente está utilizando la autentificación de reconfiguración de clave.

#### **algorithm**

El algoritmo de autentificación utilizado por el cliente:

##### **(1) HMAC-MD5**

El cliente está utilizando el algoritmo MD5 en clave para crear el resumen del mensaje.

#### **rdm**

El método de detección de reproducción utilizado por el cliente:

##### **(0) Contador que aumenta de forma monótona**

El cliente está utilizando un contador que aumenta de forma monótona para modificar el valor de reproducción.

#### **replay**

El valor actual del campo de reproducción.

La sintaxis para los archivos de punto de comprobación no se especifica. Si el servidor se cuelga o si tiene que cerrar el sistema y no puede realizar un cierre normal de la base de datos, el servidor puede procesar los archivos de punto de comprobación y de copia de seguridad para reconstruir una base de datos válida. Cualquier cliente no grabado en el archivo de punto de comprobación cuando el servidor se cuelga se

pierde. Actualmente, no se realizan operaciones de guardar intermitentes cuando se procesa un cliente. Los valores predeterminados son:

#### **/etc/dhcpv6/db\_file6.cr**

Operación de base de datos normal

#### **/etc/dhcpv6/db\_file6.crbk**

Copias de seguridad para la base de datos

### **Operaciones con hebra DHCP**

La última parte del servidor **DHCP** es en realidad un conjunto de operaciones que se utilizan para mantener todos los elementos en ejecución.

Dado que el servidor **DHCP** tiene hebras, estas operaciones se configuran realmente como hebras que en ocasiones realizan acciones para asegurarse de que todo está correcto.

#### **hebra main**

Esta hebra maneja señales. Por ejemplo,

- A SIGHUP (-1) produce una renovación de todas las bases de datos en el archivo de configuración.
- A SIGTERM (-15) hará que el servidor se detenga de forma ordenada.
- A SIGUSR1 (-30) hará que el servidor vuelque la base de datos de configuración

#### **hebra src**

Esta hebra maneja las peticiones de SRC (por ejemplo **startsrc**, **stopsrc**, **lssrc**, **traceson** y **refresh**).

#### **hebra dadmin**

Esta hebra intercambia información con el programa cliente **dadmin** y el servidor **DHCP**. Se puede utilizar la herramienta **dadmin** para obtener el estado así como para modificar la base de datos a fin de editar los archivos de base de datos manualmente. Con la adición de las hebras **dadmin** y **src**, el servidor puede manejar peticiones de servicio y seguir manejando peticiones de cliente.

#### **hebra garbage**

Esta hebra ejecuta temporizadores que limpian periódicamente la base de datos, guardan la base de datos, depuran los clientes que no tienen direcciones y eliminan direcciones reservadas que han estado en estado de reserva durante demasiado tiempo. Todos estos temporizadores son configurables.

#### **procesadores de paquetes**

Cada una de ellos puede manejar una petición de un cliente **DHCPv6**. El número de procesadores de paquetes necesarios depende de la carga y de la máquina. El número de éstos es configurable; el valor predeterminado es 1. El número máximo de hebras de paquete es 50.

#### **hebras de registro cronológico**

En un sistema donde se registran cantidades significativas de datos en archivos de registro cronológico, se puede incrementar el número de hebras de registro cronológico a un valor que supere el valor predeterminado (1) hasta el máximo (50).

#### **hebra de gestor de tabla**

Esta hebra asegura que el daemon **dhcpsdv6** no procese paquetes duplicados.

#### **hebras de proceso**

Estas hebras procesan los paquetes de cliente **DHCPv6**.

#### **hebra de reconfiguración**

Esta hebra gestiona la reconfiguración del cliente cuando se actualiza el servidor (con el mandato **dadmin -x 6 -i**, por ejemplo).

### **Configuración de DHCPv6**

De forma predeterminada, el servidor **DHCP** se configura leyendo el archivo **/etc/dhcpv6/dhcpsdv6.cnf**, que especifica la base de datos inicial de opciones y direcciones.

El servidor se inicia desde los mandatos de SRC. Si se pretende iniciar **dhcpsdv6** entre rearranques, añada una entrada en el archivo **/etc/rc.tcpip**.

La configuración del servidor **DHCP** es generalmente la parte más difícil de la utilización de **DHCP** en la red. En primer lugar, decida en qué redes desea tener los clientes **DHCP**. Cada subred de la red representa una agrupación de direcciones que el servidor **DHCP** debe añadir a la base de datos. Por ejemplo:

```
subnet dead:dead:aaaa:: 48 {  
    option 23 dead::beef beef:aaaa::bbbb:c aaaa:bbbb::cccc # lista nombres servidor  
    option 24 austin.ibm.com ibm.com # lista dominios  
}
```

El ejemplo anterior muestra una subred, `dead:dead:aaaa::`, con un prefijo de 48 bits. Todas las direcciones de esta subred, `dead:dead:aaaa::1` a `dead:dead:aaaa:ffff:ffff:ffff:ff7f`, están en la agrupación. Opcionalmente, se puede especificar un rango al final de la línea antes de '{' o se puede incluir una sentencia de exclusión o rango en el contenedor de subred.

Los comentarios empiezan con un # (signo de almohadilla). El servidor **DHCP** ignora el texto desde la # inicial hasta el final de la línea. El servidor utiliza cada línea de opción para indicar al cliente qué debe hacer.

Si el servidor no sabe cómo analizar una opción, utiliza los métodos predeterminados para enviar la opción al cliente. Esto también permite al servidor **DHCP** enviar opciones específicas de sitio que no están definidas por RFC, pero que determinados clientes o configuraciones de cliente pueden utilizar.

### **Archivo de configuración DHCPv6**

El archivo de configuración tiene una sección de dirección y una sección de definición de opciones. Estas secciones utilizan contenedores para incluir opciones, modificadores y, potencialmente, otros contenedores.

Un contenedor (un método para agrupar opciones) utiliza un identificador para clasificar los clientes en grupos. Los tipos de contenedor son `subnet`, `class`, `vendor`, `inoption` y `client`. Actualmente, no hay ningún contenedor genérico que pueda definir el usuario. El identificador define de forma exclusiva el cliente para que se pueda realizar el seguimiento del cliente si, por ejemplo, se mueve entre subredes. Se puede utilizar más de un tipo de contenedor para definir el acceso de cliente.

Las opciones son identificadores que se devuelven al cliente, por ejemplo dirección de DNS o nombres de dominio.

Después de seleccionar los modificadores, el siguiente elemento que se debe configurar es el registro cronológico. Los parámetros de registro cronológico se especifican en un contenedor como la base de datos, pero la palabra clave de contenedor es `logging_info`. Cuando se aprende a configurar **DHCP**, es aconsejable activar el registro cronológico al nivel más alto. También es mejor especificar la configuración de registro cronológico antes de otros datos de archivo de configuración para asegurar que los errores de configuración se registran después de que se haya inicializado el subsistema de registro cronológico. Utilice la palabra clave `logitem` para activar el nivel de registro cronológico o elimine la palabra clave `logitem` para inhabilitar un nivel de registro cronológico. Otras palabras clave del registro cronológico permiten especificar el nombre de archivo de registro cronológico, el tamaño de archivo y el número de archivos de registro cronológico en rotación.

### **Contenedores DHCPv6**

Cuando el servidor **DHCP** recibe una petición, el paquete se analiza y las claves de identificación determinan qué contenedores, opciones y direcciones se extraen.

Cada tipo de contenedor utiliza una opción diferente para identificar un cliente:

- El contenedor `subnet` utiliza el campo `hintlist` o la dirección de la interfaz de recepción para determinar a qué subred pertenece el cliente.
- El contenedor `class` utiliza el valor de la opción 15 (Identificador `OPTION_USER_CLASS`).
- El contenedor `vendor` utiliza el valor de la opción 16 (`OPTION_VENDOR_CLASS`).
- El contenedor `client` utiliza la opción 1 (`OPTION_CLIENTID`) del DUID del cliente DHCP.
- El contenedor `inoption` coincide con la opción solicitada del cliente.

Excepto para las subredes, cada contenedor permite la especificación del valor que coincide con él, incluida la coincidencia de expresiones regulares.

Hay también un contenedor implícito, el contenedor global. Las opciones y los modificadores se colocan en el contenedor global a menos que se alteren temporalmente o se rechacen. La mayoría de los contenedores se pueden poner dentro de otros contenedores lo que implica un ámbito de visibilidad. Los contenedores pueden tener o no tener asociados a ellos rangos de direcciones. Las subredes, por naturaleza, tienen rangos asociados a ellas.

Las normas básicas para los contenedores y subcontenedores son:

- Sólo los contenedores de subred son válidos a nivel global.
- No se pueden poner subredes dentro de otros contenedores, incluida la propia subred.
- Los contenedores restringidos no pueden contener contenedores regulares del mismo tipo. (Por ejemplo, un contenedor con una opción que sólo permite una clase de Contabilidad no puede incluir un contenedor con una opción que permite todas las clases que empiezan con la letra a.)
- Los contenedores de cliente restringidos no pueden tener subcontenedores.
- Los contenedores inoption no pueden tener subcontenedores

Según las normas anteriores, puede generar una jerarquía de contenedores que segmente las opciones en grupos para clientes o conjuntos de clientes específicos.

Si un cliente coincide con varios contenedores, el servidor **DHCP** pasa la petición a la base de datos y se genera una lista de contenedores. La lista se presenta en orden de profundidad y prioridad. La prioridad se define como una jerarquía implícita en los contenedores. Los contenedores estrictos tienen una prioridad más alta que los contenedores normales. Los clientes, las clases, los proveedores y las subredes se almacenan, en ese orden, y dentro del tipo de contenedor por profundidad. Esto genera una lista ordenada del más específico al menos específico. Por ejemplo:

```
Subnet 1
  --Class 1
  --Client 1
Subnet 2
  --Class 1
  ----Vendor 1
  ----Client 1
  --Client 1
```

El ejemplo muestra dos subredes, Subnet 1 y Subnet 2. Hay un nombre de clase, Class 1, un nombre de proveedor, Vendor 1 y un nombre de cliente, Client 1. Class 1 y Client 1 se definen en varios lugares. Dado que están en contenedores diferentes, los nombres pueden ser iguales pero los valores que contienen pueden ser diferentes. Si Client 1 envía un mensaje al servidor **DHCP** de Subnet 1 especificando Class 1 en la lista de opciones, el servidor **DHCP** generará la siguiente vía de acceso de contenedor:

```
Subnet 1, Class 1, Client 1
```

El contenedor más específico se lista en último lugar. Para obtener una dirección, la lista se examina en jerarquía inversa para encontrar la primera dirección disponible. A continuación, la lista se examina avanzando en la jerarquía para obtener las opciones. Las opciones alteran temporalmente los valores anteriores a menos que exista un rechazo de opción en el contenedor. Asimismo, dado que Class 1 y Client 1 están en Subnet 1, se ordenan de acuerdo con la prioridad de contenedor. Si el mismo cliente está en Subnet 2 y envía el mismo mensaje, la lista de contenedores generada es:

```
Subnet 2,
Class 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)
```

Subnet 2 se lista en primer lugar, a continuación Class 1, y Client 1 en el nivel Subnet 2 (porque esta sentencia de cliente sólo está un nivel por debajo en la jerarquía). La jerarquía implica que un cliente que coincide con la primera sentencia de cliente es menos específico que el cliente que coincide con Client 1 de Class 1 en Subnet 2.

La prioridad seleccionada por profundidad en la jerarquía no se reemplaza por la prioridad de los propios contenedores. Por ejemplo, si el mismo cliente emite el mismo mensaje y especifica un identificador de proveedor, la lista de contenedores es:

Subnet 2, Class 1, Vendor 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)

La prioridad de contenedor mejora el rendimiento de búsqueda porque sigue un concepto general según el cual los contenedores de cliente son el modo más específico de definir uno o varios clientes. El contenedor de clase contiene direcciones menos específicas que un contenedor de cliente, el contenedor de proveedor es incluso menos específico y el contenedor de subred es el menos específico.

#### *Direcciones y rangos de direcciones de DHCPv6*

Cualquier tipo de contenedor puede tener rangos de direcciones asociados; las subredes deben tener rangos de direcciones asociados.

Cada rango dentro de un contenedor debe ser un subconjunto del rango y no se debe solapar con rangos de otros contenedores. Por ejemplo, si se define una clase dentro de una subred y la clase tiene un rango, el rango debe ser un subconjunto del rango de subredes. Asimismo, el rango dentro de ese contenedor de clases no se puede solapar con ningún otro rango que esté a su nivel.

Los rangos se pueden expresar en la línea de contenedor y modificar mediante sentencias de exclusión y rango para permitir separar conjuntos de direcciones asociadas con un contenedor. Si tiene disponibles las diez direcciones superiores y las segundas diez direcciones de una subred, la subred puede especificar estas direcciones por rango en la cláusula de subred para reducir el uso de memoria y la posibilidad de colisión de direcciones con otros clientes que no están en los rangos especificados.

Cuando se ha seleccionado una dirección, cualquier contenedor subsiguiente de la lista que contiene rangos de direcciones se elimina de la lista junto con los hijos. Las opciones específicas de red de contenedores eliminados no son válidas si no se utiliza una dirección de ese contenedor.

#### *Opciones de archivo de configuración de DHCPv6*

Después de que se haya seleccionado la lista para determinar las direcciones, se genera un conjunto de operaciones para el cliente.

En este proceso de selección, las opciones se graban encima de las opciones seleccionadas anteriormente a menos que se encuentre un deny (rechazo), en cuyo caso, se elimina la opción rechazada de la lista que se está enviando al cliente. Este método permite la herencia de los contenedores padre para reducir la cantidad de datos que se deben especificar.

#### *Opciones específicas de servidor DHCPv6*

El último conjunto de parámetros a especificar son opciones específicas de servidor que permiten al usuario controlar el número de procesadores de paquete, la frecuencia con la que se ejecutan las hebras de recolección de basura, etc.

Por ejemplo, dos opciones específicas de servidor son:

##### ***reservedTime***

Indica el periodo de tiempo durante el cual permanece una dirección en estado reservado después de enviar un anuncio (ADVERTISE) al cliente **DHCP**

##### ***reservedTimeInterval***

Indica la frecuencia con la que el servidor **DHCP** examina las direcciones para ver si hay alguna que haya estado en estado reservado durante un periodo de tiempo más largo que *tiempoReservado*.

Estas opciones son útiles si tiene varios clientes que difunden de forma múltiple mensajes de solicitud (SOLICIT) y no difunden de forma múltiple el mensaje de petición (REQUEST) o el mensaje REQUEST se pierde en la red. La utilización de estos parámetros evita que las direcciones se reserven indefinidamente para un cliente que no cumple las normas.

Otra opción especialmente útil es *SaveInterval*, que indica con qué frecuencia se produce la operación de guardar.

### **Archivo /etc/dhcpv6/dhcpsdv6.cnf**

El servidor **DHCPv6** se configura editando el archivo /etc/dhcpv6/dhcpsdv6.cnf.

Las palabras clave son sensibles a las mayúsculas y minúsculas. Cuando se lista '{' , éste debe estar en la misma línea que la palabra clave. Se puede encontrar un archivo de configuración de ejemplo en /usr/samples/tcpip/dhcpv6.

A continuación se proporciona la descripción del archivo /etc/dhcpv6/dhcpsdv6.cnf. Se permiten las siguientes stanzas en este archivo:

- Registro cronológico
- Palabras clave globales
- Sentencias de contenedor no anidadas
- Sentencias de contenedor anidadas
- Opciones
- Opciones comunes

#### *Registro cronológico de DHCPv6*

Aquí se describen las palabras clave de servidor **DHCPv6** para las entradas de la stanza de registro cronológico.

No es necesario que esta stanza exista pero, si está presente, debe estar en la parte superior del archivo de configuración. Tiene el formato siguiente:

```
logging_info { opciones_registro }
```

Los valores de *opciones\_registro* pueden ser cualquiera de los siguientes:

Tabla 64. Palabras clave, valores y descripciones para entradas de la stanza de registro cronológico.		
Palabra clave	Valor	Descripción
logFileSize	núm	Especifica el tamaño del archivo de registro cronológico. El valor de núm es el tamaño máximo del archivo de registro cronológico en kilobytes. El archivo de registro cronológico se rotará cuando se alcance este tamaño. Se supone un tamaño infinito si no se especifica logFileSize.
logFileName	"nombrearchivo"	Especifica el nombre archivo de registro cronológico. El valor de nombrearchivo será el nombre del archivo de registro cronológico. La ubicación y el nombre archivo predeterminado es /var/tmp/dhcpsdv6.log.
numLogFiles	núm	Especifica el número de archivos de registro cronológico para la rotación de archivo. El valor predeterminado es 0.

*Tabla 64. Palabras clave, valores y descripciones para entradas de la stanza de registro cronológico.  
(continuación)*

Palabra clave	Valor	Descripción
logItem	tipo	<p>Especifica los tipos de registro cronológico deseado. Son válidos los siguientes tipos:</p> <p><b>SYSERR</b> Error del sistema, en la interfaz para la plataforma.</p> <p><b>OBJERR</b> Error de objeto, entre objetos del proceso.</p> <p><b>PROTERR</b> Error de protocolo, entre cliente y servidor.</p> <p><b>WARNING</b> Aviso, merece la atención del usuario.</p> <p><b>EVENT</b> Suceso producido en el proceso.</p> <p><b>ACTION</b> Acción realizada por el proceso.</p> <p><b>INFO</b> Información que puede ser útil.</p> <p><b>ACNTING</b> A quién se servía cuando.</p> <p><b>TRACE</b> Flujo de código, para depuración.</p>

*Palabras clave globales de DHCPv6*

Los valores de palabra clave descritos aquí son para las entradas de la stanza de palabra clave global.

Las palabras clave globales sólo son válidas fuera de un contenedor. Se permiten los siguientes valores:

*Tabla 65. Palabras clave, valores y descripciones para entradas de la stanza de palabras clave globales.*

Palabra clave	Valor	Descripción
UsedIpAddressExpiredInterval	num [unidades]	Especifica la frecuencia con la que las direcciones que están en estado BAD se recuperan y se vuelven a probar para ver su validez. Si no se ha establecido una unidad, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es -1.
leaseExpiredInterval	num [unidades]	Especifica la frecuencia con la que se comprueba si han caducado las direcciones que están en estado BOUND. Si la dirección ha caducado, el estado pasa a ser EXPIRED. Si no se ha establecido una unidad, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es 900 segundos.
reservedTime	num [unidades]	Especifica cuánto tiempo deben permanecer las direcciones en estado RESERVED antes de recuperar el estado FREE. Si no se ha establecido una unidad, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es -1.

Tabla 65. Palabras clave, valores y descripciones para entradas de la stanza de palabras clave globales.  
(continuación)

Palabra clave	Valor	Descripción
reservedTimeInterval	num [unidades]	Especifica la frecuencia con la que las direcciones en estado RESERVE se comprueban para ver si deben recuperar el estado FREE. Si no se ha establecido una unidad, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es 900 segundos.
saveInterval	num [unidades]	Especifica la frecuencia con la que el servidor <b>DHCP</b> debe forzar una operación de guardar las bases de datos abiertas. Para servidores muy cargados, debe ser 60 o 120 segundos. Si no se ha establecido una unidad, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es 3600 segundos.
clientpruneintv	num [unidades]	Especifica la frecuencia con la que el servidor <b>DHCP</b> hace que las bases de datos eliminen cliente que no están asociados con ninguna dirección (en estado UNKNOWN). Esto reduce el uso de memoria del servidor <b>DHCP</b> . Si no se han establecido unidades, el valor predeterminado de sistema se establece en segundos. El valor predeterminado es 3600 segundos.
numprocessthreads	num	Especifica el número de hebras de procesadores de paquetes que se deben crear. Un mínimo de uno. Cada hebra de proceso maneja un cliente. De forma predeterminada, es 30.
numpacketthreads	num	Especifica el número de hebras de paquete que se deben crear. Este mínimo es 1, pero se establece en 5 de forma predeterminada.
numloggingthreads	num	Especifica el número de hebras de registro cronológico. El valor predeterminado es 1.
numuidbuckets	num	La utiliza el gestor de tablas y tiene una correlación directa con numprocessthreads. De forma predeterminada se establece en 53.
numclientbuckets	num	Cantidad de cubetas que se utilizarán para almacenar los registros de cliente. De forma predeterminada, es 1021.
ignoreinterfacelist	interfaz [interfaz]	Lista de interfaces a ignorar. Puede ser una sola interfaz o varias interfaces.
backupfile	" <i>nombrearchiv</i> <i>o</i> "	Archivo a utilizar para las copias de seguridad de base de datos. El archivo predeterminado es /etc/dhcpv6/db_file6.crbk

Tabla 65. Palabras clave, valores y descripciones para entradas de la stanza de palabras clave globales.  
(continuación)

Palabra clave	Valor	Descripción
checkpointfile	" <i>nombrearchivo</i> "	Especifica los archivos de punto de comprobación de base de datos. El primer archivo de punto de comprobación es la vía de acceso. El segundo archivo de punto de comprobación es la vía de acceso con el último carácter sustituido por un 2. Por lo tanto, el archivo de punto de comprobación no debe terminar en 2.
clientrecorddb	" <i>nombrearchivo</i> "	Especifica el archivo para guardar la base de datos. El archivo contiene todos los registros de cliente que el servidor <b>DHCP</b> ha atendido. El archivo predeterminado <b>/etc/dhcpv6/db_file6.cr</b>
duid	<code>idtype <i>valor</i> [<i>valor</i>]</code>	Se utiliza para identificar el usuario. Se permiten los siguientes valores: <ul style="list-style-type: none"> <li>• <code>duid 1 <i>interfaz</i></code></li> <li>• <code>duid 2 <i>interfaz</i></code></li> <li>• <code>duid 3 enterprise number <i>identificador</i></code></li> <li>• <code>duid number <i>0xdigitohex</i></code></li> </ul>
preference-number	num	Permite a los clientes identificar el servidor del que prefieren obtener información. Cuanto más alto sea el valor, mayores serán las posibilidades de que el cliente utilice este servidor para los servicios. El valor predeterminado y máximo es 255.
unicast-enable	<i>política</i>	Política de difusión individual para el servidor. Esto permite al servidor comunicarse utilizando la difusión individual. De forma predeterminada, está activada.
tablemgr-policy	<i>política</i>	Permite al servidor tener un gestor de tablas para gestionar mejor los clientes de entrada. De forma predeterminada, está activada.
auth	<i>política</i>	Permite al servidor admitir la autenticación retardada. De forma predeterminada, está desactivada.
auth-keyfile	" <i>nombrearchivo</i> "	El archivo que contiene las claves de autenticación retardada para los clientes. El archivo predeterminado es <b>/etc/dhcpv6/dhcpsdv6.keys</b> .

#### Sentencias de contenedor no anidadas de DHCPv6

La palabra clave de servidor **DHCPv6** subred es para las entradas de las sentencias de contenedor no anidadas.

Las sentencias de contenedor no anidadas sólo pueden existir como parte de las palabras claves globales.

Tabla 66. Palabras clave, valores y descripciones para entradas de las sentencias de contenedor no anidadas.

Item	Descripción	
subnet	<i>idsubred longitud-prefijo [rango] {OPTIONS}</i>	Especifica la subred a utilizar. El <i>idsubred</i> debe ser una dirección IPv6. La <i>longitud-prefijo</i> debe ser un entero positivo menor que 128.

#### Sentencias de contenedor anidadas de DHCPv6

Las sentencias de contenedor anidadas sólo pueden existir como una opción dentro de la subred.

Todos los contenedores pueden tener otros contenedores anidados en ellos a menos que se indique lo contrario. La profundidad máxima de anidamiento es siete, incluida la subred y el contenedor global (sólo pueden existir cinco contenedores anidados bajo un contenedor de subred).

Los contenedores de proveedor e Inoption no pueden tener otros contenedores anidados.

Tabla 67. Palabras clave, valores y descripciones para entradas de las sentencias de contenedor anidado.

Palabra clave	Valor	Descripción
class	<i>nombre [rango] {OPTIONS COMMON OPTIONS }</i>	Contenedor de clase. El valor de <i>nombre</i> es una serie, series separadas por espacio, una expresión regular, hex Oxdígitohex, Oxdígitohex
vendor	<i>nombre [rango] {OPTIONS COMMON OPTIONS }</i>	Contenedor de proveedor. El valor de <i>nombre</i> es una serie, series separadas por espacio, una expresión regular, hex Oxdígitohex, Oxdígitohex
client	<i>&lt;id   0 Oxhexdigit   regular expression&gt; &lt;ip   rango   none   any&gt; {OPTIONA COMMON OPTIONS }</i>	Contenedor de cliente. <i>id</i> - 1-hexdigit, 2-hexdigit, 3-hexdigit <ip rango none any> - Dirección IP que se debe dar a los clientes que coinciden con el ID
inoption	<i>código_entrada clave_a_comparar [rango] { OPTIONS COMMON OPTIONS }</i>	Contenedor de Inoption <i>código_entrada</i> - código o número de opción de entrada que el cliente debe especificar <i>clave_a_comparar</i> - Los datos de opción con los que se debe realizar la comparación.

#### Opciones de archivo cnf de DHCPv6

Las opciones de archivo cnf descritas aquí para **DHCPv6** sólo pueden existir en un contenedor.

Tabla 68. Palabras clave, valores y descripciones para entradas de la stanza de opciones.

Palabra clave	Valor	Descripción
exclude	<i>range</i>	Rango IP a excluir del rango actual, normalmente utilizado cuando no se especifica un rango como parte de la sentencia de contenedor
exclude	<i>ip</i>	Dirección IP a excluir del rango actual
range	<i>range</i>	Uso de rango de IP para ampliar el rango actual, normalmente utilizado cuando no se especifica un rango como parte de la sentencia de contenedor

Tabla 68. Palabras clave, valores y descripciones para entradas de la stanza de opciones. (continuación)

Palabra clave	Valor	Descripción
range	ip	Dirección IP a añadir, utilizado para ampliar el rango
stealfromchildren	policy	Obtener dirección de los contenedores hijo si se han agotado todas las direcciones. De forma predeterminada, está desactivada.
stealfrompeer	policy	Obtener direcciones de los contenedores iguales si se han agotado todas las direcciones. De forma predeterminada, está desactivada.
stealfromparent	policy	Obtener direcciones de los contenedores padre si se han agotado todas las direcciones. De forma predeterminada, está desactivada.
balance-option	{ balance-policy   <option   option option ...> }	Contenedor de opciones de equilibrio, las opciones especificadas en este contenedor se darán al cliente basándose en la política. Esta palabra clave sólo puede existir bajo el contenedor de subred.
balance-policy	b_policy	El valor b_policy puede ser fill o rotate. El valor predeterminado es rotate.
fill-count	num	Número de veces que se acabará una opción antes de tomar la siguiente instancia de la misma opción
interface-id	"interfaz"	Sólo se puede listar bajo la subred. Se permitirá que las peticiones de clientes recibidas en esta interfaz obtengan direcciones.

#### Opciones comunes de DHCPv6

Estas palabras clave son opciones comunes de **DHCPv6**.

Pueden existir en los contenedores o en la sección global:

Tabla 69. Palabras clave, valores y descripciones de opciones comunes.

Palabra clave	Valor	Descripción
reconfig-policy	policy	Permite al servidor enviar el mensaje de reconfiguración al cliente. De forma predeterminada, no está establecida y se considera desactivada.
rapid-commit	policy	Permite al servidor realizar una confirmación rápida para el contenedor o establecerla globalmente. De forma predeterminada, no está establecida y se considera desactivada.
preferred-lifetime	num [unidades]	Tiempo de vida preferido de IANA o IATA. El valor predeterminado es 43200 segundos.
valid-lifetime	num [unidades]	Tiempo de vida válido de IANA o IATA. El valor predeterminado es 86400 segundos.
rebind	num	Porcentaje de tiempo de revinculación de 0 a 100 para la dirección. El valor predeterminado es 80 porcentaje.

Tabla 69. Palabras clave, valores y descripciones de opciones comunes. (continuación)

Palabra clave	Valor	Descripción
renew	num	El porcentaje de tiempo de renovación de 0 a 100 para la dirección. El valor predeterminado es de 50 por ciento.
unicast-option	policy	Permite a los contenedores ofrecer el intercambio de mensajes mediante la difusión individual. Se puede utilizar para activar y desactivar contenedores individuales y subredes incluso si la política de servidor difiere. De forma predeterminada, no está establecida y se considera desactivada.
option	num <string  strings  hex>	Para la lista de opciones, consulte el apartado “Opciones conocidas de archivo de servidor DHCPv6” en la página 336.
change-optiontable	optiontable	Sólo permitido en un contenedor de proveedor.

#### Opciones conocidas de archivo de servidor DHCPv6

Aquí se describen las opciones de archivo conocidas del servidor **DHCPv6**.

Las opciones siguientes son las opciones conocidas del archivo de servidor **DHCPv6**. Las opciones que tienen "No" en la columna **Se puede especificar** no se pueden especificar en el archivo de configuración; si se especifican, se ignorarán.

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
1	Ninguno	No	Solicitud
2	Ninguno	No	Anuncio
3	Ninguno	No	Petición
4	Ninguno	No	Confirmación
5	Ninguno	No	Address
6	Ninguno	No	Petición de opción
7	number	No	Número de preferencia del servidor
8	Ninguno	No	Tiempo transcurrido
9	Ninguno	No	Mensaje de relé
11	Ninguno	No	Autorización
12	Serie ASCII yes, no, true, false	Sí	Difusión individual
13	Ninguno	No	Estado
14	Serie ASCII yes, no, true, false	Sí	Confirmación rápida
15	Ninguno	No	Clase de usuario
16	Ninguno	No	Clase de proveedor
17	Ninguno	No	Opción de proveedor

Número de opción	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
18	Ninguno	No	Id de interfaz
19	Ninguno	No	Mensaje de reconfiguración
20	Serie ASCII yes, no, true, false	Sí	Aceptación de reconfiguración
23	Direcciones IPv6 separadas por espacio	Sí	Servidores DNS
24	Serie ASCII	Sí	Lista de dominios

*Valores de parámetros de DHCPv6*

Se pueden utilizar estos valores para los parámetros de **DHCPv6**.

*unidades*: segundos, segundos, minuto, minutos, hora, horas, día, días, semana, semanas, mes, meses, año, años

*interfaz*: en0, en1, tr0

*identificador*: números o caracteres

*política*: yes, no, true, false

*rango*: ipv6addressss-ipv6addressss

*expresión regular*: "!expression to match\$", "!expression to match^"

*Archivo /etc/dhcpv6/dhcpsdv6.cnf de ejemplo*

El archivo /etc/dhcpv6/dhypsdv6.cnf de ejemplo mostrado aquí proporciona una visión breve del contenido del archivo.

```

logging_info{
    logFileSize 4000
    logItem      SYSERR
    logItem      PROTERR
    logItem      WARNING
    logItem      EVENT
    logItem      ACTION
    logItem      INFO
    logItem      ACNTING
    logItem      TRACE
    numLogFile 3
    logFileName "/var/tmp/dhypsdv6.log"
}
duid 1 en0
numprocesssthreads 10
numpacketthreads 5
preference-number 255
reconfig-policy no
rapid-commit no
unicast-option yes
leaseExpiredInterval 3000 seconds
unicast-enable yes
saveInterval 60 seconds
reservedTimeInterval 8000 seconds
reservedTime 10000 seconds
clientpruneintv 20 seconds

subnet bbbb:aaaa:: 40 bbbb:aaaa::0004-bbbb:aaaa::000f {
    balance-option {
        option 23 dead::beef
        option 23 beef::aaaa
        option 24 yahoo.com
    }
}

subnet dead:dead:aaaa:: 48 dead:dead:aaaa:aaaa::0006-dead:dead:aaaa:aaaa::000a {
    interface-id "en1"
    preferred-lifetime 100 seconds
}

```

```

valid-lifetime      200 seconds
rapid-commit yes
option 23 dead::beef beef:aaaa::bbbb:c aaaa:bbbb::cccc
option 24 ibm.com austin.ibm.com
}

```

### Configuración de cliente DHCPv6

Se utiliza el archivo /etc/dhcpv6/dhcpc6.cnf para configurar los clientes **DHCPv6**.

Aquí se incluyen las directivas que se pueden especificar en este archivo. Si se pretende iniciar **dhcpcd6** entre rearranques, añada una entrada en el archivo /etc/rc.tcpip.

#### *Palabras clave de registro*

Aquí se describen las palabras clave de registro cronológico válidas del servidor **DHCPv6**.

Son válidas las siguientes palabras clave:

*Tabla 70. Palabras clave y descripciones para palabras clave de registro cronológico.*

Palabra clave	Descripción
log-file-name	Vía de acceso y nombre del archivo de registro cronológico más reciente. En los nombres de archivo menos recientes se añade el número 1 a (n-1); cuanto mayor es el número, menos reciente es el archivo.
log-file-size	Especifica el tamaño máximo de un archivo de registro cronológico en KB. Cuando el tamaño del archivo de registro cronológico más reciente alcanza este valor, se redenomina el archivo y se crea un archivo nuevo.
log-file-num	Especifica el número máximo de archivos de registro cronológico mantenidos cuando el tamaño del archivo de registro cronológico más reciente alcanza el valor log-file-size y se redenomina el valor para generar un archivo nuevo.

Tabla 70. Palabras clave y descripciones para palabras clave de registro cronológico. (continuación)

Palabra clave	Descripción
log-item	Especifica los elementos de registro cronológico que es necesario registrar. <b>SYSERR</b> Error de sistema <b>OBJERR</b> Error de objeto <b>PROTERR</b> Error de protocolo <b>WARNING</b> Aviso <b>EVENT</b> Suceso producido <b>ACTION</b> Acción realizada por el proceso <b>INFO</b> Información adicional <b>ACNTING</b> A quién se servía cuando <b>TRACE</b> Flujo de código, depuración

#### Palabras clave de DUID

Los valores de palabra clave siguientes son para las entradas de DUID.

El formato de las entradas de DUID es el siguiente:

```
duid <tipo_duid> <valor> <valor> ...
```

El tipo de DUID puede ser una palabra clave o un número, dejando espacio para cualquier tipo de DUID que se pueda definir en el futuro. Actualmente la RFC 3315 define tres tipos de DUID:

Tabla 71. Palabras clave y valores de las entradas de DUID.

Palabra clave	Descripción
LLT	Tipo DUID-LLT (valor 1)
LL	DUID-LL (valor 2)
EN	Tipo DUID-EN (valor 3)

El formato específico de las entradas DUID depende de la palabra clave que se utiliza.

```
duid LLT      <nombre interfaz>
duid LL       <nombre interfaz>
duid EN       <número empresa> <identificador empresa>
duid <número> <datos hexadecimales (con el prefijo '0x')>
```

#### Palabra clave sólo de información

La palabra clave sólo de información está en el formato `info-only nombre interfaz`.

A continuación se proporciona la palabra clave sólo de información:

Tabla 72. Palabra clave y descripción de la palabra clave sólo de información.

Palabra clave	Descripción
info-only nombre interfaz	Esta palabra clave especifica el nombre de interfaz para el que el cliente tiene que obtener sólo información de configuración y no direcciones del servidor.

#### Palabras clave de renovación de alquiler y revinculación

Las palabras clave de renovación de alquiler y revinculación descritas aquí son para el servidor **DHCPv6**.

Tabla 73. Palabras clave y descripciones para renovación de alquiler y revinculación

Palabras clave	Descripción
rebind-time valor	En el caso de que el cliente no pueda renovar el alquiler (porque el servidor no responde), la hora de revinculación (rebind-time) especifica la hora a la que el cliente se pone en contacto con los demás servidores para revincular el alquiler.
renew-time valor	La hora de renovación (renew-time) especifica la hora a la que el cliente se pone en contacto con el servidor del que el cliente ha obtenido información de alquiler, para renovar el alquiler.

#### Palabras clave de solicitud de retransmisión

Las palabras clave de solicitud de retransmisión incluyen **solicit-maxcount** y **solicit-timeout**.

Tabla 74. Palabras clave y descripciones para palabras clave de solicitud de retransmisión

Palabras clave	Descripciones
solicit-maxcount	La palabra clave solicit-maxcount especifica el número de mensajes de solicitud que el cliente envía al servidor antes de que el cliente reciba una respuesta del servidor.
solicit-timeout	La palabra clave solicit-timeout especifica el tiempo hasta que el cliente intenta enviar un mensaje de solicitud al servidor antes de que el cliente reciba una respuesta desde el servidor.

#### Palabras clave de opción

Si las palabras clave de opción aparecen fuera de las stanzas de 'interfaz', se consideran globales. Tales opciones se aplican a todas las interfaces. Si las palabras clave de opción aparecen en las stanzas de 'interfaz', estas opciones se aplican sólo a dicha interfaz.

La stanza de opciones sigue este formato:

```
option <palabra clave | código opción>
option <palabra clave | código opción> exec "exec string"
option <palabra clave | código opción> { parámetros específicos de opción }
option <palabra clave | código opción> { parámetros específicos de opción } exec "exec string"
```

Se puede especificar un código de opción utilizando el código de opción registrado IANA. Sin embargo, algunas de las opciones también se pueden especificar utilizando las palabras clave mostradas más abajo:

Palabra clave	Código de opción
ia-na	3

Palabra clave	Código de opción
ia-ta	4
request-option	6
rapid-commit	14
user-class	15
vendor-class	16
vendor-opts	17
reconf-accept	20
dns-servers	23
domain-list	24

A continuación se proporciona una explicación adicional de cada palabra clave:

Palabra clave	Finalidad, formato y parámetros
ia-na	<p><b>Finalidad</b> Especifica la opción 3. Si se especifica, el cliente solicita direcciones no temporales del servidor.</p> <p><b>Formato</b> option ia-na [ { parámetros } ] [ exec "exec string" ]</p> <p><b>Parámetros</b> La opción ia-na toma los parámetros siguientes:</p> <pre>ia-id      valor renew-time  valor rebind-time valor</pre> <p>Estos parámetros especifican los valores preferidos del usuario y son opcionales. El <i>valor</i> especificado puede ser un número decimal o un número hexadecimal con el prefijo '0x'</p>
ia-ta	<p><b>Finalidad</b> Especifica la opción 4. Si se especifica, el cliente solicita direcciones temporales del servidor.</p> <p><b>Formato</b> option ia-ta [ { parámetros } ] [ exec "exec string" ]</p> <p><b>Parámetros</b> La opción ia-ta toma los parámetros siguientes:</p> <pre>ia-id      valor</pre> <p>Este parámetro especifica los valores preferidos del usuario y es opcional. El <i>valor</i> especificado puede ser un número decimal o un número hexadecimal con el prefijo '0x'</p>

Palabra clave	Finalidad, formato y parámetros
request-option	<p><b>Finalidad</b> Especifica la opción 6. Si se especifica, el cliente solicita una lista de opciones del servidor.</p> <p><b>Formato</b> <code>option request-option { parámetros } [ exec "exec string" ]</code></p> <p><b>Parámetros</b> option request-option toma una lista separada por espacios de códigos de opción (en decimal) como argumento</p>
rapid-commit	<p><b>Finalidad</b> Especifica la opción 14. Si se especifica, el cliente indica que está preparado para realizar el intercambio de mensajes de solicitud y respuesta.</p> <p><b>Formato</b> <code>option rapid-commit [exec "exec string"]</code></p> <p><b>Parámetros</b> No toma ningún parámetro distinto de la sentencia exec opcional</p>
user-class	<p><b>Finalidad</b> Especifica la opción 15. Si se especifica, el cliente indica el tipo o la categoría del usuario o de las aplicaciones que representa.</p> <p><b>Formato</b> <code>option user-class { parámetros } [ exec "exec string" ]</code></p> <p><b>Parámetros</b> La opción user-class toma una o varias instancias de los datos de clase de usuario. Cada instancia de datos de clase de usuario es una serie entre comillas o sin comillas de longitud arbitraria. Si una serie contiene un espacio en blanco, se debe escribir entre comillas. Los parámetros son necesarios. El formato del parámetro es:  <code>class valor class valor</code> donde <i>valor</i> es una serie entre comillas o sin comillas.</p>
vendor-class	<p><b>Finalidad</b> Especifica la opción 16. Si se especifica, el cliente indica el proveedor que ha fabricado el hardware en el que se ejecuta el cliente.</p> <p><b>Formato</b> <code>option vendor-class { parámetros } [ exec "exec string" ]</code></p> <p><b>Parámetros</b> La opción vendor-class toma el número de empresa registrado del proveedor y una o varias instancias de datos de clase de proveedor. Cada instancia de datos de clase de proveedor es una serie entre comillas o sin comillas de longitud arbitraria, cada una de las cuales describe alguna característica de la configuración de hardware del cliente. Los parámetros <i>no</i> son opcionales. El formato es:  <code>vendor-id valor class valor class valor</code> donde <i>valor</i> es una serie entre comillas o sin comillas.</p>

Palabra clave	Finalidad, formato y parámetros
vendor-opts	<p><b>Finalidad</b> Especifica la opción 17. Si se especifica, el cliente indica la información específica del proveedor al servidor.</p> <p><b>Formato</b> <code>option vendor-opts &lt;número-empresa&gt; { parámetros } [ exec "exec string" ]</code></p> <p><b>Parámetros</b> La opción <code>vendor-opts</code> toma el número de empresa registrado del proveedor y una o varias instancias de datos de opción de proveedor. Cada instancia de datos de opción de proveedor es un código de opción de proveedor seguido de datos de opción en formato de serie o hexadecimal. Los parámetros <i>no</i> son opcionales. El formato es:</p> <pre>vendor-id valor option códigoop datos-opción option códigoop datos-opción</pre> <p>donde <i>datos-opción</i> es una serie entre comillas, sin comillas o hexadecimal (con el prefijo '0x')</p>
reconf-accept	<p><b>Finalidad</b> Especifica la opción 20. Si se especifica, el cliente indica al servidor si el cliente está dispuesto a aceptar reconfigurar el mensaje del servidor.</p> <p><b>Formato</b> <code>option reconf-accept [ { exec "exec string" } ]</code></p> <p><b>Parámetros</b> La opción <code>reconf-accept</code> no toma ningún parámetro específico de opción, excepto la sentencia <code>exec</code>.</p>
dns-servers	<p><b>Finalidad</b> Especifica la opción 23. Si se especifica, el cliente indica al servidor el conjunto preferido de servidores DNS.</p> <p><b>Formato</b> <code>option dns-servers [ { parámetros } ] [ exec "exec string" ]</code></p> <p><b>Parámetros</b> La opción <code>dns-servers</code> toma como argumento una lista separada por espacio/línea de direcciones de IPv6.</p>
domain-list	<p><b>Finalidad</b> Especifica la opción 24. Si se especifica, el cliente indica la lista de dominios preferida.</p> <p><b>Formato</b> <code>option domain-list [ { parámetros } ] [ exec "exec string" ]</code></p> <p><b>Parámetros</b> La opción <code>domain-list</code> toma una lista separada por espacio/línea de series de nombres de dominio.</p>

#### Palabras clave de interfaz

La palabra clave de interfaz está en el formato `interface <nombre_interfaz> [ { option declaration/s } ]`.

Tabla 75. Palabra clave y descripción de las palabras clave de interfaz.

Palabras clave	Descripciones
interface <nombre interfaz> [ { option declaration/s } ]	La sentencia interface toma una o varias declaraciones de opción como argumentos. Estas opciones, especificadas en la stanza de interfaz son específicas de esta interfaz, a diferencias de las opciones declaradas fuera de la stanza de interfaz, que se aplican a todas las interfaces.

```
interface en1 {
    option ia-na {
        ia-id      01
        renew-time 0x40
        rebind-time 0x60
    }

    option request-option { 3 23 24 }

    option user-class {
        class ibm
        class "userclassA and B"
        class "userclassB"
    }

    option vendor-class {
        vendor-id 1234
        class "vendorclassA"
        class "vendorclassB"
    }

    option vendor-opts {
        vendor-id 2343
        option 89      vendoroption89
        option 90      vendoroption90
    }

    option reconf-accept
```

### Agente de relé DHCP

El archivo /etc/dhcpd.cnf es el archivo de configuración para el agente de relé **DHCP** y **BOOTP**. Aquí se explica el formato del archivo y las directivas y las palabras clave permitidas.

Las directivas se especifican en el formato siguiente:

```
<palabraclave> <valor1> ... <valorN>
```

El agente de relé que se inicia y se reinicia utiliza la presencia y los valores de estos parámetros.

Este conjunto de parámetros especifica los archivos de registro cronológico que mantendrá el servidor. Cada parámetro se identifica por una palabra clave que va seguida por el valor.

<b>Palabra clave</b>	<b>Valor</b>	<b>Definición</b>
numLogFiles	0 a $n$	Número de archivos de registro cronológico. Si se especifica 0, no se mantendrá ningún archivo de registro cronológico y no se visualizará ningún mensaje de registro cronológico en ningún lugar. $n$ es el número máximo de archivos de registro cronológico mantenidos mientras el tamaño del archivo de registro cronológico más reciente alcanza su tamaño máximo y se crea un nuevo archivo de registro cronológico.
logFileSize	En KB	Tamaño máximo de un archivo de registro de cronológico. Cuando el tamaño del archivo de registro cronológico más reciente alcanza este valor, éste se redenomina y se crea un nuevo archivo de registro cronológico.
logFileName	vía de acceso de archivo	Nombre del archivo de registro cronológico más reciente. En los archivos de registro cronológico más recientes se añade el número 1 a $(n - 1)$ a los nombres; cuanto mayor es el número, menos reciente es el archivo.

Palabra clave	Valor	Definición
logItem	Un elemento que se registrará.	<p><b>SYSERR</b> Error del sistema, en la interfaz para la plataforma.</p> <p><b>OBJERR</b> Error de objeto, entre objetos del proceso.</p> <p><b>PROTERR</b> Error de protocolo, entre cliente y servidor.</p> <p><b>WARNING</b> Aviso, merece la atención del usuario.</p> <p><b>EVENT</b> Suceso producido en el proceso.</p> <p><b>ACTION</b> Acción realizada por el proceso.</p> <p><b>INFO</b> Información que puede ser útil.</p> <p><b>ACNTING</b> A quién se servía cuando.</p> <p><b>TRACE</b> Flujo de código, para depuración.</p>

Por ejemplo, un archivo `/etc/dhcprd.cnf` puede tener las entradas siguientes:

```

numLogFile 4
logFileSize 1000
logFileName /usr/tmp/dhcprd.log
logItem SYSERR
logItem OBJERR
logItem PROTERR
logItem WARNING
logItem EVENT
logItem ACTION
logItem INFO
logItem ACNTING
logItem TRACE

```

Palabra clave	Valor	Definición
relay	IPv4, IPv6 o ALL	Especifica la modalidad del relé de paquete. Si se especifica IPv4, el agente de relé actúa sólo como agente de relé <b>DHCPv4</b> . Ésta es la modalidad predeterminada del agente de relé. Si se especifica IPv6, el agente de relé actúa sólo como agente de relé <b>DHCPv6</b> . Si se especifica ALL, el agente de relé actúa como agente de relé <b>DHCPv4</b> y <b>DHCPv6</b> .
server	Dirección IP	Especifica la dirección IP de un servidor <b>BOOTP</b> o <b>DHCP</b> . El paquete se reenviará a los servidores listados en este archivo.
server6	Dirección IPv6	Especifica la dirección IPv6 del servidor <b>DHCPv6</b> . El paquete se reenviará a los servidores listados aquí.
option6	<código de opción> <datos de opción>	Especifica las opciones de agente de relé de <b>DHCPv6</b> . La palabra clave sólo es válida si la modalidad de relé se establece en IPv6. El valor de <i>código de opción</i> se especifica como un número decimal. El valor de <i>datos de opción</i> se especifica como una serie entre comillas o sin comillas o en formato hexadecimal (con el prefijo 0x)
single-site		Especifica que el dispositivo en el que se ejecuta el agente de relé pertenece a un solo sitio.

### Daemon DHCP de proxy de entorno de ejecución previa al arranque

El servidor **DHCP** de proxy PXE se comporta de manera muy parecida a un servidor **DHCP** escuchando el tráfico de cliente **DHCP** normal y respondiendo a determinadas peticiones de cliente. Sin embargo, a diferencia del servidor **DHCP**, el servidor **DHCP** de proxy PXE no administra direcciones de red y sólo responde a clientes que se identifican como clientes PXE.

Las respuestas proporcionadas por el servidor **DHCP** de proxy PXE contienen el mecanismo mediante el cual el cliente localiza los servidores de arranque o las direcciones de red y las descripciones de los servidores de arranque compatibles soportados.

La utilización de un servidor **DHCP** de proxy PXE además de un servidor **DHCP** proporciona tres características clave. En primer lugar, puede separar la administración de las direcciones de red de la administración de las imágenes de arranque. Mediante la utilización de dos procesos diferentes en el mismo sistema, puede configurar la información de arranque gestionada por el servidor **DHCP** de proxy PXE sin alterar o necesitar el acceso a la configuración de servidor **DHCP**. En segundo lugar, puede definir

varios servidores de arranque y permitir al cliente PXE seleccionar un servidor determinado durante el arranque. Por ejemplo, cada servidor de arranque puede ofrecer un tipo diferente de sistema operativo o de configuración de sistema. Finalmente, la utilización del servidor proxy ofrece la posibilidad de configurar el cliente PXE para que utilice el direccionamiento IP de multidifusión para descubrir la ubicación de los servidores de arranque compatibles.

El servidor **DHCP** de proxy PXE se puede configurar para que se ejecute en el mismo sistema que está ejecutando el servidor **DHCP** o en un sistema diferente. Asimismo, se puede configurar para que se ejecute en el mismo sistema que también está ejecutando el daemon de servidor de arranque o en un sistema diferente.

### **Componentes de servidor DHCP de proxy PXE**

Existen tres componentes del servidor PXED.

El servidor PXED se segmenta en tres partes principales, una base de datos, un motor de protocolo y un conjunto de hebras de servicio, cada una con su propia información de configuración.

#### **Base de datos PXED**

La base de datos db\_file.dhcpo se utiliza para generar las opciones que se deben enviar al cliente cuando el cliente envía un paquete REQUEST.

Las opciones devueltas por la base de datos dependen del tipo de servidor elegido. Esto se establece utilizando la palabra clave pxeservertype en el archivo pxed.cnf.

Si se utiliza la información en el archivo de configuración, la base de datos se prepara y se verifica la coherencia.

#### **Motor de protocolo PXED**

El motor de protocolo utiliza la base de datos para determinar qué información se debe devolver al cliente.

El motor de protocolo PXED se basa en Intel Preboot Execution Environment (PXE) Specification Versión 2.1 y sigue siendo compatible con Intel PXE Specification Versión 1.1.

#### **Operaciones con hebra PXED**

La última parte del servidor PXED es en realidad un conjunto de operaciones que se utilizan para mantener todos los elementos en ejecución. Dado que el servidor PXED tiene hebras, estas operaciones se configuran realmente como hebras que en ocasiones realizan acciones para asegurarse de que todo está correcto.

La primera hebra, la hebra *main*, maneja las peticiones SRC (por ejemplo **startsrc**, **stopsrc**, **lssrc**, **traceson** y **refresh**). Esta hebra también coordina todas las operaciones que afectan a todas las hebras y maneja las señales. Por ejemplo,

- A SIGHUP (-1) produce una renovación de todas las bases de datos en el archivo de configuración.
- A SIGTERM (-15) hace que el servidor se detenga de forma ordenada.

La otra hebra procesa paquetes. En función del tipo de servidor, puede haber una o dos hebras. Una hebra escucha en el puerto 67 y la segunda escucha en el puerto 4011. Cada una de ellas puede manejar una petición de un cliente.

#### **Configuración de servidor PXED**

De forma predeterminada, el servidor PXED se configura leyendo el archivo /etc/pxed.cnf, que especifica la base de datos de opciones y direcciones inicial del servidor.

El servidor se inicia desde SMIT o mediante mandatos de SRC.

La configuración del servidor PXED es generalmente la parte más difícil de la utilización de PXED en la red. En primer lugar, determine qué redes necesita que tengan clientes PXE. El ejemplo siguiente configura el daemon **pxed** para que se ejecute en la misma máquina que el servidor DHCP:

```
pxeservertype proxy_on_dhcp_server
subnet default
```

```

{
    vendor pxe
    {
        option   6      2      "# Inhabilitar descubrimiento de servidor de
                                # arranque multidifusión
        option   8      1      2      9.3.4.5  9.3.4.6  2      1      9.3.149.29
                                # La opción anterior proporciona la lista de
                                # servidores de arranque
        option   9      0      "Servidor de rutina de carga PXE" \
                                1
                                2      "Servidor de arranque de Microsoft Windows NT" \
                                "Servidor de arranque DOS/UNDI"
        option   10     20     "segundos restantes antes de que se selecciona
                                automáticamente el primer elemento del menú
                                de arranque"
    }
}

```

Las subopciones del contenedor de proveedor sólo se envían a los clientes PXE si la dirección IP del cliente está en el rango de direcciones IP de la subred (por ejemplo 9.3.149.0 a 9.3.149.255).

El ejemplo siguiente configura el daemon **pxed** para que se ejecute en una máquina diferente del servidor **DHCP**:

```

subnet default
{
    vendor pxe
    {
        option   6      10     "# El nombre del archivo de arranque está
                                # presente en el paquete de oferta pxed
                                # inicial del cliente.
        option   8      1      2      9.3.4.5  9.3.4.6  2      1      9.3.149.29
                                # La opción anterior proporciona la lista de
                                # servidores de arranque
        option   9      0      "Servidor de rutina de carga PXE" \
                                1
                                2      "Servidor de arranque de Microsoft Windows NT" \
                                "Servidor de arranque DOS/UNDI"
        option   10     20     "segundos restantes antes de que se selecciona
                                automáticamente el primer elemento del menú
                                de arranque"
        bootstrapserver 9.3.148.65
        pxebootfile     1      2      1      window.one
        pxebootfile     2      2      1      linux.one
        pxebootfile     1      2      1      hello.one
        client 6 10005a8ad14d any
        {
            pxebootfile     1      2      1      aix.one
            pxebootfile     2      2      1      window.one
        }
    }

    Vendor pxeserver
    {
        option     7      224.234.202.202
    }
}

```

La palabra clave **pxeservertype** no se establece en el archivo de configuración para que se tome el valor predeterminado, que es **pdhcp\_only**, lo que significa que el servidor PXED se ejecuta en una máquina diferente del servidor **DHCP**. Dada esta configuración, el servidor PXED escucha en dos puertos (67 y 4011) los paquetes BINLD REQUEST/INFORM de los clientes. La opción 7 se envía al servidor BINLD cuando el servidor PXED recibe un paquete REQUEST/INFORM en el puerto 67 de BINLD y la opción 60 está establecida en el servidor PXED.

La cláusula de base de datos **db\_file** indica qué método de base de datos se debe utilizar para procesar esta parte del archivo de configuración. Los comentarios empiezan con un signo de almohadilla (#). El servidor PXED ignora el texto desde la # hasta el final de la línea. El servidor utiliza cada línea **option** para indicar al cliente qué debe hacer. ["Subopciones de contenedor de proveedor PXE"](#) en la página 352 describe las opciones conocidas y soportadas actualmente. Consulte el apartado ["Sintaxis de archivo de servidor PXED para la operación de servidor general"](#) en la página 355 si desea conocer procedimientos para especificar opciones que el servidor no conoce.

## **Archivo de configuración de PXED**

El archivo de configuración tiene una sección de dirección y una sección de definición de opciones, que se basan en el concepto de contenedores que contienen opciones, modificadores y, potencialmente, otros contenedores.

Un *contenedor* (básicamente, un método para agrupar opciones) utiliza un identificador para clasificar los clientes en grupos. Los tipos de contenedor son subred, clase, proveedor y cliente. Actualmente, no hay ningún contenedor genérico que pueda definir el usuario. El identificador define de forma exclusiva el cliente para que se pueda realizar el seguimiento del cliente si, por ejemplo, se mueve entre subredes. Se puede utilizar más de un tipo de contenedor para definir el acceso de cliente.

Las *opciones* son identificadores que se devuelven al cliente, por ejemplo dirección de DNS y pasarela predeterminada.

### *Contenedores PXED*

Cuando el servidor **DHCP** recibe una petición, el paquete se analiza y las claves de identificación determinan qué contenedores, opciones y direcciones se extraen.

El ejemplo de configuración de servidor PXED muestra un contenedor de subred. La clave de identificación es la posición del cliente en la red. Si el cliente es de esa red, se clasifica en ese contenedor.

Cada tipo de contenedor utiliza una opción diferente para identificar un cliente:

- El contenedor de subred utiliza el campo **giaddr** o la dirección de la interfaz de recepción para determinar de qué subred procede el cliente.
- El contenedor de clase utiliza el valor de la opción 77 (Identificador de clase de sitio de usuario).
- El proveedor utiliza el valor de la opción 60 (Identificador de clase de proveedor).
- El contenedor de cliente utiliza la opción 61 (Identificador de cliente) para clientes PXE y el campo **chaddr** del paquete **BOOTP** para clientes de **BOOTP**.

Excepto para las subredes, cada contenedor permite especificar el valor que comparará incluyendo la comparación de expresión regular.

También existe un contenedor implícito, el contenedor *global*. Las opciones y los modificadores del contenedor global se aplican a todos los contenedores a menos que se alteren temporalmente o se rechacen. La mayoría de los contenedores se pueden poner dentro de otros contenedores lo que implica un ámbito de visibilidad. Los contenedores pueden tener o no tener asociados a ellos rangos de direcciones. Las subredes, por naturaleza, tienen rangos asociados a ellas.

Las normas básicas para los contenedores y subcontenedores son las siguientes:

- Todos los contenedores son válidos a nivel global.
- No se pueden poner nunca subredes dentro de otros contenedores.
- Los contenedores restringidos no pueden contener contenedores regulares del mismo tipo. (Por ejemplo, un contenedor con una opción que sólo permite una clase de Contabilidad no puede incluir un contenedor con una opción que permite todas las clases que empiezan con la letra "a". Esto no está permitido.)
- Los contenedores de cliente restringidos no pueden tener subcontenedores.

Según las normas anteriores, puede generar una jerarquía de contenedores que segmente las opciones en grupos para clientes o conjuntos de clientes específicos.

Si un cliente coincide con varios contenedores, ¿cómo se manejan las opciones y las direcciones? El servidor **DHCP** recibe mensajes, pasa la petición a la base de datos (archivo\_bd en este caso) y se genera una lista de contenedores. La lista se presenta en orden de profundidad y prioridad. La prioridad se define como una jerarquía implícita en los contenedores. Los contenedores estrictos tienen una prioridad más alta que los contenedores normales. Los clientes, las clases, los proveedores y finalmente las subredes se clasifican, en ese orden, y dentro del tipo de contenedor por profundidad. Esto genera una lista ordenada del más específico al menos específico. Por ejemplo:

```
Subnet 1
--Class 1
--Client 1
Subnet 2
--Class 1
----Vendor 1
----Client 1
--Client 1
```

El ejemplo anterior muestra dos subredes, Subnet 1 y Subnet 2. Hay un nombre de clase, Class 1, un nombre de proveedor, Vendor 1 y un nombre de cliente, Client 1. Class 1 y Client 1 se definen en varios lugares. Dado que están en contenedores diferentes, los nombres pueden ser iguales pero los valores que contienen pueden ser diferentes. Si Client 1 envía un mensaje al servidor **DHCP** de Subnet 1 especificando Class 1 en la lista de opciones, el servidor **DHCP** generará la siguiente vía de acceso de contenedor:

```
Subnet 1, Class 1, Client 1
```

El contenedor más específico se lista en último lugar. Para obtener una dirección, la lista se examina en jerarquía inversa para encontrar la primera dirección disponible. A continuación, la lista se examina avanzando en la jerarquía para obtener las opciones. Las opciones alteran temporalmente los valores anteriores a menos que exista un rechazo (deny) de opción en el contenedor. Asimismo dado que Class 1 y Client 1 están en Subnet 1, se ordenan de acuerdo con la prioridad de contenedor. Si el mismo cliente está en Subnet 2 y envía el mismo mensaje, la lista de contenedores generada es:

```
Subnet 2, Class 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)
```

Subnet 2 se lista en primer lugar, a continuación Class 1, y Client 1 en el nivel Subnet 2 (porque esta sentencia de cliente sólo está un nivel por debajo en la jerarquía). La jerarquía implica que un cliente que coincide con la primera sentencia de cliente es menos específico que el cliente que coincide con Client 1 de Class 1 en Subnet 2.

La prioridad seleccionada por profundidad en la jerarquía no se reemplaza por la prioridad de los propios contenedores. Por ejemplo, si el mismo cliente emite el mismo mensaje y especifica un identificador de proveedor, la lista de contenedores es:

```
Subnet 2, Class 1, Vendor 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)
```

La prioridad de contenedor mejora el rendimiento de búsqueda porque sigue un concepto general según el cual los contenedores de cliente son el modo más específico de definir uno o varios clientes. El contenedor de clase contiene direcciones menos específicas que un contenedor de cliente, el contenedor de proveedor es incluso menos específico y el contenedor de subred es el menos específico.

#### *Direcciones y rangos de direcciones de PXED*

Cualquier tipo de contenedor puede tener rangos de direcciones asociados; las subredes deben tenerlos. Cada rango dentro de un contenedor debe ser un subconjunto del rango del contenedor padre y no se debe solapar con rangos de otros contenedores.

Por ejemplo, si se define una clase dentro de una subred y la clase tiene un rango, el rango debe ser un subconjunto del rango de la subred. Asimismo, el rango dentro de ese contenedor de clases no se puede solapar con ningún otro rango que esté a su nivel.

Los rangos se pueden expresar en la línea de contenedor y modificar mediante sentencias de exclusión y rango para permitir separar conjuntos de direcciones asociadas con un contenedor. Por lo tanto, si tiene disponibles las diez direcciones superiores y las segundas diez direcciones de una subred, la subred puede especificar estas direcciones por rango en la cláusula de subred para reducir el uso de memoria y la posibilidad de colisión de direcciones con otros clientes que no están en los rangos especificados.

Cuando se ha seleccionado una dirección, cualquier contenedor subsiguiente de la lista que contiene rangos de direcciones se elimina de la lista junto con los hijos. La razón de ello es que las opciones específicas de red de contenedores eliminados no son válidas si no se utiliza una dirección de ese contenedor.

### *Opciones de archivos de configuración de PXED*

Después de que se haya seleccionado la lista para determinar las direcciones, se genera un conjunto de operaciones para el cliente.

En este proceso de selección, las opciones se graban encima de las opciones seleccionadas anteriormente a menos que se encuentre un *deny* (rechazo), en cuyo caso la opción rechazada se elimina de la lista que se está enviando al cliente. Este método permite la herencia de los contenedores padre para reducir la cantidad de datos que se deben especificar.

### *Registro cronológico de PXED*

Los parámetros de registro cronológico se especifican en un contenedor como la base de datos, pero la palabra clave de contenedor es `logging_info`.

Cuando se aprende a configurar PXED, es aconsejable activar el registro cronológico al nivel más alto. También es mejor especificar la configuración de registro cronológico antes de otros datos de archivo de configuración para asegurar que los errores de configuración se registran después de que se haya inicializado el subsistema de registro cronológico. Utilice la palabra clave `logitem` para activar el nivel de registro cronológico o elimine la palabra clave `logitem` para inhabilitar un nivel de registro cronológico. Otras palabras clave del registro cronológico permiten especificar el nombre de archivo de registro cronológico, el tamaño de archivo y el número de archivos de registro cronológico en rotación.

### *Consideraciones acerca del rendimiento de PXED*

Es importante conocer que determinadas palabras clave de configuración y la estructura del archivo de configuración tienen un efecto en el uso de memoria y el rendimiento del servidor PXED.

En primer lugar, se puede evitar el uso de memoria excesivo conociendo el modelo de opciones de herencia de los contenedores padre a hijo. En un entorno que no soporta clientes no listados, el administrador debe listar explícitamente cada cliente en el archivo. Cuando se listan opciones para cualquier cliente específico, el servidor utiliza más memoria almacenando ese árbol de configuración que cuando se heredan opciones de un contenedor padre (por ejemplo, los contenedores de subred, red o globales). Por consiguiente, el administrador debe verificar si se repiten opciones a nivel de cliente en el archivo de configuración y, si es así, determinar si estas opciones se pueden especificar en el contenedor padre y compartir entre el conjunto de clientes en general.

Asimismo, al utilizar las entradas de `logItem INFO` y `TRACE`, se registran muchos mensajes durante el proceso del mensaje de cada cliente PXE. La adición de una línea al archivo de registro puede ser una operación costosa; por consiguiente, si se limita la cantidad de registro, mejorará el rendimiento del servidor PXED. Cuando se sospecha un error con el servidor PXED, se puede volver a habilitar el registro dinámicamente utilizando el mandato **traceson** de SRC.

### **Subopciones de contenedor de proveedor PXE**

Cuando se soporta un cliente PXE, el servidor **DHCP** pasa la opción siguiente al servidor BINLD que BINLD utiliza para configurarse a sí mismo:

Núm. opc.	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
6	Número decimal	Sí	<p>PXE_DISCOVERY_CONTROL. Límite 0 a 16. Es un campo de bit. El bit 0 es el bit menos significativo.</p> <p><b>bit 0</b> Si se establece, inhabilita el descubrimiento de difusión.</p> <p><b>bit 1</b> Si se establece, inhabilita el descubrimiento de multidifusión.</p> <p><b>bit 2</b> Si se establece, sólo utiliza/acepta servidores en PXE_BOOT_SERVERS.</p> <p><b>bit 3</b> Si se establece y existe un nombre de archivo de arranque en el paquete de oferta PXED inicial, descarga el archivo de arranque (no solicita/menú/descubre servidor de arranque).</p> <p><b>bit 4-7</b> Debe ser 0. Si no se proporciona esta opción, el cliente supone que todos los bits son iguales a 0.</p>
7	Una doble palabra con puntos	Sí	Dirección IP multidifusión. Dirección IP multidifusión de descubrimiento de servidor de arranque. Los servidores de arranque capaces del descubrimiento de multidifusión deben escuchar en esta dirección de multidifusión. Esta opción es necesaria si el bit de inhabilitación de descubrimiento de multidifusión (bit 1) en la opción PXE_DISCOVERY_CONTROL no se ha establecido.

Núm. opc.	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
8	Servidor de arranque tipo(0-65535)	Sí	<p>PXE_BOOT_SERVERS cuenta direcciones IP (0-256)</p> <p><b>Tipo 0</b> Microsoft Windows dirección IP...dirección IP NT Boot Server Servidor de arranque tipo dirección IP</p> <p><b>Tipo 1</b> Intel LCM Boot Server count dirección IP ...</p> <p><b>Tipo 3</b> DOS/UNDI Boot Server dirección IP</p> <p><b>Tipo 4</b> NEC ESMPRO Boot Server</p> <p><b>Tipo 5</b> IBM WSoD Boot Server</p> <p><b>Tipo 6</b> IBM LCCM Boot Server</p> <p><b>Tipo 7</b> CA Unicenter TNG Boot Server.</p> <p><b>Tipo 8</b> HP OpenView Boot Server.</p> <p><b>Tipo 9 a 32767</b> Reservado</p> <p><b>Tipo 32768 a 65534</b> Uso de proveedor</p> <p><b>Tipo 65535</b> PXE API Test Server.</p> <p>Si cuenta de direcciones IP es cero para un tipo de servidor, el cliente puede aceptar ofertas de cualquier servidor de arranque de dicho tipo. Los servidores de arranque no responden las peticiones de descubrimiento de tipos que no soportan.</p>
9	Servidor de arranque tipo (0-65535)	Sí	PXE_BOOT_MENU "descripción" El "orden" de arranque del servidor de arranque está implícito en el tipo. "descripción"...orden menú.

Núm. opc.	Tipo de datos predeterminado	¿Se puede especificar?	Descripción
10	<i>Tiempo de espera en segundos (0-255)</i>	Sí	PXE_MENU_PROMPT "solicitud" El tiempo de espera es el número de segundos a espera antes de seleccionar automáticamente el primer elemento de menú de arranque. En el sistema cliente, se visualiza la solicitud seguida del número de segundos que quedan antes de que se seleccione automáticamente el primer elemento del menú de arranque. Si se pulsa la tecla F8 en el sistema cliente, se visualiza un menú. Si se proporciona esta opción en el cliente, el menú se visualiza sin solicitud ni tiempo de espera. Si el tiempo de espera es 0, el primer elemento del menú se selecciona automáticamente. Si el tiempo de espera es 255, se visualiza el menú y la solicitud sin selección automática ni tiempo de espera.

#### Sintaxis de archivo de servidor PXED para la operación de servidor general

Las palabras clave de archivo de servidor PXED del servidor **DHCPv6** que se describen aquí son para la operación general del servidor. Se identifican los formatos, subcontenedores, valores predeterminados y significados.

**Nota:** Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
database	database <i>tipo bd</i>	Sí	Ninguno	El contenedor primario que contiene las definiciones para las agrupaciones de dirección, las opciones y las sentencias de acceso de cliente. <i>tipo bd</i> es el nombre de un módulo que se carga para procesar esta parte del archivo. El único valor actualmente disponible es db_file.
logging_info	logging_info	Sí	Ninguno	El contenedor de registro cronológico primario que define los parámetros de registro.
logitem	logitem NONE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem SYSERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem OBJERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem PROTOCOL	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem PROTERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem WARN	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem WARNING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem CONFIG	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem EVENT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem PARSEERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem ACTION	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem ACNTING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem STAT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem TRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem RTRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
logitem	logitem START	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas
numLogFile	numLogFile <i>n</i>	No	0	Especifica el número de archivos de registro cronológico a crear. El registro cronológico rota cuando el primero se llena. <i>n</i> es el número de archivos que se deben crear.
logFileSize	logFileSize <i>n</i>	No	0	Especifica el tamaño de cada archivo de registro cronológico en unidades de 1024 bytes.
logFileName	logFileName <i>vía_acceso</i>	No	Ninguno	Especifica la vía de acceso al primer archivo de registro cronológico. El archivo de registro cronológico original se denomina <i>nombre_archivo</i> o <i>nombre_arch.ext</i> . El <i>nombre_archivo</i> debe tener ocho caracteres o menos. Cuando un archivo se rota, se redenomina empezando con el <i>nombre_archivo</i> base y, a continuación, añadiendo un número o sustituyendo la extensión por un número. Por ejemplo, si el nombre de archivo original es <i>file</i> , el nombre de archivo rotado se convierte en <i>file01</i> . Si el nombre de archivo original es <i>file.log</i> , se convierte en <i>file.01</i> .

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
pxeservertype	pxeservertype <i>tipo_servidor</i>	No	dhcp_only	Indica el tipo de servidor <b>dhcpsd</b> del que se trata. <i>tipo_servidor</i> puede ser <b>proxy_on_dhcp_server</b> , que significa que PXED se ejecuta en la misma máquina que el servidor <b>DHCP</b> y está escuchando las peticiones de cliente PXE en el puerto 4011 solamente, o el valor predeterminado de <b>pdhcp_only</b> , que significa que PXED se ejecuta en una máquina independiente y tiene que escuchar paquetes de cliente en el puerto 67 y 4011.

#### Sintaxis de archivo de servidor PXED para la base de datos db\_file

Aquí se describe la sintaxis de archivo de servidor PXED para la base de datos db\_file. Se identifican los formatos, subcontenedores, valores predeterminados y significados.

**Nota:**

1. Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.
2. Los elementos especificados en un contenedor se pueden alterar temporalmente en otro subcontenedor. Por ejemplo, puede definir globalmente clientes **BOOTP**, pero dentro de una subred determinada permitir clientes **BOOTP** especificando la palabra clave supportBootp en ambos contenedores.
3. Los contenedores de cliente, clase y proveedor permiten el soporte de expresiones regulares. Para clase y proveedor, una serie entrecerrillada donde el primer carácter después de las comillas es un punto de exclamación (!) indica que se debe tratar el resto de la serie como una expresión regular. El contenedor de cliente permite expresiones regulares en los campos **hwtype** y **hwaddr**. Se utiliza una sola serie para representar ambos campos con el formato siguiente:

número\_decimal-datos

Si número\_decimal es cero, los datos son una serie ASCII. Si es cualquier otro número, los datos son dígitos hexadecimales.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subnet	subnet default	Sí	Ninguno	Especifica una subred que no tienen ningún rango. El servidor utiliza la subred sólo cuando está respondiendo al paquete INFORM del cliente.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subnet	subnet <i>id subred máscara de red</i>			Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subnet	subnet <i>id subred máscara de red rango</i>			Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subnet	subnet <i>id subred máscara de red etiqueta:prioridad</i>			Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subnet	<i>subnet id subred máscara de red rango etiqueta:prioridad</i>			Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guion. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.
subnet	<i>subnet id subred rango</i>	Sí	Ninguno	Especifica una subred que va dentro de un contenedor de red. Define un rango de direcciones que es la subred entera a menos que se especifique la parte de rango opcional. La máscara de red asociada con la subred se toma del contenedor de red que la rodea.  <b>Nota:</b> Este método está en desuso y se ha sustituido por los demás formatos de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
option	option <i>número</i> <i>datos</i> ...	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula * deny opcional significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.
option	option <i>númerodeny</i>	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula * deny opcional significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
option	option * deny	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula * deny opcional significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.
exclude	exclude <i>una dirección IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
exclude	exclude <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.
range	range <i>dirección_IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
range	range <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
client	client <i>tipohw dirhw</i> NONE	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.
client	client <i>tipohw dirhw</i> ANY	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
client	client <i>tipohw dirhw doble_puntos</i>	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex o hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.
client	client <i>tipohw dirhw rango</i>	Sí	Ninguno	Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex o hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
class	class <i>serie</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.
class	class <i>serie rango</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
network	network <i>id red</i> máscara <i>red</i>	Sí	Ninguno	<p>Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.</p> <p><b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.</p>

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
network	network <i>id red</i>	Sí	Ninguno	<p>Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.</p> <p><b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.</p>

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
network	network <i>id red rango</i>	Sí	Ninguno	<p>Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.</p> <p><b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.</p>

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor hex</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor hex</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> 0xdata			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>0xdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> <i>rango</i>			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor rango hex</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> <i>rango hex</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> <i>rango Oxdata</i>			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor rango</i> ""			Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
inoption	inoption <i>número</i> <i>datos_opción</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida con los caracteres 0x.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
inoption	inoption <i>número</i> <i>datos_opción rango</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida con los caracteres 0x.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual fill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual sfill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual rotate <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual srotate <i>id</i> <i>id</i> ...	No	Ninguno	Especifica una subred virtual con una política. <b>fill</b> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <b>rotate</b> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <b>sfill</b> y <b>srotate</b> son lo mismo que <b>fill</b> y <b>rotate</b> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo id de subred.
inorder:	inorder: <i>id</i> <i>id</i> ...	No	Ninguno	Especifica una subred virtual con una política de llenado, que significa utilizar todas las direcciones del contenedor antes de ir al siguiente contenedor. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
balance:	balance: <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política de rotación, que significa utilizar la siguiente dirección del siguiente contenedor. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.
bootstrapserver	bootstrapserver <i>dirección IP</i>	No	Ninguno	Especifica el servidor que los clientes deben utilizar para realizar <b>TFTP</b> en los archivos después de recibir paquetes <b>BOOTP</b> o <b>DHCP</b> . Este valor rellena el campo <b>siaddr</b> del paquete. Es válido en cualquier nivel de contenedor.
giaddrfield	giaddrfield <i>dirección IP</i>	No	Ninguno	Especifica giaddrfield para los paquetes de respuesta. <b>Nota:</b> Esta especificación no está permitida en los protocolos <b>BOOTP</b> y <b>DHCP</b> , pero algunos clientes necesitan que el campo <b>giaddr</b> sea la pasarela predeterminada para la red. Debido a este potencial conflicto, giaddrfield sólo se deberá utilizar en un contenedor cliente, aunque puede funcionar a cualquier nivel.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
bootfile	bootfile <i>vía de acceso</i>	No	Ninguno	Especifica el archivo de arranque a utilizar en la sección de archivo del paquete de respuesta. Se puede especificar a cualquier nivel de contenedor. La política de archivo de arranque (bootfile) define cómo interactúan los elementos especificados en la sección de archivo del paquete de entrada con el archivo de arranque y las sentencias de directorio inicial.
pxebootfile	pxebootfile <i>Arch sistema VerPrinc VerSecund NombArchArranque</i>	No	Ninguno	Especifica el archivo de arranque que se debe proporcionar a un cliente. El analizador de archivo config genera un error si el número de parámetros después de la palabra clave es menor que 4 y lo ignora si es mayor que 4. Esta palabra clave sólo se puede utilizar en un contenedor.

Para obtener detalles sobre otras opciones, consulte “[Opciones conocidas del archivo de servidor DHCP en la página 231](#)” y “[Subopción de contenedor de proveedor de entorno de ejecución previa al arranque en la página 235](#)”.

## Daemon de capa de negociación de imagen de arranque

El servidor BINLD (Boot Image Negotiation Layer Daemon - Daemon de capa de negociación de imagen de arranque) es la tercera etapa de contacto para los clientes de entorno de ejecución previa al arranque (PXE).

Después de comunicarse con el servidor DHCP para obtener una dirección IP y después de comunicarse con el servidor DHCP de proxy PXE para obtener la ubicación del servidor de arranque, se establece contacto con el servidor de arranque para obtener el nombre de archivo y la ubicación de la que se puede descargar la imagen de arranque. El cliente PXE puede volver para comunicarse con el servidor de arranque varias veces en el transcurso del arranque si el cliente necesita varios archivos en el proceso de arranque.

La etapa final del arranque de red PXE es descargar la imagen de arranque proporcionada por el servidor de arranque. La ubicación del servidor TFTP y el nombre de archivo que se debe descargar la proporciona el servidor de arranque al cliente PXE.

### Componentes de servidor BINLD

Aquí se presentan los tres componentes principales del servidor BINLD.

El servidor BINLD se segmenta en tres partes principales: una base de datos, un motor de protocolo y un conjunto de hebras de servicio, cada una con su propia información de configuración.

### **Base de datos de BINLD**

Se utiliza la base de datos db\_file.dhcpo para generar las opciones que responden al paquete REQUEST de un cliente.

Las opciones devueltas por la base de datos dependen del tipo de servidor elegido. Las opciones se establecen utilizando la palabra clave pxeservertype en el archivo binld.cnf.

Si se utiliza la información en el archivo de configuración, la base de datos se prepara y se verifica la coherencia.

### **Motor de protocolo BINLD**

El motor de protocolo utiliza la base de datos para determinar qué información se debe devolver al cliente.

El motor de protocolo PXED se basa en Intel Preboot Execution Environment (PXE) Specification Versión 2.1, pero sigue siendo compatible con Intel PXE Specification Versión 1.1.

### **Operaciones con hebra BINLD**

La última parte del servidor BINLD es en realidad un conjunto de operaciones que se utilizan para mantener todos los elementos en ejecución.

Dado que el servidor BINLD tiene hebras, estas operaciones se configuran realmente como hebras que en ocasiones realizan acciones para asegurarse de que todo está correcto.

La primera hebra, la hebra *main*, maneja las peticiones SRC (por ejemplo **startsrc**, **stopsrc**, **lssrc**, **traceson** y **refresh**). Esta hebra también coordina todas las operaciones que afectan a todas las hebras y maneja las señales. Por ejemplo,

- A SIGHUP (-1) produce una renovación de todas las bases de datos en el archivo de configuración.
- A SIGTERM (-15) hace que el servidor se detenga de forma ordenada.

La otra hebra procesa paquetes. En función del tipo de servidor, puede haber una o dos hebras. Una hebra escucha en el puerto 67 y la segunda en el puerto 4011. Cada una puede manejar una petición de un cliente.

### **Configuración de BINLD**

De forma predeterminada, el servidor BINLD se configura leyendo el archivo /etc/binld.cnf, que especifica la base de datos de opciones y direcciones inicial del servidor.

El servidor se inicia desde SMIT o mediante mandatos de SRC.

La configuración del servidor BINLD es generalmente la parte más difícil de la utilización de BINLD en la red. En primer lugar, determine qué redes necesita que tengan clientes PXE. El ejemplo siguiente configura un servidor BINLD para que se ejecute en la misma máquina que el servidor DHCP:

```
pxeservertype      binld_on_dhcp_server
subnet default
{
    vendor pxe
    {
        bootstrapserver 9.3.149.6      #Dirección IP de servidor TFTP
        pxebootfile    1   2   1   window.one   1   0
        pxebootfile    2   2   1   linux.one    2   3
        pxebootfile    1   2   1   hello.one   3   4
        client 6 10005a8ad14d any
        {
            pxebootfile  1   2   1   aix.one     5   6
            pxebootfile  2   2   1   window.one  6   7
        }
    }
}
```

Dada la configuración anterior, el servidor BINLD escucha los paquetes de difusión individual del cliente en el puerto 4011 y los paquetes de multidifusión en el puerto 4011 si BINLD obtiene la dirección de multidifusión de dhcpsd/pxed. El servidor BINLD responde a los paquetes REQUEST/INFORM de cliente con el nombre de archivo de arranque y la dirección IP del servidor TFTP. Si BINLD no encuentra el

archivo de arranque con una capa coincidente especificada por el cliente, intente buscar un archivo de arranque para la capa siguiente. BINLD no responde cuando no hay ningún archivo de arranque que coincida con los requisitos de cliente (*Tipo*, *ArchSistema*, *VersPrinc*, *VersSecun* y *Capa*).

El ejemplo siguiente configura BINLD para que se ejecute en una máquina independiente (es decir, DHCP / PXED no se ejecuta en la misma máquina).

```
subnet 9.3.149.0 255.255.255.0
{
    vendor pxe
    {
        bootstrapserver      9.3.149.6      # Dirección ip de servidor TFTP.
        pxebootfile 1 2 1 window.one 1 0
        pxebootfile 2 2 1 linux.one 2 3
        pxebootfile 1 2 1 hello.one 3 4
        client 6 10005a8ad14d any
        {
            pxebootfile 1 2 1 aix.one 5 6
            pxebootfile 2 2 1 window.one 6 7
        }
    }
}
```

En el ejemplo anterior, no se ha establecido *pxeservertype*, de modo que el tipo de servidor predeterminado es **binld\_only**. El servidor BINLD escucha los paquetes de difusión individual del cliente en el puerto 4011, difunde los paquetes de difusión individual en el puerto 67 y los paquetes de multidifusión en el puerto 4011 si BINLD obtiene la dirección de multidifusión de dhcpsd/pxed. El nombre del archivo de arranque y la dirección IP del servidor TFTP se envía a un cliente PXE sólo si la dirección IP del cliente está en el rango de direcciones IP de la subred (9.3.149.0 a 9.3.149.255).

El ejemplo siguiente configura BINLD para que se ejecute en la misma máquina que el servidor PXED:

```
pxeservertype binld_on_proxy_server
subnet default
{
    vendor
    {
        bootstrapserver      9.3.149.6      # Dirección ip de servidor TFTP.
        pxebootfile 1 2 1 window.one 1 0
        pxebootfile 2 2 1 linux.one 2 3
        pxebootfile 1 2 1 hello.one 3 4
        client 6 10005a8ad14d any
        {
            pxebootfile 1 2 1 aix.one 5 6
            pxebootfile 2 2 1 window.one 6 7
        }
    }
}
```

Dada esta configuración, el servidor BINLD sólo escucha los paquetes de multidifusión en el puerto 4011 si BINLD obtiene la dirección de multidifusión de dhcpsd/pxed. Si no recibe ninguna dirección de multidifusión, BINLD sale y se registra un mensaje de error en el archivo de registro cronológico.

La cláusula *db\_file* de base de datos indica qué método de base de datos se debe utilizar para procesar esta parte del archivo de configuración. Los comentarios empiezan con un signo de almohadilla (#). El servidor PXED ignora el texto desde la # hasta el final de la línea. El servidor utiliza cada línea *option* para indicar al cliente qué debe hacer. ["Subopciones de contenedor de proveedor PXE"](#) en la página 352 describe las subopciones conocidas y soportadas actualmente. Consulte el apartado ["Sintaxis de archivo de servidor BINLD para la operación de servidor general"](#) en la página 395 si desea conocer procedimientos para especificar opciones que el servidor no conoce.

### **Archivo de configuración de BINLD**

El archivo de configuración tiene una sección de dirección y una sección de definición de opciones, que se basan en el concepto de contenedores que contienen opciones, modificadores y, potencialmente, otros contenedores.

Un *contenedor* (básicamente, un método para agrupar opciones) utiliza un identificador para clasificar los clientes en grupos. Los tipos de contenedor son subred, clase, proveedor y cliente. Actualmente, no hay ningún contenedor genérico que pueda definir el usuario. El identificador define de forma exclusiva el cliente para que se pueda realizar el seguimiento del cliente si, por ejemplo, se mueve entre subredes. Se puede utilizar más de un tipo de contenedor para definir el acceso de cliente.

Las *opciones* son identificadores que se devuelven al cliente, por ejemplo dirección de DNS y pasarela predeterminada.

#### *Contenedores BINLD*

Cuando el servidor DHCP recibe una petición, se analiza el paquete y las claves de identificación determinan qué contenedores, opciones y direcciones se extraen.

El último ejemplo de Configuración de BINLD muestra un contenedor de subred. La clave de identificación es la posición del cliente en la red. Si el cliente es de esa red, se clasifica en ese contenedor.

Cada tipo de contenedor utiliza una opción diferente para identificar un cliente:

- El contenedor de subred utiliza el campo giaddr o la dirección de la interfaz de recepción para determinar de qué subred procede el cliente.
- El contenedor de clase utiliza el valor de la opción 77 (Identificador de clase de sitio de usuario).
- El proveedor utiliza el valor de la opción 60 (Identificador de clase de proveedor).
- El contenedor de cliente utiliza la opción 61 (Identificador de cliente) para clientes PXED y el campo chaddr del paquete BOOTP para clientes de BOOTP.

Excepto para las subredes, cada contenedor permite la especificación del valor con el que coincide, incluida la coincidencia de expresiones regulares.

También existe un contenedor implícito, el contenedor *global*. Las opciones y los modificadores colocados en el contenedor global se aplican a todos los contenedores a menos que se alteren temporalmente o se rechacen. La mayoría de los contenedores se pueden poner dentro de otros contenedores lo que implica un ámbito de visibilidad. Los contenedores pueden tener o no tener asociados a ellos rangos de direcciones. Las subredes, por naturaleza, tienen rangos asociados a ellas.

Las normas básicas para los contenedores y subcontenedores son las siguientes:

- Todos los contenedores son válidos a nivel global.
- No se pueden poner nunca subredes dentro de otros contenedores.
- Los contenedores restringidos no pueden contener contenedores regulares del mismo tipo. (Por ejemplo, un contenedor con una opción que sólo permite una clase de Contabilidad no puede incluir un contenedor con una opción que permite todas las clases que empiezan con la letra "a". Esto no está permitido.)
- Los contenedores de cliente restringidos no pueden tener subcontenedores.

Según las normas anteriores, puede generar una jerarquía de contenedores que segmenta las opciones en grupos para clientes o conjuntos de clientes específicos.

Si un cliente coincide con varios contenedores, ¿cómo se manejan las opciones y las direcciones? El servidor DHCP recibe mensajes, pasa la petición a la base de datos (archivo\_bd en este caso) y se genera una lista de contenedores. La lista se presenta en orden de profundidad y prioridad. La prioridad se define como una jerarquía implícita en los contenedores. Los contenedores estrictos tienen una prioridad más alta que los contenedores normales. Los clientes, las clases, los proveedores y finalmente las subredes se clasifican, en ese orden, y dentro del tipo de contenedor por profundidad. Esto genera una lista ordenada del más específico al menos específico. Por ejemplo:

```
Subnet 1
--Class 1
--Client 1
Subnet 2
--Class 1
----Vendor 1
----Client 1
--Client 1
```

El ejemplo muestra dos subredes, Subnet 1 y Subnet 2. Hay un nombre de clase, Class 1, un nombre de proveedor, Vendor 1 y un nombre de cliente, Client 1. Class 1 y Client 1 se definen en varios lugares. Dado que están en contenedores diferentes, los nombres pueden ser iguales pero los valores que contienen pueden ser diferentes. Si Client 1 envía un mensaje al servidor DHCP de Subnet 1 especificando Class 1 en la lista de opciones, el servidor DHCP generará la siguiente vía de acceso de contenedor:

Subnet 1, Class 1, Client 1

El contenedor más específico se lista en último lugar. Para obtener una dirección, la lista se examina en jerarquía inversa para encontrar la primera dirección disponible. A continuación, la lista se examina avanzando en la jerarquía para obtener las opciones. Las opciones alteran temporalmente los valores anteriores a menos que exista un rechazo (*deny*) de opción en el contenedor. Asimismo dado que Class 1 y Client 1 están en Subnet 1, se ordenan de acuerdo con la prioridad de contenedor. Si el mismo cliente está en Subnet 2 y envía el mismo mensaje, la lista de contenedores generada es:

Subnet 2, Class 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)

Subnet 2 se lista en primer lugar, a continuación Class 1, y Client 1 en el nivel Subnet 2 (porque esta sentencia de cliente sólo está un nivel por debajo en la jerarquía). La jerarquía implica que un cliente que coincide con la primera sentencia de cliente es menos específico que el cliente que coincide con Client 1 de Class 1 en Subnet 2.

La prioridad seleccionada por profundidad en la jerarquía no se reemplaza por la prioridad de los propios contenedores. Por ejemplo, si el mismo cliente emite el mismo mensaje y especifica un identificador de proveedor, la lista de contenedores es:

Subnet 2, Class 1, Vendor 1, Client 1 (a nivel de Subnet 2), Client 1 (a nivel de Class 1)

La prioridad de contenedor mejora el rendimiento de búsqueda porque sigue un concepto general según el cual los contenedores de cliente son el modo más específico de definir uno o varios clientes. El contenedor de clase contiene direcciones menos específicas que un contenedor de cliente, el contenedor de proveedor es incluso menos específico y el contenedor de subred es el menos específico.

#### *Direcciones y rangos de direcciones de BINLD*

Cualquier tipo de contenedor puede tener rangos de direcciones asociados; las subredes deben tener un rango de direcciones asociado.

Cada rango dentro de un contenedor debe ser un subconjunto del rango del contenedor padre y no se debe solapar con rangos de otros contenedores. Por ejemplo, si se define una clase dentro de una subred y la clase tiene un rango, el rango debe ser un subconjunto del rango de la subred. Asimismo, el rango dentro de ese contenedor de clases no se puede solapar con ningún otro rango que esté a su nivel.

Los rangos se pueden expresar en la línea de contenedor y modificar mediante sentencias de exclusión y rango para permitir separar conjuntos de direcciones asociadas con un contenedor. Por lo tanto, si tiene disponibles las diez direcciones superiores y las segundas diez direcciones de una subred, la subred puede especificar estas direcciones por rango en la cláusula de subred para reducir el uso de memoria y la posibilidad de colisión de direcciones con otros clientes que no están en los rangos especificados.

Una vez que se ha seleccionado una dirección, cualquier contenedor subsiguiente de la lista que contiene rangos de direcciones se elimina de la lista junto con los hijos. La razón de ello es que las opciones específicas de red de contenedores eliminados no son válidas si no se utiliza una dirección de ese contenedor.

#### *Opciones de archivo de configuración BINLD*

Después de que se haya seleccionado la lista para determinar las direcciones, se genera un conjunto de operaciones para el cliente.

En este proceso de selección, las opciones se graban encima de las opciones seleccionadas anteriormente a menos que se encuentre un *deny* (rechazo), en cuyo caso la opción rechazada se elimina de la lista que se está enviando al cliente. Este método permite la herencia de los contenedores padre para reducir la cantidad de datos que se deben especificar.

### *Registro cronológico de BINLD*

Los parámetros de registro cronológico se especifican en un contenedor como la base de datos, pero la palabra clave de contenedor es `logging_info`.

Cuando se aprende a configurar PXED, es aconsejable activar el registro cronológico al nivel más alto. También es mejor especificar la configuración de registro cronológico antes de otros datos de archivo de configuración para asegurar que los errores de configuración se registran después de que se haya inicializado el subsistema de registro cronológico. Utilice la palabra clave `logitem` para activar el nivel de registro cronológico o elimine la palabra clave `logitem` para inhabilitar un nivel de registro cronológico. Otras palabras clave del registro cronológico permiten especificar el nombre de archivo de registro cronológico, el tamaño de archivo y el número de archivos de registro cronológico en rotación.

### *Consideraciones acerca del rendimiento de BINLD*

Es importante conocer que determinadas palabras clave de configuración y la estructura del archivo de configuración tienen un efecto en el uso de memoria y el rendimiento del servidor PXED.

En primer lugar, se puede evitar el uso de memoria excesivo conociendo el modelo de opciones de herencia de los contenedores padre a hijo. En un entorno que no soporta clientes no listados, el administrador debe listar explícitamente cada cliente en el archivo. Cuando se listan opciones para cualquier cliente específico, el servidor utiliza más memoria almacenando ese árbol de configuración que cuando se heredan opciones de un contenedor padre (por ejemplo, los contenedores de subred, red o globales). Por consiguiente, el administrador debe verificar si se repiten opciones a nivel de cliente en el archivo de configuración y, si es así, determinar si estas opciones se pueden especificar en el contenedor padre y compartir entre el conjunto de clientes en general.

Asimismo, al utilizar las entradas de `logItem INFO` y `TRACE`, se registran muchos mensajes durante el proceso del mensaje de cada cliente PXE. La adición de una línea al archivo de registro puede ser una operación costosa; por consiguiente, si se limita la cantidad de registro, mejorará el rendimiento del servidor PXED. Cuando se sospecha un error con el servidor PXED, se puede volver a habilitar el registro dinámicamente utilizando el mandato `traceson` de SRC.

### **Sintaxis de archivo de servidor BINLD para la operación de servidor general**

Aquí se describe la sintaxis de archivo de servidor BINLD para la operación de servidor general. Se identifican los formatos, subcontenedores, valores predeterminados y significados.

**Nota:** Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
database	database <i>tipo bd</i>	Sí	Ninguno	El contenedor primario que contiene las definiciones para las agrupaciones de dirección, las opciones y las sentencias de acceso de cliente. <i>tipo bd</i> es el nombre de un módulo que se carga para procesar esta parte del archivo. El único valor actualmente disponible es <code>db_file</code> .
logging_info	logging_info	Sí	Ninguno	El contenedor de registro cronológico primario que define los parámetros de registro.

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
logitem	logitem NONE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem SYSERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem OBJERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem PROTOCOL	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem PROTERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem WARN	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem WARNING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem CONFIG	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem EVENT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
logitem	logitem PARSEERR	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem ACTION	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem ACNTING	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem STAT	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem TRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem RTRACE	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
logitem	logitem START	No	De forma predeterminada todos toman el valor no habilitado.	Habilita el nivel de registro cronológico. Se permiten varias líneas.
numLogFiles	numLogFiles <i>n</i>	No	0	Especifica el número de archivos de registro cronológico a crear. El registro cronológico rota cuando el primero se llena. <i>n</i> es el número de archivos que se deben crear.
logFileSize	logFileSize <i>n</i>	No	0	Especifica el tamaño de cada archivo de registro cronológico en unidades de 1024 bytes.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
logFileName	logFileName <i>vía_acceso</i>	No	Ninguno	Especifica la vía de acceso al primer archivo de registro cronológico. El archivo de registro cronológico original se denomina <i>nombre_archivo</i> o <i>nombre_arch.ext</i> . Cuando un archivo se rota, se redenomina empezando con el <i>nombre_archivo</i> base y, a continuación, añadiendo un número o sustituyendo la extensión por un número. Por ejemplo, si el nombre de archivo original es <i>file</i> , el nombre de archivo rotado se convierte en <i>file01</i> . Si el nombre de archivo original es <i>file.log</i> , se convierte en <i>file.01</i> .
pxeservertype	pxeservertype <i>tipo_servidor</i>	No	dhcp_only	Indica el tipo de servidor dhcpsd del que se trata. <i>tipo_servidor</i> puede ser uno de los siguientes <b>binld_on_dhcp_server</b> Esto significa que BINLD se ejecuta en la misma máquina que el servidor DHCP y está escuchando la petición de cliente PXE en el puerto 4011 y la dirección de multidifusión si se recibe de DHCP / PXED. <b>binld_on_proxy_server</b> Esto significa que BINLD se ejecuta en la misma máquina que el servidor PXED y está escuchando la petición del cliente PXE en la dirección de multidifusión si se recibe de DHCP / PXED. El valor predeterminado es <b>binld_only</b> , que significa que BINLD se ejecuta en una máquina independiente y tiene que escuchar los paquetes del cliente en el puerto 67, 4011 y la dirección de multidifusión si se recibe de DHCP / PXED.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
dhcp_or_proxy_address	dhcp_or_proxy_addresses <i>dirección IP</i>	No	Ninguno	Proporciona la dirección IP del servidor dhcp o pxed al que el servidor BINLD puede enviar un paquete de una sola difusión de tipo REQUEST/INFORM para recibir la dirección de multidifusión. Esta palabra clave sólo se define cuando dhcp o pxed están en una subred diferente de BINLD.

#### Sintaxis de archivo de servidor BINLD para base de datos db\_file

Aquí se describe la sintaxis de archivo de servidor BINLD para la base de datos db\_file. Se identifican los formatos, subcontenedores, valores predeterminados y significados.

##### Nota:

1. Las unidades de tiempo (*unidades\_tiempo*) mostradas en la tabla siguiente son opcionales y representan un modificador en la hora real. La unidad de tiempo predeterminada son los minutos. Los valores válidos son segundos (1), minutos (60), horas (3600), días (86400), semanas (604800), meses (2392000) y años (31536000). El número mostrado entre paréntesis es un multiplicador aplicado al valor especificado *n* para expresar el valor en segundos.
2. Los elementos especificados en un contenedor se pueden alterar temporalmente en otro subcontenedor. Por ejemplo, puede definir globalmente clientes BOOTP, pero dentro de una subred determinada permitir clientes BOOTP especificando la palabra clave supportBootp en ambos contenedores.
3. Los contenedores de cliente, clase y proveedor permiten el soporte de expresiones regulares. Para clase y proveedor, una serie entrecerrillada donde el primer carácter después de las comillas es un punto de exclamación (!) indica que se debe tratar el resto de la serie como una expresión regular. El contenedor de cliente permite expresiones regulares en los campos hwtype y hwaddr. Se utiliza una sola serie para representar ambos campos con el formato siguiente:

número\_decimal-datos

Si número\_decimal es cero, los datos son una serie ASCII. Si es cualquier otro número, los datos son dígitos hexadecimales.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subred	subnet default	Sí	Ninguno	Especifica una subred que no tienen ningún rango. Un servidor utiliza la subred sólo cuando está respondiendo al paquete INFORM del cliente y la dirección del cliente no tiene otro contenedor de subred coincidente.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subred	subnet <i>id subred máscara de red</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guión. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.
subred	subnet <i>id subred máscara de red rango</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guión. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subred	<i>subnet id subred máscara de red etiqueta:prioridad</i>	Sí	Ninguno	Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guión. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.
subred	<i>subnet id subred máscara de red rango etiqueta:prioridad</i>			Especifica una subred y una agrupación de direcciones. Se supone que todas las direcciones están en la agrupación a menos que se especifique un rango en la línea o que las direcciones se modifiquen posteriormente en el contenedor mediante un rango o una sentencia de exclusión. El rango opcional es un par de direcciones IP en formato de doble palabra con puntos separadas por un guión. Se pueden especificar una etiqueta y una prioridad opcionales. Las subredes virtuales las utilizan para identificar y ordenar las subredes en la subred virtual. La etiqueta y la prioridad se separan mediante dos puntos. Estos contenedores sólo se permiten a nivel de contenedor de base de datos o global.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
subred	subnet <i>id subred rango</i>	Sí	Ninguno	<p>Especifica una subred que va dentro de un contenedor de red. Define un rango de direcciones que es la subred entera a menos que se especifique la parte de rango opcional. La máscara de red asociada con la subred se toma del contenedor de red que la rodea.</p> <p><b>Nota:</b> Este método está en desuso y se ha sustituido por los demás formatos de subred.</p>
option	option <i>número datos ...</i>	No	Ninguno	<p>Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), 0xdígitoshex, hex"<i>dígitoshex</i>" o hex "<i>dígitoshex</i>". Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.</p>

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
option	option <i>númerodeny</i>	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.
option	option * deny	No	Ninguno	Especifica una opción a enviar a un cliente o, en el caso de rechazo, una opción para impedir que se envíe al cliente. La cláusula de opción * deny significa que todas las opciones no especificadas en el contenedor actual no se devuelvan al cliente. La opción <i>númerodeny</i> sólo rechaza la opción especificada. <i>número</i> es un entero de 8 bits sin signo. <i>datos</i> es específico de la opción (vea más arriba) o se puede especificar como serie entre comillas (indicando texto ASCII), <i>Oxdígitoshex</i> , <i>hex"dígitoshex"</i> o <i>hex "dígitoshex"</i> . Si la opción está en un contenedor de proveedor, se encapsulará con otras opciones en una opción 43.

Palabra clave	Formato	¿Subcontene-dores?	Valor predeterminado	Significado
exclude	exclude <i>una dirección IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.
exclude	exclude <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de exclusión (exclude). La sentencia exclude no es válida en los niveles de contenedor de base de datos o global. La sentencia exclude elimina la dirección o el rango especificados del rango actual del contenedor. La sentencia exclude le permite crear rangos no contiguos para subredes u otros contenedores.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
range	range <i>dirección_IP</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
range	range <i>doble_puntos-doble_puntos</i>	No	Ninguno	Modifica el rango en el contenedor en el que está la sentencia de rango (range). La sentencia range no es válida en los niveles de contenedor de base de datos o global. Si el rango es el primero en el contenedor que no especifica un rango en la línea de definición de contenedor, el rango del contenedor se convierte en el rango especificado por la sentencia de rango. Cualquier sentencia de rango después de la primera sentencia de rango o de todas las sentencias de rango para un contenedor que especifica que los rangos en la definición se añaden al rango actual. Con la sentencia de rango, se puede añadir al rango una sola dirección o un conjunto de direcciones. El rango debe adaptarse en la definición de contenedor de subred.
client	client <i>tipohw dirhw</i> NONE			Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
client	client <i>tipohw dirhw</i> ANY			Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.
client	client <i>tipohw dirhw doble_puntos</i>			Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
client	client <i>tipohw dirhw rango</i>			Especifica un contenedor de cliente que impide que el cliente especificado por la <i>tipohw</i> y el <i>tipohw</i> obtenga una dirección. Si <i>tipohw</i> es 0, <i>dirhw</i> es una serie ASCII. De lo contrario, <i>tipohw</i> es el tipo de hardware para el cliente y <i>dirhw</i> es la dirección de hardware del cliente. Si la <i>dirhw</i> es una serie, se acepta que la serie esté entre comillas. Si la <i>dirhw</i> es una serie hexadecimal, la dirección se puede especificar mediante <i>Oxdígitoshex</i> o <i>hex dígitos</i> . <i>rango</i> permite que el cliente especificado por la <i>dirhw</i> y el <i>tipohw</i> obtenga una dirección en el <i>rango</i> . Deben ser expresiones regulares para comparar varios clientes.
class	class <i>serie</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
class	class <i>serie rango</i>	Sí	Ninguno	Especifica un contenedor de clase con el nombre <i>serie</i> . La serie puede estar entre comillas o no. Si está entre comillas, las comillas se eliminan antes de la comparación. Las comillas son necesarias para las series con espacios o tabuladores. Este contenedor es válido en cualquier nivel. Se puede proporcionar un rango para indicar un conjunto de direcciones a pasar a un cliente con esta clase. El rango es una dirección IP de doble palabra con puntos individual o dos direcciones IP de doble palabra con puntos separadas por un guión.
red	network <i>id red máscara red</i>	Sí	Ninguno	Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.  <b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
red	network <i>id red</i>	Sí	Ninguno	<p>Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.</p> <p><b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.</p>
red	network <i>id red rango</i>			<p>Especifica un ID de red utilizando información de clase (por ejemplo 9.3.149.0 con una máscara de red de 255.255.255.0 será la red 9.0.0.0 255.255.255.0). Esta versión del contenedor de red se utiliza para contener subredes con el mismo ID de red y la misma máscara de red. Cuando se proporciona un rango, todas las direcciones del rango están en la agrupación. El rango debe estar en la red del ID de red. Esto utiliza el direccionamiento completo de clase. Esto sólo es válido en el nivel de contenedor de base de datos o global.</p> <p><b>Nota:</b> La palabra clave de red está en desuso y se ha sustituido por el contenedor de subred.</p>

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor hex"</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor hex"</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> 0xdata	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> ""	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor rango</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor rango hex</i> ""	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor</i> <i>rango hex</i> ""	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o <i>hex"dígitos"</i> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

<b>Palabra clave</b>	<b>Formato</b>	<b>¿Subcontenedores?</b>	<b>Valor predeterminado</b>	<b>Significado</b>
vendor	vendor <i>id_proveedor</i> <i>rango Oxdata</i>	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor <i>id_proveedor rango</i> ""	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <i>Oxdígitoshex</i> o hex" <i>dígitos</i> ". Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. pxe después de la palabra clave vendor creará un contenedor de proveedor para PXEClient. pxeserver después de la palabra clave vendor creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor pxe	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <code>Oxdígitoshex</code> o <code>hex"dígitos"</code> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. <code>pxe</code> después de la palabra clave <code>vendor</code> creará un contenedor de proveedor para PXEClient. <code>pxeserver</code> después de la palabra clave <code>vendor</code> creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
vendor	vendor pxeserver	Sí	Ninguno	Especifica un contenedor de proveedor. Los contenedores de proveedor se utilizan para devolver la opción 43 al cliente. El id de proveedor se puede especificar en una serie entrecomillada o una serie binaria con el formato <code>Oxdígitoshex</code> o <code>hex"dígitos"</code> . Se puede poner un rango opcional después del id de proveedor. El rango se especifica como dos dobles palabras con puntos separadas por un guión. Después del rango opcional, se puede especificar una serie hexadecimal o una serie ASCII opcional como la primera parte de la opción 43. Si las opciones están en el contenedor, se añaden a los datos de la opción 43. Después de procesar todas las opciones, se añade a los datos una opción de fin de lista de opciones (End Of Option List). Para devolver opciones fuera de una opción 43, utilice un cliente de expresión regular que coincida con todos los clientes para especificar opciones normales a devolver basándose en el ID de proveedor. <code>pxe</code> después de la palabra clave <code>vendor</code> creará un contenedor de proveedor para PXEClient. <code>pxeserver</code> después de la palabra clave <code>vendor</code> creará un contenedor de proveedor para PXEServer.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
inoption	inoption <i>número</i> <i>datos_opción</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida con los caracteres 0x.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
inoption	inoption <i>número</i> <i>datos_opción rango</i>	Sí	Ninguno	Especifica un contenedor que se debe comparar con cualquier opción de entrada arbitraria especificada por el cliente. <i>número</i> especifica el número de opción. <i>datos_opción</i> especifica la clave a comparar para que se seleccione este contenedor durante la selección de dirección y opción para el cliente. <i>datos_opción</i> se especifica en el formato esperado — serie entrecomillada, dirección IP, valor entero — para opciones conocidas públicamente o se puede especificar opcionalmente como una serie hexadecimal de bytes si va precedida de los caracteres 0x. Para opciones que no se conocen públicamente en el servidor, se puede especificar una serie hexadecimal de bytes del mismo modo. Adicionalmente, los <i>datos_opción</i> pueden indicar una expresión regular que se debe comparar con la representación de serie de los datos de opción del cliente. Las expresiones regulares se especifican en una serie entrecomillada empezando con " ! (comillas dobles seguidas de un punto de exclamación). El formato de serie de las opciones no conocidas públicamente en el servidor serán una serie hexadecimal de bytes NO precedida con los caracteres 0x.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual fill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <b>fill</b> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <b>rotate</b> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <b>sfill</b> y <b>srotate</b> son lo mismo que <b>fill</b> y <b>rotate</b> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <b>id</b> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo <b>id</b> de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual sfill <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo <i>id</i> de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual rotate <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo <i>id</i> de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual	virtual srotate <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política. <i>fill</i> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <i>rotate</i> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <i>sfill</i> y <i>srotate</i> son lo mismo que <i>fill</i> y <i>rotate</i> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo <i>id</i> de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
virtual		No	Ninguno	Especifica una subred virtual con una política. <code>fill</code> significa utilizar todas las direcciones del contenedor antes de pasar al siguiente contenedor. <code>rotate</code> significa seleccionar una dirección de la siguiente agrupación de la lista en cada petición. <code>sfill</code> y <code>srotate</code> son lo mismo que <code>fill</code> y <code>rotate</code> , pero se realiza una búsqueda para ver si el cliente compara los contenedores, los proveedores o las clases de la subred. Si se encuentra una coincidencia que puede proporcionar una dirección, se toma la dirección de dicho contenedor en lugar de seguir la política. Puede haber tantos ID como sean necesarios. <code>id</code> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo <code>id</code> de subred.
inorder:	<code>inorder: id id ...</code>	No	Ninguno	Especifica una subred virtual con una política de llenado, que significa utilizar todas las direcciones del contenedor antes de ir al siguiente contenedor. Puede haber tantos ID como sean necesarios. <code>id</code> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
balance:	balance: <i>id id ...</i>	No	Ninguno	Especifica una subred virtual con una política de rotación, que significa utilizar la siguiente dirección del siguiente contenedor. Puede haber tantos ID como sean necesarios. <i>id</i> es el ID de subred de la definición de subred o la etiqueta de la definición de subred. La etiqueta es necesaria si hay varias subredes con el mismo ID de subred.
bootstrapserver	bootstrapserver <i>dirección IP</i>	No	Ninguno	Especifica el servidor que los clientes deben utilizar para realizar TFTP en los archivos después de recibir paquetes BOOTP o DHCP. Este valor rellena el campo <b>siaddr</b> del paquete. Es válido en cualquier nivel de contenedor.
giaddrfield	giaddrfield <i>dirección IP</i>	No	Ninguno	Especifica giaddrfield para los paquetes de respuesta. <b>Nota:</b> Esta especificación no está permitida en los protocolos BOOTP y DHCP, pero algunos clientes necesitan que el campo <b>giaddr</b> sea la pasarela predeterminada para la red. Debido a este potencial conflicto, giaddrfield sólo se deberá utilizar en un contenedor cliente, aunque puede funcionar a cualquier nivel.
bootfile	bootfile <i>vía de acceso</i>	No	Ninguno	Especifica el archivo de arranque a utilizar en la sección de archivo del paquete de respuesta. Se puede especificar a cualquier nivel de contenedor. La política de archivo de arranque (bootfile) define cómo interactúan los elementos especificados en la sección de archivo del paquete de entrada con el archivo de arranque y las sentencias de directorio inicial.

Palabra clave	Formato	¿Subcontenedores?	Valor predeterminado	Significado
pxebootfile	pxebootfile <i>ArchSistema VerPrinc VerSecund nombArchArranque Tipo Capa</i>	No	Ninguno	Especifica el archivo de arranque que se debe proporcionar a un cliente PXE. El analizador de archivo config genera un error si el número de parámetros después de la palabra clave es menor que 4, lo ignora si es mayor que 7 y si es 4, supone que el valor para Type = 0 y Layer = 0. Esta palabra clave sólo se puede utilizar en un contenedor.

Para obtener detalles sobre otras opciones, consulte [“Opciones conocidas del archivo de servidor DHCP”](#) en la página 231 y [“Subopciones de contenedor de proveedor PXE”](#) en la página 352.

## Daemons TCP/IP

Los daemons (también conocidos como *servidores*) son procesos que se ejecutan continuamente en segundo plano y realizan funciones necesarias para otros procesos. **TCP/IP (Transmission Control Protocol/Internet Protocol)** proporciona daemons para implementar determinadas funciones en el sistema operativo.

Estos daemons son procesos en segundo plano que se ejecutan sin interrumpir otros procesos (a menos que esto forme parte de la función del daemon).

Los daemons se invocan utilizando mandatos a nivel de gestión de sistema, otros daemons o scripts de shell. También puede controlar los daemons con el daemon **inetd**, el script de shell **rc.tcpip** y el SRC (Controlador de recursos del sistema).

### Subsistemas y servidores

Un *subsistema* es un daemon, o servidor, controlado por el SRC. Un *subservidor* es un daemon controlado por un subsistema. (Los mandatos de daemon y los nombres de daemon se suelen indicar mediante una **d** al final del nombre.)

Las categorías de subsistema y subservidor se excluyen mutuamente. Es decir, los daemons no se listan como subsistema y como subservidor. El único subsistema **TCP/IP** que controla otros daemons es el daemon **inetd**. Todos los subservidores **TCP/IP** también son subservidores **inetd**.

Para obtener una lista de los daemons **TCP/IP**, consulte el apartado [“Daemons TCP/IP”](#) en la página 511.

### Control de recursos del sistema

Entre otras funciones, SRC le permite iniciar daemons, detenerlos y rastrear su actividad. Además, SRC proporciona la posibilidad de agrupar los daemons en subsistemas y subservidores.

SRC (System Resource Control - Control de recursos del sistema) es una herramienta diseñada para ayudarle a controlar daemons. SRC permite el control más allá de los distintivos y parámetros disponibles con cada mandato de daemon.

Consulte el apartado [Controlador de recursos del sistema](#) en la publicación *Sistema operativo y gestión de dispositivos* para obtener más información relacionada con el Controlador de recursos del sistema.

Para obtener una lista de los mandatos de SRC, consulte el apartado [“Mandatos de SRC”](#) en la página 509.

### Configuración del daemon inetd

Siga estos pasos para configurar el daemon **inetd** de **TCP/IP**.

Para configurar el daemon **inetd**:

1. Especifique qué subservidores lo invocarán añadiendo un daemon **inetd**.
2. Especifique las características de reinicio cambiando dichas características del daemon **inetd**.

*Tabla 76. Configuración de las tareas de daemon inetd*

Tarea	Vía rápida de SMIT	Mandato o archivo
Iniciar el daemon <b>inetd</b>	smit mkinetd	<b>startsrc -s inetd</b>
Cambiar las características de inicio del daemon <b>inetd</b>	smit chinetc o smit lsinetd	
Detención del daemon <b>inetd</b>	smit rminetd	<b>stopsrc -s inetd</b>
Listar todos los subservidores <b>inetd</b>	smit inetdconf	
Añadir un subservidor <sup>1</sup> <b>inetd</b>	smit mkinetdconf	Edite /etc/inetd.conf y, a continuación, ejecute <b>refresh -s inetd</b> o <b>kill -1 PIDinetd</b> <sup>2</sup>
Cambiar/Mostrar características de un subservidor <b>inetd</b>	smit inetdconf	Edite /etc/inetd.conf y, a continuación, ejecute <b>refresh -s inetd</b> o <b>kill -1 PIDinetd</b> <sup>2</sup>
Eliminar un subservidor <b>inetd</b>	smit rminetd	Edite /etc/inetd.conf y, a continuación, ejecute <b>refresh -s inetd</b> o <b>kill -1 PIDinetd</b> <sup>2</sup>

**Nota:**

1. Al añadir un subservidor **inetd** se configura el daemon **inetd** para que invoque el subservidor cuando se necesite.
2. El mandato **refresh** y el mandato **kill** informan al daemon **inetd** de los cambios en el archivo de configuración.

### Servicios de red de cliente

Servicios de red del cliente (al que se accede utilizando la vía de acceso rápida de SMIT, smit clientnet), hace referencia a los protocolos **IP TCP/** disponibles para que los utilice este sistema operativo.

Cada protocolo (o servicio) se conoce por el número de puerto que utiliza en la red y por eso se utiliza el término *puerto conocido públicamente*. Por comodidad de los programadores, se puede hacer referencia a los números de puerto utilizando nombres así como números. Por ejemplo, el protocolo de correo **TCP/IP** utiliza el puerto 25 y se conoce por el nombre **smtp**. Si un protocolo se lista (no comentado) en el archivo /etc/services, un sistema principal puede utilizar dicho protocolo.

De forma predeterminada, todos los protocolos **TCP/IP** se definen en el archivo /etc/services. No tiene que configurar este archivo. Si escribe sus propios programas de cliente/servidor, es posible que desee añadir el servicio al archivo /etc/services y reservar un número de puerto y nombre específicos para el servicio. Si decide añadir el servicio a /etc/services, tenga en cuenta que los números de puerto 0 a 1024 están reservados para uso del sistema.

*Tabla 77. Tareas de servicios de red de cliente*

Tarea	Vía rápida de SMIT	Mandato o archivo
Listar todos los servicios	smit lsservices	view /etc/services
Añadir un servicio	smit mkservices	edit /etc/services
Cambiar/Mostrar características de un servicio	smit chservices	edit /etc/services

Tabla 77. Tareas de servicios de red de cliente (continuación)

Tarea	Vía rápida de SMIT	Mandato o archivo
Eliminar un servicio	smit rmsservices	edit /etc/services

#### Servicios de red de servidor

Los servicios de red de servidor incluyen el control del acceso remoto, el inicio o la detención de **TCP/IP** y la gestión del controlador de dispositivo pty, como se muestra en esta tabla.

El controlador de dispositivo pty se instala automáticamente con el sistema. De forma predeterminada, se configura para soportar 16 enlaces simbólicos de estilo BSD y está disponible para que lo utilice el sistema en el arranque.

Tabla 78. Tareas de servicios de red de servidor

Tarea	Vía rápida de SMIT	Mandato o archivo
Controlar el acceso remoto		Consulte "Remote Command Execution Access" y "Restricted File Transfer Program Users" en la publicación <i>Security</i> .
Iniciar, reiniciar o detener subsistemas TCP/IP	smit otherserv	Consulte el apartado "Control de recursos del sistema" en la página 431.
Cambiar/mostrar características del controlador de dispositivo pty	smit chgpty	<b>chdev -l ptyX -P -a num=X</b> donde X está en un rango de 0 a 64
Dejar el controlador de dispositivo pty no disponible para uso	smit pty y, a continuación, seleccione <b>Eliminar la PTY; conservar la definición</b>	Ningún mandato o archivo relacionado.
Dejar el controlador de dispositivo pty disponible para uso	smit pty y, a continuación, seleccione <b>Configurar la PTY definida</b>	Ningún mandato o archivo relacionado.
Generar un informe de error	smit errpt	Ningún mandato o archivo relacionado.
Rastrear la pty	smit trace	Ningún mandato o archivo relacionado.

#### Direccionamiento TCP/IP

Una *ruta* define una vía de acceso para enviar paquetes a través de la red Internet a una dirección de otra red.

Una ruta no define la vía de acceso completa, sólo el segmento de vía de acceso de un sistema principal a una pasarela que puede reenviar paquetes a un destino (o de una pasarela a otra). Existen cinco tipos de rutas:

Item	Descripción
<b>ruta de sistema principal</b>	Define una pasarela que puede reenviar paquetes a un sistema principal específico de otra red.
<b>ruta de red</b>	Define una pasarela que puede reenviar paquetes a cualquiera de los sistemas principales de una red específica.
<b>ruta predeterminada</b>	Define una pasarela que se deberá utilizar cuando no se haya definido una ruta de sistema principal o de red a un destino.

Item	Descripción
<b>ruta de bucle de retorno</b>	Ruta predeterminada para todos los paquetes enviados a direcciones de red locales. El IP de ruta de bucle de retorno es siempre 127.0.0.1.
<b>ruta de difusión</b>	Ruta predeterminada para todos los paquetes de difusión. Se asignan automáticamente dos rutas de difusión a cada subred en la que la red tiene un IP (una a la dirección de subred y otra a la dirección de difusión de la subred).

Las rutas se definen en la *tabla de direccionamiento* de kernel. Las definiciones de ruta incluyen información sobre las redes que se pueden alcanzar desde el sistema principal local y sobre las pasarelas que se pueden utilizar para alcanzar redes remotas. Cuando una pasarela recibe un datagrama, comprueba las tablas de direccionamiento para averiguar dónde se debe enviar a continuación el datagrama por la vía de acceso hasta su destino.

Puede añadir varias rutas para el mismo destino en la tabla de direccionamiento de kernel. Una búsqueda de direccionamiento evalúa todas las rutas que coinciden con la petición y, a continuación, elige la ruta con la métrica de distancia más baja. Si varias rutas coincidentes tienen una distancia igual, una búsqueda elige la ruta más específica. Si ambos criterios son iguales para varias rutas, las búsquedas de direccionamiento alternan las elecciones de rutas coincidentes.

### Direccionamiento estático y dinámico

En **TCP/IP**, el direccionamiento es uno de dos tipos: *estático* o *dinámico*.

Con el direccionamiento estático, mantiene la tabla de direccionamiento manualmente utilizando el mandato **route**. El direccionamiento estático es práctico para una red individual que se comunica con una o con otras dos redes. Sin embargo, cuando la red empieza a comunicarse con más redes, aumenta el número de pasarelas y también aumenta la cantidad de tiempo y esfuerzo necesarios para mantener la tabla de direccionamiento manualmente.

Con el direccionamiento dinámico, los daemons actualizan la tabla de direccionamiento automáticamente. Los daemons de direccionamiento reciben continuamente información difundida por otros daemons de direccionamiento y, por consiguiente, actualizan continuamente la tabla de direccionamiento.

**TCP/IP** proporciona dos daemons para utilizarlos en el direccionamiento dinámico, los daemons **routed** y **gated**. El daemon **gated** soporta simultáneamente los protocolos de direccionamiento **Routing Information Protocol (RIP)**, **Routing Information Protocol Next Generation (RIPng)**, **Exterior Gateway Protocol (EGP)**, **Border Gateway Protocol (BGP)** y **BGP4+**, **Defense Communications Network Local-Network Protocol (HELLO)**, **Open Shortest Path First (OSPF)**, **Intermediate System to Intermediate System (IS-IS)** e **Internet Control Message Protocol (ICMP and ICMPv6)/Router Discovery**. Además, el daemon **gated** soporta **Simple Network Management Protocol (SNMP)**. El daemon **routed** sólo soporta **Routing Information Protocol**.

Los daemons de direccionamiento pueden funcionar en una de dos modalidades, *pasiva* o *activa*, en función de las opciones que se utilicen al iniciar los daemons. En modalidad activa, los daemons de direccionamiento difunden periódicamente información de direccionamiento sobre la red local a las pasarelas y los sistemas principales y reciben información de direccionamiento de los sistemas principales y las pasarelas. En modalidad pasiva, los daemons de direccionamiento reciben información de direccionamiento de los sistemas principales y las pasarelas, pero no intentan mantener actualizadas las pasarelas remotas (no anuncian su propia información de direccionamiento).

Estos dos tipos de direccionamiento se pueden utilizar no sólo para las pasarelas, sino también para otros sistemas principales de una red. El direccionamiento estático funciona igual para las pasarelas que para otros sistemas principales. Sin embargo, los daemons de direccionamiento dinámico se deben ejecutar en modalidad pasiva (lacónica) cuando se ejecutan en un sistema principal que no es una pasarela.

### Pasarelas de direccionamiento TCP/IP

Las pasarelas son un tipo de direccionador. Los *direcciónadores* conectan dos o más redes y proporcionan la función de direccionamiento. Algunos direcciónadores, por ejemplo, direccionan a nivel de interfaz de red o a nivel físico. Sin embargo, las *pasarelas* direccionan a nivel de red.

Las pasarelas reciben datagramas IP de otras pasarelas o sistemas principales para entregarlos a los sistemas principales de la red local y direccionan los datagramas IP de una red a otra. Por ejemplo, una pasarela que conecta dos Redes en anillo tiene dos tarjetas adaptadoras de Red en anillo, cada una con su propia interfaz de Red en anillo. Para pasar información, la pasarela recibe datagramas a través de una interfaz de red y los envía a través de la otra interfaz de red. Las pasarelas verifican periódicamente las conexiones de red mediante mensajes de estado de interfaz.

Las pasarelas direccionan los paquetes de acuerdo con la red de destino, no de acuerdo con el sistema principal de destino. Es decir, no se necesita una máquina de pasarela para hacer el seguimiento de cada destino de sistema principal posible para un paquete. En lugar de ello, una pasarela direcciona los paquetes de acuerdo con la red del sistema principal de destino. Entonces la red de destino se encarga de enviar el paquete al sistema principal de destino. De este modo, una máquina de pasarela típica sólo necesita una capacidad de almacenamiento de disco limitada (si existe) y una capacidad de memoria principal limitada.

La distancia que un mensaje debe viajar del sistema principal de origen al sistema principal de destino depende del número de *saltos de pasarela* que deba realizar. Una pasarela está a cero saltos de una red a la que está conectada directamente, a un salto de una red que es alcanzable a través de una pasarela, y así sucesivamente. La distancia de mensaje se suele expresar como el número de saltos de pasarela necesarios, o *cuentas de salto* (que también se denomina *métrica*).

#### **Pasarelas de direccionamiento interiores y exteriores**

Las pasarelas interiores son pasarelas que pertenecen al mismo sistema autónomo. Se comunican entre ellas utilizando los protocolos **Routing Information Protocol (RIP)**, **Routing Information Protocol Next Generation (RIPng)**, **Intermediate System to Intermediate System**, **Open Shortest Path First (OSPF)** o **HELLO Protocol (HELLO)**. Las pasarelas exteriores pertenecen a sistemas autónomos diferentes. Utilizan los protocolos **Exterior Gateway Protocol (EGP)**, **Border Gateway Protocol (BGP)** o **BGP4+**.

Por ejemplo, examine dos sistemas autónomos. El primero son todas las redes administradas por la empresa Widget. El segundo son todas las redes administradas por la empresa Gadget. La empresa Widget tiene una máquina, denominada apple, que es la pasarela de Widget a Internet. La empresa Gadget tiene una máquina, denominada orange, que es la pasarela de Gadget a Internet. Ambas empresas tienen varias redes diferentes internas de la empresa. Las pasarelas que conectan las redes internas son pasarelas internas. Pero apple y orange son pasarelas exteriores.

Cada pasarela exterior no se comunica con cada una de las otras pasarelas exteriores. En lugar de ello, la pasarela exterior adquiere un conjunto de vecinos (otras pasarelas exteriores) con las que se comunica. Estos vecinos no se definen por proximidad geográfica, sino por las comunicaciones establecidas entre ellos. Las pasarelas de vecinos, a su vez, tiene otros vecinos de pasarelas exteriores. De este modo, las tablas de direcciónamiento de pasarela exterior se actualizan y la información de direcciónamiento se propaga entre las pasarelas exteriores.

La información de direcciónamiento se envía en un par, (N,D), donde N es la red y D es una distancia que refleja el coste de alcanzar la red especificada. Cada pasarela anuncia las redes que puede alcanzar y los costes de alcanzarlas. La pasarela receptora calcula las vías de acceso más cortas a las demás redes y pasa esta información a los vecinos. De este modo, cada pasarela exterior está continuamente recibiendo información de direcciónamiento, actualizando la tabla de direcciónamiento y, a continuación, pasando esa información a los vecinos exteriores.

#### **Protocolos de pasarela**

Todas las pasarelas, interiores o exteriores, utilizan protocolos para comunicarse entre ellas. A continuación se proporcionan descripciones breves de los protocolos de pasarela **TCP/IP** utilizados más comúnmente:

##### **HELLO (Protocolo HELLO)**

**HELLO** es un protocolo que las pasarelas interiores utilizan para comunicarse entre ellas. **HELLO** calcula la vía de acceso más corta a las demás redes determinando la vía de acceso que tiene el menor tiempo de retardo.

##### **RIP (Routing Information Protocol - Protocolo de información de direcciónamiento)**

**Routing Information Protocol** es un protocolo que las pasarelas interiores utilizan para comunicarse entre ellas. Como el **Protocolo HELLO**, **RIP** calcula la vía de acceso más corta a las demás redes. A

diferencia de **HELLO**, **RIP** calcula la distancia no por tiempo de retardo, sino por cuentas de saltos. Puesto que el daemon **gated** almacena toda la métrica internamente como retardos de tiempo, convierte las cuentas de saltos de **RIP** en retardos de tiempo.

#### **Routing Information Protocol Next Generation (Protocolo de información de direccionamiento de siguiente generación)**

**RIPng** es el protocolo **RIP** que se ha mejorado para soportar **IPv6**.

#### **OSPF (Open Shortest Path First - Primero vía de acceso abierta más corta)**

**OSPF** es un protocolo que las pasarelas interiores utilizan para comunicarse entre ellas. Es un protocolo de estado de enlace que es más adecuado que **RIP** para las redes complejas con muchos direcccionadores. Proporciona direccionamiento de varias vías de acceso de coste igual.

#### **EIGP (Exterior Gateway Protocol - Protocolo de pasarela exterior)**

Las pasarelas exteriores pueden utilizar el **Exterior Gateway Protocol** para comunicarse entre ellas. El **EIGP** no calcula la vía de acceso más corta a las demás redes. En lugar de ello, simplemente indica si una red determinada es alcanzable o no.

#### **BGP (Border Gateway Protocol - Protocolo de pasarela de borde)**

Las pasarelas exteriores pueden utilizar este protocolo para comunicarse entre ellas. Intercambia información sobre la posibilidad de alcance entre sistemas autónomos, pero proporciona más posibilidades que **EIGP**. **BGP** utiliza atributos de vía de acceso para proporcionar más información sobre cada ruta como ayuda para seleccionar la mejor.

#### **Border Gateway Protocol 4+ (Protocolo de pasarela de borde 4+)**

**BGP4+** es la versión 4 del protocolo **BGP**, que soporta **IPv6** y tiene otras mejoras respecto a las versiones pasadas del protocolo.

#### **IS-IS (Intermediate System to Intermediate System - Sistema intermedio a sistema intermedio)**

Las pasarelas interiores utilizan el protocolo **IS-IS** para comunicarse entre ellas. Es un protocolo de estado de enlace que puede direccionar paquetes IP e ISO/CLNP y, como **OSPF**, utiliza un algoritmo "primero vía de acceso más corta" para determinar las rutas.

#### **Consideraciones acerca de las pasarelas**

Realice estas acciones antes de configurar la pasarela.

Antes de configurar las pasarelas para la red, debe realizar lo siguiente:

1. Tenga en cuenta el número de pasarelas que se deberán utilizar.

El número de pasarelas que necesita configurar depende de lo siguiente:

- El número de redes que desea conectar.
- Cómo desea conectar las redes.
- El nivel de actividad de las redes conectadas.

Por ejemplo, suponga que todos los usuarios de la Red 1, Red 2 y Red 3 necesitan comunicarse entre ellos.

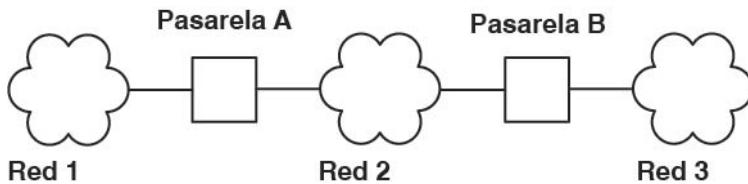


Figura 24. Configuración de pasarela simple

Esta ilustración contiene tres redes en forma de nube numeradas una, dos y tres. Las redes uno y dos están conectadas con la pasarela A. Las redes dos y tres están conectadas con la pasarela B.

Para conectar la Red 1 directamente a la Red 2, deberá utilizar una pasarela individual (Pasarela A). Para conectar la Red 2 directamente a la Red 3, deberá utilizar otra pasarela (Pasarela B). Ahora, suponiendo que se han definido las rutas correctas, todos los usuarios de las tres redes se pueden comunicar.

Sin embargo, si la Red 2 está muy ocupada, es posible que las comunicaciones entre la Red 1 y la Red 3 sufran retardos inaceptables. Además, si la mayor parte de las comunicaciones entre redes se produce entre la Red 1 y la Red 3, es aconsejable que conecte la Red 1 directamente a la Red 3. Para ello, puede utilizar un par adicional de pasarelas, la Pasarela C (en la Red 1) y la Pasarela D (en la Red 3), con una conexión directa entre estas dos pasarelas adicionales. Sin embargo, es posible que esta solución no sea eficiente porque una pasarela puede conectar más de dos redes.

Una solución más eficiente puede ser conectar directamente la Pasarela A a la Pasarela B, así como a la Red 2. Para ello se necesitará un segundo adaptador de red en la Pasarela A y la Pasarela B. En general, el número de redes que conecte mediante una sola pasarela estará limitado por el número de tarjetas de adaptador de red que la máquina de pasarela pueda soportar.

## 2. Decide el tipo de direccionamiento que se deberá utilizar.

Si la red es pequeña y la configuración apenas cambia, es aconsejable que utilice el direccionamiento estático. Pero si tiene una red grande cuya configuración cambia frecuentemente, es aconsejable que utilice el direccionamiento dinámico. Puede que decida utilizar una combinación de direccionamiento estático y dinámico. Es decir, es posible que desee proporcionar definiciones estáticas a unas cuantas rutas específicas, al mismo tiempo que permitir que los daemons actualicen otras rutas. Las rutas estáticas que cree no se anunciarán en otras pasarelas y los daemons de direccionamiento no las actualizarán.

## 3. Si está utilizando el direccionamiento dinámico, elija el daemon de direccionamiento de acuerdo con el tipo de pasarela que necesita y los protocolos que la pasarela debe soportar.

Si la pasarela es una pasarela interior y sólo necesita soportar **RIP**, elija el daemon **routed**. Si la pasarela debe soportar cualquier otro protocolo o es una pasarela exterior, elija el daemon **gated**.

**Nota:** Se pueden producir resultados imprevisibles si los daemons **gated** y **routed** se ejecutan en el mismo sistema principal al mismo tiempo.

## Configuración de una pasarela

Para configurar una máquina para que actúe como pasarelas, utilice estas instrucciones.

Para que resulte más claro, este procedimiento supone que la máquina de pasarela conecta dos redes y que la máquina de pasarela ya se ha configurado mínimamente en una de las redes.

1. Instale y configure el segundo adaptador de red, si aún no lo ha hecho. (Consulte el apartado “Instalación de un adaptador de red” en la página 170 y el apartado “Configuración y gestión de los adaptadores” en la página 170.)
2. Elija una dirección IP para la segunda interfaz de red y, a continuación, configure la interfaz de red siguiendo las instrucciones del apartado “Gestión de interfaz de red” en la página 176.
3. Añada una ruta a la segunda red.
4. Para utilizar una máquina como direccionador entre redes a través de redes **TCP/IP**, escriba:

```
no -o ipforwarding=1
```

La máquina de pasarela puede acceder ahora a ambas redes a las que está conectada directamente.

1. Si desea utilizar el direccionamiento estático para comunicarse con sistemas principales o redes más allá de estas dos redes, añada cualquier otra ruta que desee.
2. Si desea utilizar el direccionamiento dinámico, siga las instrucciones del apartado “Configuración del daemon **routed**” en la página 440 o del apartado “Configuración del daemon **gated**” en la página 440. Si la gestión entre redes va a unirse a Internet, también deberá seguir las instrucciones del apartado “Números de sistema autónomo” en la página 443.

Tabla 79. Configuración de tareas de pasarela

Tarea	Vía rápida de SMIT	Archivo de mandatos
Visualización de la tabla de direccionamiento	smit lsroute	<a href="#">netstat</a> <sup>1</sup>

Tabla 79. Configuración de tareas de pasarela (continuación)

Tarea	Vía rápida de SMIT	Archivo de mandatos
Adición de una ruta estática	smit mkroute	<b>route add destino pasarela<sup>2</sup></b>
Eliminación de una ruta estática	smit rmroute	<b>route delete destino pasarela<sup>2</sup></b>
Desechar tabla de direccionamiento	smit fshrttbl	<b>route flush</b>

**Nota:**

1. La tabla se divide en columnas para la dirección de destino, la dirección de pasarela, los distintivos, la cuenta de referencias (cuenta de saltos) y la interfaz de red. Si las tramas no alcanzan su destino y las tablas de direccionamiento indican la ruta correcta, es posible que existan una o varias de las condiciones siguiente:
  - La red falla.
  - El sistema principal remoto o la pasarela falla.
  - El sistema principal remoto o la pasarela están inactivos o no preparados para recibir tramas.
  - El sistema principal remoto no tiene una ruta de retorno a la red de origen.
2. El valor de *destino* es la dirección decimal con puntos o el nombre simbólico de la red o del sistema principal de destino y el valor de *pasarela* es la dirección decimal con puntos o el nombre simbólico de la pasarela. (Una ruta predeterminada especifica 0 como destino.)

**Restricciones de uso de rutas**

Las rutas se pueden restringir para que sólo las pueda utilizar algunos usuarios. Las restricciones se basan en los ID de grupo primario de usuarios.

Mediante el mandato **route**, puede especificar una lista de un máximo de 32 ID de grupo que estén autorizados o no estén autorizados a utilizar una ruta. Si la lista es de grupos autorizados, cualquier usuario que pertenezca a cualquier grupo de la lista podrá utilizar la ruta. Si la lista es de grupos no autorizados, sólo los usuarios que no pertenezcan a cualquiera de los grupos de la lista podrán utilizar la ruta. El usuario root puede utilizar cualquier ruta.

Los grupos también se pueden asociar con una interfaz utilizando el mandato **ifconfig**. En este caso, un paquete que se pueda reenviar puede utilizar cualquier ruta autorizada para los grupos asociados con la interfaz de entrada.

Si hay dos o más rutas al mismo destino, cualquier redirección ICMP que se reciba para dicho destino se ignorará y el descubrimiento de MTU de vía de acceso no se realizará en esas rutas.

**Detección de pasarela muerta**

Un sistema principal se puede configurar para que detecte si una pasarela que utiliza está inactiva, y puede ajustar la tabla de direccionamiento de acuerdo a ello.

Si la opción de red **-passive\_dgd** es 1, se habilita la detección de pasarela muerta pasiva para el sistema entero. Si no se recibe ninguna respuesta para solicitudes **ARP dgd\_packets\_lost** consecutivas a una pasarela, se presupone que dicha pasarela está inactiva y que las métricas de distancia (también conocidas como *hopcount* o *cost*) para todas las rutas que utilizan esa pasarela se elevan al valor máximo posible. Después de **dgd\_retry\_time** minutos hayan pasado, los costes de la ruta se restauran a los valores configurados por el usuario. El sistema principal también realiza la acción basándose en las conexiones **TCP** anómalas. Si se pierden paquetes **dgd\_packets\_lost** de **TCP**, la entrada **ARP** para la pasarela en uso se suprime y la conexión **TCP** intenta la mejor ruta siguiente. La siguiente vez que se utilice la pasarela, las acciones anteriores tendrán lugar si la pasarela está realmente inactiva. Los parámetros **passive\_dgd**, **dgd\_packets\_lost** y **dgd\_retry\_time** se pueden configurar utilizando el mandato **no**.

Los sistemas principales también se pueden configurar para utilizar la detección activa de pasarela muerta en cada ruta con el distintivo **-active\_dgd** del mandato **route**. La detección de pasarela no

operativa activa hace ping en todas las pasarelas utilizadas por las rutas para las que se habilita cada segundo **dgd\_ping\_time**. Si no se recibe ninguna respuesta de una pasarela, se hace ping en ella más rápidamente hasta un máximo de **dgd\_packets\_lost** veces. Si se sigue sin recibir respuesta, se elevarán los costes de todas las rutas que utilizan esa pasarela. Se continúa haciendo ping en la pasarela y si finalmente se recibe una respuesta, los costes de las rutas se restauran a los valores configurados por el usuario. El parámetro **dgd\_ping\_time** se puede configurar utilizando el mandato **no**.

La detección de pasarela no operativa es más útil para sistemas principales que utilizan el direccionamiento estático en lugar del dinámico. La detección de pasarela no operativa pasiva da como resultado menos problemas de rendimiento y se recomienda utilizarla en cualquier red que tenga pasarelas redundantes. Sin embargo, la detección pasiva de pasarela muerta se realiza sólo para llevar a cabo el esfuerzo óptimo. Algunos protocolos, por ejemplo **UDP**, no proporcionan ninguna información de retorno al sistema principal si falla una transmisión de datos y, en este caso, la detección pasiva de pasarela muerta no puede realizar ninguna acción.

La detección activa de pasarela muerta es muy útil cuando un sistema principal debe descubrir inmediatamente cuándo se desactiva una pasarela. Dado que consulta cada pasarela para la que está habilitado cada pocos segundos, existe algún exceso de uso de red asociado con su uso. Sólo se recomienda la detección activa de pasarela muerta para sistemas principales que proporcionan servicios críticos y en redes con un número limitado de sistemas principales.

**Nota:** La detección de pasarela no operativa y los protocolos de direccionamiento que utilizan los daemons **gated** y **routed** realizan una función similar descubriendo cambios en la configuración de red y ajustando la tabla de direccionamiento de acuerdo a ello. Sin embargo, para ello utilizan distintos mecanismos, y si se ejecutan al mismo tiempo, es posible que entren en conflicto entre ellos. Por este motivo, la detección de pasarela no operativa no se debe utilizar en sistemas que ejecutan los daemons **gated** o **routed**.

Cuando la detección de pasarela no operativa detecta que la ruta primaria vuelve a estar en línea y que el parámetro **dgd\_flush\_cached\_route** está habilitado, se desecharán las rutas en memoria caché actuales de todas las conexiones activas. Las rutas de todas las conexiones activas actuales se validarán de nuevo, para buscar la mejor ruta para el envío de datos. Se puede configurar el parámetro **dgd\_flush\_cached\_route**, utilizando el mandato **no**. De forma predeterminada, se inhabilitará el parámetro **dgd\_flush\_cached\_route**.

**Nota:** Se debe habilitar el parámetro **dgd\_flush\_cached\_route** sólo en un entorno de red estable. De lo contrario, es posible que haya mayores problemas de rendimiento debido a direccionadores de hardware incorrectos o inestables, lo que hace que la detección de pasarela no operativa actualice frecuentemente la tabla de direccionamiento. El vaciado frecuente de las rutas en memoria caché también puede ser caro.

### Réplica de ruta

La réplica de ruta permite crear una ruta de sistema principal para cada sistema principal con el que se comunica un sistema.

Cuando se está a punto de enviar tráfico de red, se realiza una búsqueda de la tabla de direccionamiento para buscar una ruta a dicho sistema principal. Si se encuentra una ruta de sistema principal específica, se utiliza ésta. Si no se encuentra una ruta de sistema principal específica, se puede encontrar una ruta de red o la ruta predeterminada. Si la ruta que se encuentra tiene establecido el distintivo de réplica 'c', se creará una ruta de sistema principal para el destino utilizando la pasarela de la ruta que se está replicando. Las búsquedas subsiguientes tabla de direccionamiento de ese destino encontrarán la ruta de sistema principal replicada. Las rutas replicadas tienen establecido el distintivo 'W'. Estas rutas excederán el tiempo de espera y se suprimirán de la tabla de direccionamiento si no se utilizan durante *caducidad\_ruta* minutos. Puede modificar *caducidad\_ruta* utilizando el mandato **no**.

La característica de réplica de ruta la utiliza principalmente el protocolo de descubrimiento de MTU de vía de acceso dentro del sistema operativo AIX, para permitirle hacer el seguimiento de la información de MTU de vía de acceso para cada destino con el que se comunica. Si las opciones de red **tcp\_pmtu\_discover** o **udp\_pmtu\_discover** (que se pueden establecer con el mandato **no**) son 1, el distintivo de réplica se activa para todas las rutas de red del sistema. El protocolo de descubrimiento de MTU de vía de acceso está activo de forma predeterminada.

**Nota:** Para añadir manualmente una entrada de ruta de réplica, puede manipular la tabla de direccionamiento a través del mandato **route**.

## Información relacionada

### mandato route

#### Eliminación de rutas dinámicas

Si se utiliza el daemon **routed**, una ruta suprimida manualmente *no* se sustituye por la información RIP de entrada (porque se utilizan ioctl).

Si se utiliza el daemon **gated** y no se utiliza el distintivo **-n**, la ruta suprimida manualmente *sí* se sustituye por la ruta tal como se descubre en la información RIP de entrada.

#### Configuración del daemon routed

Siga estos pasos para configurar el daemon **routed**.

Para configurar el daemon **routed**:

1. Elimine el símbolo de comentario (#) y modifique la cláusula **routed** en el script de shell /etc/rc.tcpip.

Esto inicia automáticamente el daemon **routed** con cada arranque de sistema.

- Especifique si desea que la pasarela se ejecute en modalidad activa (distintivo **-s**) o pasiva (distintivo **-q**).
- Especifique si desea que el rastreo de paquetes esté activado o desactivado (distintivo **-t**). El rastreo de paquetes también se puede activar después de que el daemon **routed** ya se haya iniciado utilizando el mandato **kill** para enviar una señal **SIGUSR1** al daemon. Esta señal también se puede utilizar para incrementar el nivel de rastreo a través de cuatro niveles. Además, el rastreo de paquetes se puede desactivar mientras se ejecuta el daemon **routed** utilizando el mandato **kill** para enviar una señal **SIGUSR2** al daemon. Para obtener más información, consulte el daemon **routed** y el mandato **kill**.
- Especifique si desea que la depuración está activada o desactivada (distintivo **-d**). Si utiliza este distintivo, especifique en qué archivo de registro cronológico desea que se almacene la información de depuración o elija que se esta información se direccione a la pantalla de consola.
- Especifique si está ejecutando el daemon **routed** en una pasarela (distintivo **-g**).

- Nota:** Un sistema principal que no es una pasarela puede ejecutar el daemon **routed**, pero se debe ejecutar en modalidad pasiva.
2. Identifique los métodos conocidos listándolos en el archivo /etc/networks.

Consulte [Networks File Format for TCP/IP](#) en la publicación *Referencia de archivos* para obtener más información. Encontrará un archivo networks de ejemplo en el directorio /usr/samples/tcpip.

3. Configure rutas en el archivo /etc/gateways a las pasarelas conocidas que no estén directamente conectadas a la red.

Consulte [Gateways File Format for TCP/IP](#) en la publicación *Referencia de archivos* para ver ejemplos detallados de las entradas del archivo /etc/gateways. Encontrará un archivo gateways de ejemplo en el directorio /usr/samples/tcpip.

 **Atención:** No ejecute el daemon **routed** y el daemon **gated** en la misma máquina. Esta acción puede tener resultados imprevisibles.

#### Configuración del daemon gated

Al configurar el daemon **gated**, debe decidir qué protocolos de pasarela son más apropiados para el sistema.

Para configurar el daemon **gated**:

1. Decida qué protocolos de pasarela son los más apropiados para el sistema.

Las opciones para los protocolos de direccionamiento son **EGP**, **BGP**, **RIP**, **RIPng**, **HELLO**, **OSPF**, **ICMP/Router Discovery** e **IS-IS**. También puede utilizar **SNMP**, un protocolo que le permite cambiar o mostrar información de gestión para un elemento de red desde un sistema principal remoto.

**Nota:** Utilice **EGP**, **BGP** o **BGP4+** para anunciar direcciones de redes de un sistema autónomo en pasarelas de otros sistemas autónomos. Si está en Internet, se debe utilizar **EGP**, **BGP** o **BGP4+** para anunciar la posibilidad de red para alcanzar el sistema de pasarela central. Utilice los protocolos de direccionamiento interiores para anunciar la información de alcance en sistema autónomos.

2. Identifique los métodos conocidos listándolos en el archivo /etc/networks.

Consulte [Networks File Format for TCP/IP](#) en la publicación *Referencia de archivos* para obtener más información. Encontrará un archivo networks de ejemplo en el directorio /usr/samples/tcpip.

3. Edite el archivo /etc/gated.conf para reflejar la configuración deseada del daemon **gated**.

**Nota:** La versión de gated Daemon en AIX 4.3.2 y superior es 3.5.9. La sintaxis del archivo /etc/gated.conf ha cambiado. Los ejemplos proporcionados más abajo son para la versión 3.5.9 de **gated**. Para configurar el archivo /etc/gated.conf para versiones anteriores a AIX 4.3.2, utilice la sintaxis proporcionada en el propio archivo /etc/gated.conf.

- Especifique el nivel de salida de rastreo que desea. Si se necesita utilizar el rastreo antes de que se utilice el archivo gated.conf, use el distintivo **-t** para activar el rastreo cuando se inicie el daemon.

- Especifique los protocolos de direccionamiento que desea utilizar.

Cada protocolo tiene su propia sentencia de protocolo. Elimine los símbolos de comentario (#) y modifique las sentencias correspondientes a los protocolos que desea utilizar.

- Si utiliza **EGP**:

- Configure la cláusula **EGP autonomousystem**. Obtenga un número de sistema autónomo de la autoridad de Internet si está en Internet o, si no lo está, asigne un número de sistema autónomo teniendo en cuenta los números de sistema autónomo de otros sistemas de la red.
- Establezca la sentencia **EGP** en yes.
- Configure una cláusula **group** para cada sistema autónomo.
- Configure una cláusula **neighbor** para cada vecino de ese sistema autónomo. Por ejemplo:

```
autonomousystem 283 ;  
  
egp yes {  
    group maxup 1 {  
        neighbor nogendefault 192.9.201.1 ;  
        neighbor nogendefault 192.9.201.2 ;  
    } ;  
    group {  
        neighbor 192.10.201.1 ;  
        neighbor 192.10.201.2 ;  
    } ;  
};
```

- Si utiliza **RIP** o **HELLO**:

- Establezca la sentencia **RIP** o **HELLO** en yes.
- Especifique nobroadcast en la sentencia **RIP** o **HELLO** si desea que la pasarela sólo acepte información de direccionamiento, no información de difusión. O especifique broadcast en la sentencia **RIP** o **HELLO** si desea que la pasarela difunda información de direccionamiento y que acepte información de direccionamiento.
- Si desea que la pasarela envíe directamente a las pasarelas de origen, utilice la sentencia **sourcегateways**. Especifique un nombre de pasarela o una dirección de Internet en anotación decimal con puntos en la cláusula sourcегateways. Por ejemplo:

```
# Enviar directamente a pasarelas específicas  
  
rip/Hello yes {  
    sourcегateways  
        101.25.32.1  
        101.25.32.2 ;  
};
```

El ejemplo siguiente muestra la stanza **RIP/HELLO** del archivo `gated.conf` de una máquina que no envía paquetes **RIP** y no recibe paquetes **RIP** en la interfaz `tr0`.

```
rip/Hello nobroadcast {  
    interface tr0 noripin ;  
};
```

- Si utiliza **BGP**:

- Configure la cláusula **BGP** `autonomoussystem`. Obtenga un número de sistema autónomo de la autoridad de Internet si está en Internet o, si no lo está, asigne un número de sistema autónomo teniendo en cuenta los números de sistema autónomo de otros sistemas de la red.
- Establezca la sentencia **BGP** en `yes`.
- Configure una cláusula `peer` para cada vecino de ese sistema autónomo. Por ejemplo:

```
# Realizar todas las operaciones de BGP  
bgp yes {  
    peer 192.9.201.1 ;  
};
```

- Si utiliza **SNMP**:

- Establezca la sentencia **SNMP** en `yes`.

```
snmp yes ;
```

### *Configuración del daemon gated para ejecutar IPv6*

Utilice este procedimiento para configurar el daemon **gated** para ejecutar **Internet Protocol versión 6 (IPv6)**.

Para configurar el daemon **gated** para ejecutar bajo **Internet Protocol versión 6 (IPv6)**, asegúrese de que el sistema se ha configurado para el direccionamiento de **IPv6** e **IPv6**:

1. Ejecute **autoconf6** para configurar automáticamente las interfaces para **IPv6**.
2. Configure las direcciones locales de sitio para cada interfaz **IPv6** en la que desee utilizar el direccionamiento de **IPv6** utilizando el mandato siguiente:

```
ifconfig interfaz inet6 fec0:n::dirección/64 alias
```

donde

**interfaz**

Es el nombre de interfaz, por ejemplo `tr0` o `en0`.

**n**

Es cualquier número decimal; por ejemplo `11`

**dirección**

Es la parte de la dirección de interfaz **IPv6** que sigue a los dos puntos dobles; por ejemplo, dada la dirección **IPv6** `fe80::204:acff:fe86:298d`, la entrada de **dirección** será `204:acff:fe86:298d`.

**Nota:** Puede utilizar el mandato **netstat -i** para ver cuál es la dirección **IPv6** para cada interfaz configurada.

Si la Red en anillo `tr0` tiene una dirección **IPv6** de `fe80::204:acff:fe86:298d`, emita el siguiente mandato:

```
ifconfig tr0 inet6 fec0:13::204:acff:fe86:298d/64 alias
```

3. Active el reenvío de **IPv6** con el mandato siguiente:

```
no -o ip6forwarding=1
```

4. Inicie **ndpd-router** con el mandato siguiente:

```
ndpd-router -g
```

El inicio de **ndpd-router** permite al sistema actuar como un direccionador para **Neighbor Discovery Protocol**. Los direccionadores de **Neighbor Discovery Protocol** proporcionan a los sistemas principales de descubrimiento de vecinos información de direccionamiento para que los sistemas principales puedan direccionar paquetes **IPv6**.

Cualquier sistema principal de la red que desee que forme parte de la red **IPv6** debe ejecutar **ndpd-host**. Los sistemas principales de la red que ejecutan **ndpd-host** se reconocerán a sí mismos como parte de una red **IPv6** y utilizarán el **Neighbor Discovery Protocol**, que les permitirá determinar y supervisar las direcciones de capa de enlace para permitir el direccionamiento de vecinos y para buscar direccionadores de vecinos para el reenvío de paquetes.

5. A continuación, configure el daemon **gated**:

- Decida qué protocolos de pasarela **IPv6** son los más apropiados para el sistema.

Las opciones para los protocolos de direccionamiento **IPv6** son **Border Gateway Protocol** mejorado para **IPv6 (BGP4+)** y **Routing Information Protocol Next Generation (RIPng)**.

- Edite el archivo `/etc/gated.conf` para reflejar la configuración deseada del daemon **gated**.

**Nota:** AIX 4.3.2 y posteriores ejecutan **gated** versión 3.5.9. La sintaxis del archivo `gated.conf` ha cambiado ligeramente respecto a las versiones anteriores. Consulte la documentación de `gated.conf` en *Files Reference* o utilice el archivo de ejemplo del directorio `/usr/sample/tcpip` para una sintaxis correcta.

Al configurar **BGP4+** o **RIPng**, utilice las direcciones **IPv6** en las que la sintaxis especifica una dirección IP.

**Nota:** De forma predeterminada, **RIPng** difunde forma múltiple los paquetes.

Después de que el archivo `/etc/gated.conf` se haya modificado, se puede iniciar el daemon **gated**.

#### Números de sistema autónomo

Si utiliza **EGP** o **BGP**, deberá obtener un *número de sistema autónomo* oficial para la pasarela.

Para obtener un número de sistema autónomo oficial, póngase en contacto con el NIC en la siguiente dirección de internet:

INFO@INTERNIC.NET

## IPv6 móvil

**IPv6** móvil proporciona soporte de movilidad para **IPv6**. Le permite conservar la misma dirección de internet en todo el mundo y permite a las aplicaciones que utilizan dicha dirección mantener conexiones de capa superior y de transporte al cambiar de ubicaciones. Permite tener movilidad en soportes homogéneos y heterogéneos.

Por ejemplo, **IPv6** móvil facilita el movimiento de nodos de un segmento Ethernet a una célula de LAN inalámbrica mientras que la dirección IP del nodo móvil se queda como estaba.

En **IPv6** móvil, cada nodo móvil se identifica por dos direcciones IP: la dirección inicial y la dirección de atención. La dirección inicial es una dirección IP permanente que identifica el nodo móvil independientemente de la ubicación. La dirección de atención cambia en cada nuevo punto de conexión y proporciona información sobre la situación actual del nodo móvil. Cuando un nodo móvil llega a una red visitada, debe adquirir la dirección de atención, que se utilizará durante el tiempo que el nodo móvil esté bajo esta ubicación en la red visitada. Puede utilizar los métodos de Descubrimiento de vecino de **IPv6** para obtener la dirección de atención (consulte el apartado “[Rutas y direcciones ampliadas de IPv6](#)” en la [página 132](#)). Son posibles ambas configuraciones automáticas sin estado y de estado completo. La dirección de atención también se puede configurar manualmente. El modo en que se adquiere la dirección de atención es irrelevante para **IPv6** móvil.

Debe haber como mínimo un agente inicial configurado en la red inicial y el nodo móvil debe estar configurado para conocer la dirección IP del agente inicial. El nodo móvil envía un paquete que contiene una actualización de vinculación al agente inicial. El agente inicial recibe el paquete y realiza una asociación entre la dirección inicial en el nodo móvil y la dirección de atención que ha recibido. El agente inicial responde con un paquete que contiene un reconocimiento de vinculación.

El agente inicial mantiene una antememoria de vinculación que contiene asociaciones entre las direcciones iniciales y las direcciones de atención para los nodos móviles que sirve. El agente inicial intercepta los paquetes destinados a la dirección inicial y los reenvía a los nodos móviles. A continuación un nodo móvil enviará una actualización de vinculación al nodo correspondiente informándole de la dirección de atención y el nodo correspondiente creará una entrada de antememoria de vinculación para poder enviar el tráfico futuro directamente al nodo móvil en la dirección de atención.

El soporte de movilidad de AIX proporciona las funciones básicas siguientes:

#### Como nodo de **Agente inicial**:

- Mantener una entrada en la antememoria de vinculación para cada nodo móvil para el que está sirviendo.
- Interceptar los paquetes direccionados a un nodo móvil al que está sirviendo actualmente como agente inicial, en el enlace inicial del nodo móvil, mientras el nodo móvil está fuera del inicio.
- Encapsular los paquetes interceptados de este tipo a fin de transferirlos por un túnel a la dirección de atención primaria para el nodo móvil indicado en la vinculación de la antememoria de vinculación del agente inicial.
- Devolver una opción de reconocimiento de vinculación en respuesta a una opción de actualización de vinculación recibida con el conjunto de bits de reconocimiento.
- Procesar la Detección de dirección duplicada en la dirección de atención del nodo móvil para asegurar que las direcciones de **IPv6** son exclusivas.
- Soportar el Descubrimiento de direcciones de agente inicial dinámico para ayudar a los nodos móviles a descubrir las direcciones de los agentes iniciales.
- Soportar la recepción de la Solicitud de prefijo móvil y el envío del Anuncio de prefijo móvil.

#### Como nodo **correspondiente estacionario**:

- Procesar una opción de dirección inicial recibida en cualquier paquete **IPv6**
- Procesar una opción de actualización de vinculación recibida en un paquete y devolver una opción de reconocimiento de vinculación si el bit de reconocimiento (A) se establece en la actualización de vinculación recibida
- Mantener una antememoria de las vinculaciones recibidas en actualizaciones de vinculación aceptadas
- Enviar paquetes utilizando una cabecera de direccionamiento cuando hay una entrada de antememoria de vinculación para un nodo móvil que contiene la dirección de atención actual del nodo móvil

#### Como nodo de **Direccionador** en una red visitada por el nodo móvil:

- Enviar una opción de intervalo de anuncio en los anuncios de direccionador para ayudar a que los nodos móviles detecten movimiento. Se puede configurar con el parámetro **-m** en el daemon **ndpd-router**.
- Soportar el envío de anuncios de direccionador multidifusión no solicitados a la velocidad más rápida descrita en RFC 2461. Se puede configurar con los parámetros **-m** y **-D** en el daemon **ndpd-router**.
- Enviar una opción de Información de agente inicial (preferencia de agente inicial y tiempo de vida) en los anuncios de direccionador para ayudar a los nodos móviles a elegir el agente inicial. Se puede configurar con el parámetro **-H** en el daemon **ndpd-router**.

#### **Seguridad de IPv6 móvil**

Los mensajes de reconocimiento de vinculación y actualización de vinculación intercambiados entre el nodo móvil y el agente inicial se deben proteger mediante la Seguridad IP utilizando la protección ESP (Encapsulating Security Payload) con un algoritmo de autentificación de carga no NULL.

Para obtener más información sobre seguridad IP, consulte el apartado [Security](#).

El establecimiento de vinculación entre el nodo móvil y el nodo correspondiente se hace seguro utilizando el procedimiento de Direccionamiento de retorno. En este procedimiento, los mensajes que se intercambian entre el nodo de agente inicial y los nodos móviles se deben proteger mediante la seguridad IP utilizando ESP. Puesto que los mensajes de actualización de vinculación y de reconocimiento de vinculación intercambiados entre un nodo correspondiente y un nodo móvil están protegidos por el procedimiento de Direccionamiento de retorno, no hay requisitos de seguridad IP para los correspondientes. Pero, si un correspondiente utiliza la seguridad IP para restringir el acceso, se deben permitir los mensajes con el protocolo MH (135).

Se pueden definir túneles manualmente o utilizando IKE que actúe como respondedor (sólo se soporta la modalidad agresiva). Como mínimo, se definirán los siguientes túneles de seguridad IP en el agente inicial utilizando la cabecera ESP:

- un túnel en modalidad de transporte con el protocolo MH (135) entre la dirección IP de agente inicial y la dirección inicial de cada nodo móvil susceptible de registrarse en este agente inicial.
- un túnel en modalidad de túnel con el protocolo MH (135) entre cualquier dirección IP y la dirección inicial de cada nodo móvil susceptible de registrarse en este agente inicial.

Se deben definir túneles correspondientes en los nodos móviles.

**Nota:** Los mensajes de actualización de vinculación y de reconocimiento de vinculación se envían utilizando una cabecera de movilidad y se deben proteger mediante la seguridad IP utilizando ESP.

En implementaciones anteriores de IPv6 móvil en AIX, se proporcionaba soporte para los nodos móviles utilizando paquetes de opciones de destino para enviar mensajes de actualización de vinculación. Estos mensajes se podían proteger con la seguridad IP utilizando una cabecera de autentificación.

Para que un agente inicial o un nodo correspondiente acepte tales mensajes de actualización de vinculación utilizando una opción de destino, edite el archivo `/etc/rc.mobip6` y habilite la variable **Enable\_Draft13\_Mobile** antes de iniciar **IPv6** móvil. En este caso, si utiliza la seguridad IP para proteger los mensajes de actualización de vinculación, debe definir túneles manuales o IKE en modalidad de transporte en el protocolo 60, lo que protegerá los mensajes de reconocimiento y actualización de vinculación.

Para que un agente inicial o un nodo correspondiente acepte tales mensajes de actualización de vinculación no protegidos por la seguridad IP, edite el archivo `/etc/rc.mobip6` e inhabilite la variable **Check\_IPsec**. Este método no se recomienda porque presenta una vulnerabilidad significativa de la seguridad por la posibilidad de afectar el direccionamiento de paquetes dirigidos a un nodo móvil.

### Configuración de IPv6 móvil

Presenta información sobre la configuración de **IPv6** móvil. Para utilizar **IPv6** móvil, primero debe instalar el catálogo de archivos `bos.net.mobip6.rte`.

Para obtener información sobre cómo instalar catálogos de archivos, consulte el apartado que trata sobre la Instalación opcional de productos de software y las actualizaciones de servicio en la publicación *Installation and migration*

#### *Inicio de IPv6 móvil como agente inicial*

Utilice este procedimiento para iniciar **IPv6** móvil como agente inicial.

1. Defina túneles IKE (fases 1 y 2) como respondedores utilizando el protocolo **ESP** o IP Security Association de ESP manual entre la dirección IP de agente inicial y cada dirección inicial móvil con la que se puede comunicar el nodo correspondiente.
2. Habilite el sistema como un agente inicial **IPv6** móvil y el nodo correspondiente. En la línea de mandatos, escriba `smit enable_mobip6_home_agent`.
3. Seleccione cuándo desea que se habilite.

#### *Inicio de IPv6 móvil como nodo correspondiente*

Utilice este procedimiento para iniciar IPv6 móvil como nodo correspondiente.

1. Defina túneles IKE (fases 1 y 2) como respondedores utilizando el protocolo **ESP** o IP Security Association de ESP manual entre la dirección IP de agente inicial y cada dirección inicial móvil con la que se puede comunicar el nodo correspondiente.
2. Habilite el sistema como nodo **IPv6** móvil correspondiente. En la línea de mandatos, escriba smit enable\_mobip6\_correspondent.
3. Seleccione cuándo desea que se habilite.

#### **Inicio de Mobile IPv6 como direccionador**

Utilice este procedimiento para iniciar Mobile **IPv6** como direccionador.

Ejecute el mandato siguiente para facilitar la detección de movimiento:

```
ndpd-router -m
```

#### **Detención de Mobile IPv6**

Utilice este procedimiento para detener Mobile **IPv6**.

1. Escriba smit disable\_mobip6 en la línea de mandatos.
2. Seleccione cuándo desea que se detenga Mobile **IPv6**.
3. Seleccione si desea detener el daemon **ndpd-router**.
4. Seleccione si desea inhabilitar el reenvío de **IPv6**.

#### **Resolución de problemas de Mobile IPv6**

Utilice el mandato **mobip6ctrl -b** para solucionar problemas de Mobile **IPv6**.

1. Obtenga los estados de enlace ejecutando lo siguiente:

```
mobip6ctrl -b
```

2. Consulte el apartado “Resolución de problemas de TCP/IP” en la página 497 para obtener información sobre cómo utilizar los programas de utilidad de resolución de problemas de **TCP/IP**.

## **Dirección IP virtual**

Una dirección IP virtual elimina la dependencia de un sistema principal de las interfaces de red individuales.

Los paquetes de entrada se envían a la dirección VIPA del sistema, pero todos los paquetes viajan a través de las interfaces de red reales.

Anteriormente, si fallaba una interfaz, se perdían las conexiones a dicha interfaz. Con VIPA en el sistema y los protocolos de direccionamiento en la red proporcionando el redireccionamiento automático, la recuperación de anomalías se produce sin interrupciones en las conexiones de usuario existentes que utilizan la interfaz virtual porque los paquetes largos pueden llegar a través de otra interfaz física. Los sistemas que ejecutan VIPA están mucho más disponibles porque las interrupciones de adaptador ya no afectan a las conexiones activas. Dado que varios adaptadores físicos transportan el tráfico IP de sistema, la carga general no se concentra en un solo adaptador y la subred asociada.

La función VIPA de AIX es transparente en el equipo de red. No se necesita ningún equipo de red especial ni otro hardware. Para implementar VIPA, necesita tener los elementos siguientes:

- dos o más interfaces IP existentes de cualquier tipo físico en subredes diferentes que se conectan en la red de empresa
- protocolos de direccionamiento IP que se ejecutan en la red de empresa

#### **Configuración de VIPA**

VIPA se configura en SMIT como cualquier interfaz de red IP. Además, puede especificar un grupo de interfaces mientras configura VIPA.

Cuando se configura de este modo, para todas las conexiones de salida iniciadas por el sistema principal VIPA a través de estas interfaces, que se han designado para utilizar una VIPA, la dirección virtual se convierte en la dirección de origen colocada en la cabecera de paquete **TCP/IP** de los paquetes de salida.

1. Para un VIPA IPv4, escriba smit mkinetvi en la línea de mandatos. Para un VIPA IPv6, escriba smit mkinetvi6 en la línea de mandatos.
2. Cumplimente los campos correspondientes. Para obtener más información, consulte el apartado “Entorno VIPA de ejemplo” en la página 447. Pulse Intro.

### **Adición de un adaptador a una VIPA**

Utilice este procedimiento para añadir un adaptador a una dirección IP virtual.

Para añadir un adaptador a una interfaz VIPA, siga estos pasos:

1. Escriba smit chvi en la línea de mandatos.
2. Seleccione la VIPA a la que desee añadir un adaptador y pulse Intro.
3. Entre el adaptador que desee añadir en el campo **Nombre(s) de interfaz**.
4. Escriba AÑADIR en el campo **AÑADIR/ELIMINAR interfaz (interfaces)** y pulse Intro.

### **Eliminación de un adaptador de una VIPA**

Utilice este procedimiento para eliminar un adaptador de una dirección IP virtual.

Para eliminar un adaptador de una VIPA, siga estos pasos:

1. Escriba smit chvi en la línea de mandatos.
2. Seleccione la VIPA de la que desea eliminar un adaptador y pulse Intro.
3. Entre el adaptador que desea eliminar en el campo **Nombre(s) de interfaz**.
4. Escriba ELIMINAR en el campo **AÑADIR/ELIMINAR interfaz (interfaces)** y pulse Intro.

### **Entorno VIPA de ejemplo**

El siguiente entorno VIPA de ejemplo con conexiones Ethernet incluye un sistema con una dirección IP virtual y dos conexiones físicas.

Un sistema tiene una dirección IP virtual, vi0, de 10.68.6.1 y dos conexiones físicas, en1 con la dirección IP 10.68.1.1 y en5, con la dirección IP 10.68.5.1. En este ejemplo, ambas conexiones físicas son Ethernet, pero se soportará cualquier combinación de interfaces IP, por ejemplo Red en anillo o FDDI, a condición de que las subredes se conecten finalmente a una red corporativa mayor y que se conozcan en otros direccionadores corporativos.

La ejecución del mandato **lsattr -El vi0** produce los siguientes resultados:

netaddr	10.68.6.1	N/A	Verdadero
state	up	Interfaz de red Ethernet estándar	Verdadero
netmask	255.255.255.0	Tamaño máximo de paquete IP para este dispositivo	Verdadero
netaddr6		Tamaño máximo de paquete IP para redes REMOTAS	Verdadero
alias6		Dirección de Internet	Verdadero
prefixlen		Estado actual de la interfaz	Verdadero
alias4		Encapsulación de nivel de enlace DE COLA	Verdadero
interface_names	en1,en5	Interfaces que utilizan la dirección virtual	Verdadero

La ejecución del mandato **ifconfig vi0** produce los resultados siguientes:

```
vi0: flags=84000041<UP,RUNNING,64BIT>
      inet 10.68.6.1 netmask 0xffffffff00
          iflist : en1 en5
```

La ejecución del mandato **netstat -rn** produce los resultados siguientes:

Destino	Pasarela	Distint.	Ref.	Uso	Si	PMTU	Grupos	Exp
Árbol de ruta para la familia de protocolos 2 (Internet):								
default	10.68.1.2	UG	3	1055	en1	-	-	-
10.68.1/24	10.68.1.1	U	0	665	en1	-	-	-
10.68.5/24	10.68.5.1	U	0	1216	en5	-	-	-
127/8	127.0.0.1	U	4	236	lo0	-	-	-
10.68.6.1	127.0.0.1	UH	0	0	lo0	-	-	-

Los paquetes de salida que no tienen una dirección de origen establecida y que se direccionan a través de las interfaces en1 y en5 tendrán la dirección de origen establecida en la dirección virtual (10.68.6.1). Los paquetes de entrada se direccionan a la dirección VIPA (10.68.6.1) anunciada en la red. Dado que vi0 es virtual (es decir, no está asociado a ningún dispositivo) no deberá haber entradas para el mismo en la tabla de direccionamiento de todo el sistema visualizada utilizando el mandato **netstat -rn**. Esto significa que no se añade ninguna ruta de interfaz cuando la interfaz se configura en SMIT.

Si falla una de las interfaces físicas, una conexión de red o una vía de acceso de red, los protocolos de red se direccionan a la otra interfaz física del mismo sistema. Si un sistema remoto utiliza telnet en la dirección vi0, los paquetes en vi0 pueden llegar utilizando en1 o en5. Si en1 está inactivo, por ejemplo, los paquetes aún pueden llegar en en5. Tenga en cuenta que los protocolos de direccionamiento pueden tardar tiempo en propagar las rutas.

Cuando se utiliza VIPA, los sistemas finales y los direccionadores que intervienen deben poder direccionar los paquetes destinados para VIPA (vi0) a una de las interfaces físicas (en1 o en5).

### **VIPA frente a alias**

El concepto VIPA es similar a los alias de IP excepto en que las direcciones no se asocian con una interfaz de hardware.

VIPA ofrece varias ventajas que no ofrecen los alias de IP:

- VIPA ofrece un dispositivo virtual que se puede arrancar y detener de forma independiente sin que ello afecte a las interfaces físicas
- Las direcciones de VIPA se pueden cambiar mientras que los alias sólo se pueden añadir o suprimir

### **Acceso utilizando la dirección IP de los adaptadores reales**

Las interfaces individuales aún son accesibles para otros sistemas después de que se haya implementado VIPA. Sin embargo, la utilización de las direcciones IP reales para sesiones ping y telnet evita la ventaja de VIPA de comunicarse de forma independiente de los adaptadores físicos. VIPA oculta las anomalías de adaptador físico a los clientes externos. La utilización de las direcciones reales reintroduce la dependencia de los adaptadores físicos.

Si un sistema remoto se pone en contacto con el sistema VIPA utilizando la dirección VIPA o si una aplicación del sistema VIPA inicia las comunicaciones con otro sistema, se utilizará la dirección VIPA como dirección IP de origen del paquete. Sin embargo, si el sistema remoto inicia la sesión utilizando la dirección IP de la interfaz real, esa dirección IP real será la dirección IP de origen de los paquetes de respuesta. Existe una excepción. Para aplicaciones que se enlazan a una interfaz IP determinada, los paquetes de salida llevarán la dirección de origen de la interfaz a la que están enlazadas.

### **VIPA y protocolos de direccionamiento**

El daemon gated se ha modificado para VIPA para que no añada la ruta de interfaz o envíe anuncios a través de las interfaces virtuales.

El protocolo **OSPF**, soportado por gated, anunciará la interfaz virtual a los direccionadores vecinos. Los demás sistemas principales de la red podrán comunicarse con el sistema principal VIPA mediante el direccionador de primer salto.

### **Varias direcciones VIPA**

Se pueden configurar varias interfaces virtuales. Por ejemplo, serán útiles varias interfaces VIPA si los direccionadores de red pueden dar un trato preferente a los paquetes que se envían hacia y desde determinadas direcciones VIPA.

O puede utilizar varias interfaces VIPA si éstas están enlazando aplicaciones a una interfaz VIPA específica. Por ejemplo, para ejecutar varios servidores web para varias empresas en una sola máquina, puede configurar lo siguiente:

- vi0 200.1.1.1 www.empresA.com
- vi1 200.1.1.2 www.empresB.com
- vi2 200.1.1.3 www.empresC.com

## EtherChannel, Agregación de enlaces IEEE 802.3ad, Teaming

EtherChannel, Agregación de enlaces IEEE 802.3ad y Teaming son tecnologías de agregación de puertos de red que permiten la agregación de varios adaptadores Ethernet juntos para formar un solo dispositivo pseudo Ethernet.

Por ejemplo, ent0 y ent1 se pueden agregar en un adaptador EtherChannel denominado en3; la interfaz en3 se configuraría con una dirección IP. El sistema considera estos adaptadores agregados como un solo adaptador. Por lo tanto, IP se configura a través de ellos, como cualquier adaptador Ethernet. Además, todos los adaptadores de EtherChannel o de la Agregación de enlaces tendrán la misma dirección de hardware (Mac), de forma que los sistemas remotos los traten como si fueran un solo adaptador. Tanto EtherChannel como la Agregación de enlaces IEEE 802.3ad necesitan soporte en el conmutador para que estas dos tecnologías sepan qué puertos del conmutador se deben tratar como uno.

>| En el mecanismo de agregación Teaming, cada adaptador en el canal conserva su dirección de hardware original (MAC). Por lo tanto, no es necesario configurar ningún conmutador. EtherChannel y la Agregación de enlaces IEEE 802.3ad pueden tener un canal primario y un canal de copia de seguridad. Sin embargo, el mecanismo de agregación Teaming utiliza solo un canal. Si selecciona la modalidad Teaming, no puede controlar cómo el canal envía los paquetes. El canal utiliza automáticamente la modalidad estándar para enviar paquetes. La modalidad Teaming controla qué adaptador en EtherChannel recibe tráfico para que la configuración del conmutador no sea necesaria.|<

**Nota:** El controlador EtherChannel asigna una dirección no válida de control de accesos a soporte (MAC), 02:00:00:00:00, en el puerto HEA (Host Ethernet Adapter) del canal inactivo de la configuración de EtherChannel. La dirección de MAC no válida se asigna cuando se crea EtherChannel o cuando se agregan puertos HEA en el canal inactivo en tiempo de ejecución. Durante la recuperación o migración tras error de EtherChannel, la dirección MAC no válida se intercambia por la dirección MAC válida. En tiempo de ejecución, la dirección MAC válida se intercambia por la dirección MAC no válida.

La ventaja principal de EtherChannel y de la Agregación de enlaces IEEE 802.3ad es que poseen el ancho de banda de red de todos sus adaptadores en una sola presencia en la red. Si un adaptador tiene una anomalía, el tráfico de la red se envía al siguiente adaptador disponible de forma automática, sin interrumpir las conexiones del usuario existentes. El adaptador se devuelve automáticamente al servicio del EtherChannel o la Agregación de enlaces cuando se recupera.

Existen algunas diferencias entre EtherChannel, la Agregación de enlaces IEEE 802.3ad y el mecanismo de agregación Teaming. Tenga en cuenta las diferencias que se listan en [Tabla 80 en la página 449](#) para determinar la tecnología que mejor se adapte a sus requisitos.

*Tabla 80. Diferencias entre EtherChannel, la Agregación de enlaces IEEE 802.3ad y Teaming.*

EtherChannel	Agregación de enlaces IEEE 802.3ad	> Teaming <
Requiere la configuración del conmutador.	Requiere la configuración del conmutador para el intercambio de unidad de datos del Protocolo de control de Agregación de enlaces (LACPDU).	> No requiere la configuración del conmutador. <
Las pulsaciones no se intercambian entre el puerto del conmutador y el puerto del sistema adyacente.	Las pulsaciones (LACPDU) se intercambian durante el intervalo definido por el IEEE 802.3ad estándar. Las pulsaciones proporcionan protección adicional en caso de anomalía.	> Las pulsaciones no se intercambian entre el puerto del conmutador y el puerto del sistema adyacente. <
Se pueden utilizar tanto los canales primarios como los de copia de seguridad.	Se pueden utilizar tanto los canales primarios como los de copia de seguridad.	> Sólo se utiliza un único canal (primario). <

La funcionalidad Pertenencia dinámica de los adaptadores está disponible en el sistema operativo AIX. Puede utilizar esta funcionalidad para añadir o eliminar adaptadores de un EtherChannel sin interrumpir las conexiones del usuario.

### Información relacionada

[Pertenencia dinámica de los adaptadores \(DAM\)](#)

[EtherChannel](#)

[Configuración de la Agregación de enlaces IEEE 802.3ad](#)

[Ejemplos de interoperabilidad](#)

### EtherChannel

Los adaptadores que pertenezcan a un EtherChannel deben conectarse al mismo conmutador, que debe tener habilitado el EtherChannel. Si los adaptadores están conectados a conmutadores distintos, los conmutadores se deben apilar y actuar como un solo conmutador.

Este conmutador debe configurarse manualmente para que trate los puertos que pertenecen al EtherChannel como un enlace agregado. Es posible que la documentación del conmutador haga referencia a esta función como *Agregación de enlaces* o *truncamiento*.

Para que EtherChannel funcione correctamente, el mecanismo de sondeo de enlaces que periódicamente verifica el estado de enlace se debe habilitar en cada adaptador antes de crear el EtherChannel. El tráfico se distribuye a través de los adaptadores de la forma estándar (donde el adaptador a través del cual se envían los paquetes se elige en función de un algoritmo) o según la modalidad round-robin (donde los paquetes se envían uniformemente a través de todos los adaptadores). El tráfico de entrada se distribuye de acuerdo con la configuración del conmutador y no depende de la modalidad de funcionamiento del EtherChannel.

Puede configurar varios EtherChannels por sistema. Si todos los enlaces de un EtherChannel están conectados a un único conmutador y si el conmutador está desenchufado o falla, se perderá todo el EtherChannel. Para resolver este problema, está disponible una opción de copia de seguridad que conserva el servicio activo cuando presenta una anomalía el EtherChannel principal. Los adaptadores de seguridad y de EtherChannel deben estar conectados a distintos conmutadores de red, que deben estar interconectados para que esta configuración funcione correctamente. Si todos los adaptadores del EtherChannel fallan, el adaptador de seguridad se utilizará para enviar y recibir todo el tráfico. Cuando se restablezca algún enlace en el EtherChannel, el servicio se devolverá al EtherChannel.

Por ejemplo, ent0 y ent1 se pueden configurar como los adaptadores EtherChannel principales, y ent2 como el adaptador de copia de seguridad, creando un EtherChannel denominado en3. Idealmente, ent0 y ent1 están conectados al mismo conmutador habilitado para EtherChannel, y ent2 está conectado a un conmutador distinto. En este ejemplo, todo el tráfico enviado a través de en3 (la interfaz de EtherChannel) se envía a través de ent0 o ent1 de forma predeterminada (en función del esquema de distribución de paquetes de EtherChannel), mientras que ent2 está desocupado. Si fallan en cualquier momento ent0 y ent1, todo el tráfico se enviará a través del adaptador de seguridad ent2. Cuando ent0 o ent1 se recupere, éste volverá a utilizarse para todo el tráfico.

La seguridad de la interfaz de red, una modalidad de funcionamiento disponible para EtherChannel, proporciona protección en caso de un solo punto de anomalía en la red Ethernet. No se necesita hardware especial para utilizar la seguridad de la interfaz de red, pero el adaptador de seguridad debe estar conectado a un conmutador independiente para obtener la máxima fiabilidad. En la modalidad de seguridad de la interfaz de red sólo se utiliza de forma activa un adaptador para el tráfico de red cada vez. EtherChannel prueba el adaptador actualmente activo y, opcionalmente, la vía de acceso de red en un nodo especificado por el usuario. Cuando se detecta una anomalía, se utiliza el adaptador siguiente para todo el tráfico. La modalidad de seguridad de la interfaz de red proporciona funciones de detección y recuperación tras error sin interrumpir las conexiones del usuario. La seguridad de interfaz de red se ha implementado originalmente como una modalidad en el menú de la herramienta SMIT (system management interface tool) de EtherChannel. El adaptador de seguridad proporciona la función equivalente, por lo que la modalidad se ha eliminado del menú SMIT. Para configurar la seguridad de la interfaz de red, consulte el apartado ["Configuración de la seguridad de la interfaz de red"](#) en la página 455.

## **Consideraciones sobre la configuración del EtherChannel**

Consulte la lista de recomendaciones antes de configurar el EtherChannel.

- Cada EtherChannel puede tener hasta ocho adaptadores Ethernet primarios y ocho adaptadores de seguridad.
- Es posible configurar varios EtherChannels en un solo sistema, pero cada EtherChannel constituirá una interfaz de Ethernet adicional. Puede que sea necesario aumentar la opción **ifsize** del mandato **no** para incluir no sólo las interfaces de Ethernet de cada adaptador, sino también los EtherChannels que estén configurados. En AIX 5.2 y versiones anteriores, el valor predeterminado de **ifsize** es ocho. El tamaño predeterminado es 256.
- Es posible utilizar cualquier adaptador Ethernet al que se proporcione soporte en un EtherChannel (consulte el apartado “Adaptadores soportados” en la página 468). Sin embargo, los adaptadores Ethernet deben conectarse a un conmutador que proporcione soporte al EtherChannel. Consulte la documentación que se proporciona con el conmutador para determinar si éste proporciona soporte al EtherChannel (la documentación del conmutador también puede hacer referencia a esta función como agregación de enlaces o truncamiento).
- Todos los adaptadores del EtherChannel deben configurarse con la misma velocidad (100 Mbps, por ejemplo) y en modalidad dúplex.
- El sistema no podrá acceder a los adaptadores que se utilicen en el EtherChannel una vez se haya configurado el EtherChannel. Si desea modificar alguno de sus atributos como, por ejemplo, la velocidad del soporte, el tamaño de la cola de transmisión o de recepción, etc., deberá hacerlo antes de incluirlos en el EtherChannel.
- Los adaptadores que piense utilizar para el EtherChannel no deben tener configurada una dirección IP antes de iniciar este procedimiento. Al configurar un EtherChannel con adaptadores que anteriormente se hubieran configurado con una dirección IP, asegúrese de que sus interfaces se encuentren en estado desconectado. Los adaptadores que deban añadirse al EtherChannel no pueden tener interfaces configuradas en estado activo en el Gestor de datos de objeto (ODM), lo que sucederá si las direcciones IP se han configurado utilizando SMIT. Esto puede provocar problemas al activar el EtherChannel cuando se rearranje la máquina, porque la interfaz subyacente se ha configurado antes que el EtherChannel con la información que se encuentra en el ODM. Por lo tanto, cuando EtherChannel está configurado, detecta que uno de sus adaptadores está en uso. Para cambiar esto, antes de crear el EtherChannel, escriba **smitty chinet**, seleccione cada una de las interfaces de los adaptadores que deban incluirse en el EtherChannel y cambie el valor de **estado** de las mismas a desconectar. Esto garantizará que cuando se rearranje la máquina EtherChannel pueda configurarse sin errores.

Para obtener más información acerca del ODM, consulte el apartado Object Data Manager (ODM) de la publicación *General Programming Concepts: Writing and Debugging Programs*.

- Si va a utilizar adaptadores Ethernet 10/100 en el EtherChannel para versiones de AIX anteriores a AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03., es posible que necesite habilitar el sondeo de enlaces en estos adaptadores antes de añadirlos al EtherChannel. Escriba **smitty chgenet** en la línea de mandatos. Cambie el valor de **Habilitar sondeo de enlaces** a sí y pulse Intro.

**Nota:** En AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03. y versiones posteriores, no es necesario el mecanismo de sondeo de enlaces. El sondeador de enlaces se inicia de forma automática.

- Si tiene previsto utilizar tramas de gran tamaño, es posible que necesite habilitar esta función en cada adaptador antes de crear el EtherChannel y en el propio EtherChannel. Escriba **smitty chgenet** en la línea de mandatos. Cambie el valor de **Habilitar tramas de gran tamaño** a sí y pulse Intro. Haga esto para cada adaptador para el que desee habilitar las tramas de gran tamaño. A continuación deberá habilitar las tramas de gran tamaño en el propio EtherChannel.

**Nota:** La habilitación de tramas de gran tamaño en cada adaptador subyacente no es necesario una vez que se hayan habilitado en el propio EtherChannel. La función se habilitará de forma automática si el atributo **Habilitar tramas de gran tamaño** se establece en sí.

- Los niveles AIX 5.3y AIX 6.1 dan soporte a las siguientes configuraciones para Adaptadores Ethernet de sistema principal (HEA).

- Se da soporte a la agregación de enlaces entre el puerto HEA dedicado y el adaptador PCI/PCI-E, tanto para agregación manual como para agregación LACP.
- Configuración de EtherChannel que incluye soporte a puertos HEA no dedicados, EtherChannel con adaptador de copia de seguridad configurado como PCI/PCI-E, o Ethernet virtual.

**Nota:** En el caso de un puerto HEA no dedicado en la configuración EtherChannel, existen limitaciones respecto a la agregación de enlaces.

- AIX Versión 6.1 con el nivel de tecnología 6100-06 y posterior da soporte a EtherChannel en conmutadores apilados.
- El arranque de red o la instalación de red por EtherChannel en clientes de Gestión de instalación de red (NIM) no están soportados.

### Configuración de un EtherChannel

Siga este procedimiento para configurar un EtherChannel.

1. Escriba smitty etherchannel en la línea de mandatos.
2. Seleccione **Añadir un EtherChannel / Agregación de enlace** en la lista y pulse Intro.
3. Seleccione los adaptadores primarios de Ethernet que desee utilizar con el EtherChannel y pulse Intro.  
Si piensa utilizar la copia de seguridad del EtherChannel, no seleccione el adaptador que piensa utilizar para la copia de seguridad todavía.
4. Escriba la información en los campos en función de las directrices siguientes:

- **Adaptador padre:** Proporciona información sobre el dispositivo padre de un EtherChannel (por ejemplo, cuando un EtherChannel pertenece a un adaptador Ethernet compartido). Este campo visualiza el valor NINGUNO si el EtherChannel no está incluido en otro adaptador (el valor predeterminado). Si el EtherChannel está contenido en otro adaptador, este campo visualiza el nombre del adaptador padre (por ejemplo, ent6). Este campo es sólo informativo y no puede modificarse. La opción del adaptador padre está disponible en AIX 5.3 y versiones posteriores.
- **Adaptadores de agregación de enlace / EtherChannel:** Debería ver todos los adaptadores primarios que se utilicen en el EtherChannel. Estos adaptadores se han seleccionado en el paso anterior.
- **Habilitar dirección alternativa:** Este campo es opcional. Si se establece en sí, podrá especificar la dirección MAC que desee que utilice el EtherChannel. Si se establece esta opción en no, el EtherChannel utilizará la dirección MAC del primer adaptador.
- **Dirección alternativa:** Si se establece **Habilitar dirección alternativa** en sí, especifique aquí la dirección MAC que desee utilizar. La dirección que especifique debe empezar por 0x y ser una dirección hexadecimal de 12 dígitos (por ejemplo, 0x001122334455).
- **Habilitar tramas de gran tamaño de Ethernet en gigabits:** Este campo es opcional. Para poder utilizarlo, el conmutador debe proporcionar soporte a las tramas de gran tamaño. Sólo funcionará con una interfaz Ethernet estándar (en), no una interfaz IEEE 802.3 (et). Establézcalo en sí si desea habilitarlo.
- **Modalidad:** Puede elegir entre las modalidades siguientes:
  - **estándar:** En esta modalidad, el EtherChannel utiliza un algoritmo para elegir a través de qué adaptador enviará los paquetes. El algoritmo consiste en tomar un valor de datos, dividirlo entre el número de adaptadores del EtherChannel y utilizar el resto (utilizando el operador de módulo) para identificar el enlace de salida. El valor de la modalidad hash determina el valor de datos que se introduce en este algoritmo (vea una explicación de las distintas modalidades hash en el atributo Modalidad hash). Por ejemplo, si la modalidad hash es estándar, utilizará la dirección IP de destino del paquete. Si es 10.10.10.11 y hay 2 adaptadores en el EtherChannel, (1 / 2) = 0 y el resto es 1, por lo que se utiliza el segundo adaptador (los adaptadores se numeran empezando por el 0). Los adaptadores se numeran en el orden en que aparecen en el menú SMIT. Esta es la modalidad de funcionamiento por omisión.

- **round\_robin**: En esta modalidad, el EtherChannel irá rotando entre los adaptadores, dando un paquete a cada adaptador antes de volver a repetir. Los paquetes pueden enviarse en un orden ligeramente distinto a aquel en que se proporcionaron al EtherChannel, pero el ancho de banda se aprovechará de la mejor forma posible. La combinación de esta modalidad con una modalidad hash que no sean el valor predeterminado no se permite. Si elige la modalidad round-robin, deje el valor de la modalidad hash en su valor predeterminado.
- **netif\_backup**: Para habilitar Modalidad de seguridad de la interfaz de red, puede configurar uno o más adaptadores en el EtherChannel primario y en el EtherChannel de seguridad. Para obtener más información, consulte el apartado “Configuración de la seguridad de la interfaz de red” en la página 456.
- **8023ad**: Esta opción permite utilizar el protocolo LACP(IEEE 802.3ad Link Aggregation Control Protocol) para la agregación automática de enlaces. Para obtener más detalles sobre esta función, consulte el apartado “Configuración de la Agregación de enlaces IEEE 802.3ad” en la página 463.
- **Intervalo IEEE 802.3ad**: Puede elegir entre los valores siguientes:
  - **largo**: Es el valor predeterminado del intervalo. Cuando está seleccionado, EtherChannel solicitará paquetes LACP de su asociado en el valor de intervalo largo especificado por el protocolo
  - **corto**: Cuando está seleccionado, EtherChannel solicitará paquetes LACP de su asociado en el valor de intervalo corto especificado por el protocolo.

**Nota:** El valor de intervalo sólo se utiliza cuando EtherChannel realiza operaciones en modalidad IEEE 802.3ad. De lo contrario, se omite el valor.

**Nota:** AIX satisface la solicitud de intervalo larga y corta de su asociado.
- **Modalidad hash**: Elija entre las siguientes modalidades hash, que determinarán el valor de los datos que el algoritmo utilizará para determinar el adaptador de salida:
  - **valor predeterminado**: Se utiliza la dirección IP de destino del paquete para determinar el adaptador de salida. Para el tráfico que no es IP (como, por ejemplo, ARP), se utiliza el último byte de la dirección MAC de destino para efectuar el cálculo. Esta modalidad garantiza que los paquetes se envíen a través del EtherChannel en el orden en el que se hayan recibido pero es posible que el ancho de banda no se utilice completamente.
  - **src\_port**: Se utiliza el valor del puerto UDP o TCP de origen para determinar el adaptador de salida. Si el paquete no es UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino.
  - **dst\_port**: Se utiliza el valor del puerto UDP o TCP de destino del paquete para determinar el adaptador de salida. Si el paquete no es tráfico UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino.
  - **src\_dst\_port**: Se utilizan los valores tanto del puerto UDP o TCP de origen como de destino del paquete para determinar el adaptador de salida (de hecho, se añaden los puertos de origen y de destino y, a continuación, se dividen entre dos antes de pasarse al algoritmo). Si el paquete no es tráfico UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino. Esta modalidad puede proporcionar una buena distribución de los paquetes en la mayoría de situaciones, tanto para los clientes como para los servidores.

**Nota:** La combinación de una modalidad hash que no sea el valor predeterminado con la modalidad round\_robin no se permite.

Para saber más acerca de la distribución de paquetes y el equilibrado de la carga, consulte el apartado “Opciones para el equilibrado de la carga en EtherChannel” en la página 457.
- **Adaptador de seguridad**: Este campo es opcional. Especifique una lista de los adaptadores que deseé utilizar como copia de seguridad del EtherChannel.
- **Dirección Internet con la que realizar ping**: Este campo es opcional y sólo surte efecto si se ejecuta la modalidad **Seguridad de la interfaz de red** o si tiene uno o más adaptadores en el EtherChannel y uno o más adaptadores en la lista de seguridad. El EtherChannel realizará ping a la

dirección IP o nombre del sistema principal que se especifique aquí. Si el EtherChannel no puede realizar ping a esta dirección durante el número de veces especificado en el campo **Número de reintentos** dentro del intervalo de tiempo especificado en el campo **Tiempo de espera entre reintentos**, el Etherchannel comuta a los otros adaptadores de la lista de seguridad. Para restablecer este campo de forma que se elimine el valor especificado anteriormente para esta opción, especifique el valor de opción **Dirección Internet con la que realizar ping:** como 0.

- **Número de reintentos:** Entre el número de fallos a la respuesta de ping que se permite antes de que el EtherChannel comute los adaptadores. El valor predeterminado es de 3. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.
- **Tiempo de espera entre reintentos:** Entre el número de segundos entre las veces en que el EtherChannel ejecutará ping con la **Dirección Internet con la que realizar ping**. El valor predeterminado es un segundo. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.

5. Pulse Intro después de cambiar los campos que desee para crear el EtherChannel.
6. Configure IP a través del dispositivo EtherChannel que acaba de crearse escribiendo smitty chinet en la línea de mandatos.
7. Seleccione la nueva interfaz de EtherChannel en la lista.
8. Rellene todos los campos necesarios y pulse Intro.

Para ver las tareas adicionales que pueden realizarse después de configurar el EtherChannel, consulte el apartado “Listado de los EtherChannels o de las agregaciones de enlaces” en la página 460.

### Opciones de recuperación y recuperación tras error

Las funciones de recuperación y recuperación tras error están disponibles para la Agregación de enlaces IEEE 802.3ad o EtherChannel.

Estas funciones posibilitan las mejoras siguientes:

- Puede evitarse la pérdida de paquetes durante la recuperación
- Es posible establecer las recuperaciones tras error para que se produzcan de forma simultánea
- La recuperación automática puede desactivarse para que el adaptador de seguridad continúe funcionando
- Las agregaciones de enlaces pueden pasarse a prueba de fallos desde el canal principal a la copia de seguridad y viceversa.

### Recuperación sin pérdidas

La característica de recuperación sin pérdidas asegura que la recuperación del adaptador de copia de seguridad en el canal primario pierda el menor número de paquetes posible.

Antes de la recuperación sin pérdidas, EtherChannel o IEEE 802.3ad se recupera en el canal primario en el mismo instante que detecta la recuperación de uno de los adaptadores primarios. En algunos casos, el commutador del adaptador no está en un estado en el que pueda enviar o recibir datos y algunos paquetes se pierden inmediatamente después de una recuperación.

Con la recuperación sin pérdidas, el adaptador EtherChannel o IEEE 802.3ad se recupera en el canal primario sólo cuando ha sido capaz de recibir realmente el tráfico. Esto asegura que el puerto de commutador esté totalmente inicializado y que no se pierdan paquetes.

### Modalidad a prueba de fallos sin pérdidas

La característica de modalidad a prueba de fallos sin pérdidas modifica el comportamiento de la característica de recuperación sin pérdidas.

Cuando las anomalías de ping producen una prueba de fallos, se observa de forma predeterminada la recuperación sin pérdidas. Esto incluye un periodo de espera hasta que el commutador del adaptador inactivo recibe tráfico antes de finalizar la prueba de fallos. Sin embargo, si se establece el atributo **noLoss\_failover** en no, las pruebas de fallos de ping se producen inmediatamente.

## **Recuperación automática**

Después de pasar el control del canal principal al adaptador de seguridad, el EtherChannel y la Agregación de enlaces IEEE 802.3ad inicia una recuperación automática en el canal principal cuando se recupera por lo menos uno de sus adaptadores.

Esta opción de recuperación no está soportada en la modalidad IEEE 802.3ad y la migración tras error para el adaptador de seguridad es debido a la anomalía del Protocolo de control de Agregación de enlaces (LACP). La anomalía de LACP se produce cuando todos los adaptadores del canal primario no reciben las unidades de datos de LACP (LACPDU) dentro del período de tiempo de espera. El período de tiempo de espera excedido se determina mediante el estándar IEEE, que se basa en el intervalo configurado para la modalidad IEEE 802.3ad.

Este comportamiento predeterminado se puede modificar estableciendo el atributo **auto\_recovery** en no. Con este valor, el EtherChannel o la Agrupación de enlaces IEEE 802.3ad continúa funcionando en el adaptador de seguridad después de la recuperación tras error. Las operaciones del adaptador de seguridad continuarán hasta que se produzca una de las situaciones siguientes:

- Se forzará una migración tras error.
- Fallará el adaptador de copia de seguridad.
- Se detectará una anomalía de ping en el adaptador de copia de seguridad.

## **Recuperaciones forzadas**

Es posible forzar la Agregación de enlaces de IEEE 802.3ad o EtherChannel para que pase del canal principal al adaptador de seguridad o del adaptador de seguridad al canal principal.

Las recuperaciones forzadas sólo funcionan si hay definido un adaptador de seguridad y si el canal inactivo está en funcionamiento. Por ejemplo, para forzar el paso del canal principal al adaptador de seguridad, el adaptador de seguridad debe estar en ejecución.

Para utilizar esta función, escriba `smitty etherchannel` y seleccione la opción **Forzar una recuperación tras error en una Agregación de enlaces / EtherChannel** en la pantalla. A continuación, seleccione la Agregación de enlaces IEEE 802.3ad o EtherChannel donde deba forzarse la recuperación tras error.

## **Configuración de la seguridad de la interfaz de red**

La modalidad de seguridad de la interfaz de red protege frente a una anomalía de red en un solo punto proporcionando funciones de detección y recuperación tras error sin interrumpir las conexiones del usuario. Cuando se trabaja en esta modalidad, sólo hay un adaptador activo en un momento determinado.

Si el adaptador activo presenta una anomalía, se utilizará otro adaptador del EtherChannel para todo el tráfico. Cuando se trabaja en la modalidad de seguridad de la interfaz de red, no es necesario conectar con los commutadores en los que está habilitado el EtherChannel.

La configuración de la seguridad de la interfaz de red resulta más eficaz cuando los adaptadores están conectados a distintos commutadores de red, ya que esto proporciona una redundancia mayor que si se conectan todos los adaptadores a un commutador. Al conectar con commutadores distintos, asegúrese de que exista una conexión entre los commutadores. Esto proporciona funciones de recuperación tras error de un adaptador a otro, garantizando que siempre existe una ruta hacia el adaptador activo actualmente.

Se da prioridad al adaptador configurado en el EtherChannel primario, a través del adaptador de copia de seguridad. El adaptador primario se utilizará siempre que esté operativo. Esto contrasta con el comportamiento de la modalidad de seguridad de la interfaz de red en releases anteriores, donde el adaptador de copia de seguridad se había utilizado hasta que fallara, independientemente de si el adaptador primario se había recuperado.

Por ejemplo, `ent0` podría configurarse como el adaptador principal y `ent2` como el adaptador de seguridad para crear un EtherChannel denominado `ent3`. Idealmente, `ent0` y `ent2` estarían conectados a dos commutadores distintos. En este ejemplo, todo el tráfico enviado a través de `ent3` (la interfaz del EtherChannel) se envía a través de `ent0` de forma predeterminada, mientras que `ent2` está desocupado. Si en algún momento se produce una anomalía en `ent0`, todo el tráfico se enviará a través del adaptador de seguridad, `ent2`. Cuando `ent0` se recupere, volverá a utilizarse para todo el tráfico.

Ahora es posible configurar el EtherChannel para detectar anomalías de enlace y falta de conexión con la red para varios EtherChannels que tengan un adaptador de seguridad. Para ello, utilice el atributo **netaddr** para especificar la dirección IP o el nombre de sistema principal remoto donde la conectividad siempre deba estar presente. El EtherChannel realizará ping con este sistema principal de forma periódica para determinar si continúa existiendo una vía de acceso de red con el mismo. Si un número determinado de intentos de realizar ping no reciben respuesta, el EtherChannel pasará el control al otro adaptador, esperando que a través del otro adaptador sí que exista una vía de acceso de red con el sistema principal remoto. En esta configuración, no sólo es necesario conectar cada adaptador con un conmutador distinto, sino que cada conmutador también debería tener una ruta distinta con el sistema principal con el que se realizará el ping.

Esta función para realizar ping está disponible para uno o más EtherChannels que tengan un adaptador de seguridad. Sin embargo, si se produce una anomalía debido a la falta de respuesta de los pings ejecutados en el adaptador primario, el adaptador de seguridad continúa siendo el canal activo mientras esté funcionando. Mientras se trabaja en el adaptador de seguridad no es posible saber si es posible alcanzar el sistema principal al que se ejecuta ping desde el adaptador primario. Para evitar ir pasando el control del adaptador primario al de seguridad, continúa funcionando en el adaptador de seguridad (a menos que los pings ejecutados tampoco reciban respuesta en el adaptador de seguridad o el propio adaptador de seguridad presente una anomalía, en cuyo caso pasaría el control al adaptador principal). Sin embargo, si el paso de control se debe a una anomalía en el adaptador principal (no a la falta de respuesta de los pings realizados), el EtherChannel volverá al adaptador principal tan pronto como éste se encuentre activo, como normalmente.

Para configurar la seguridad de la interfaz de red en las versiones más recientes, consulte “[Configuración de la seguridad de la interfaz de red](#)” en la página 456.

### **Configuración de la seguridad de la interfaz de red**

Utilice este procedimiento para configurar una seguridad de la interfaz de red en las versiones más recientes.

1. Con autorización root, escriba smitty etherchannel en la línea de mandatos.
2. Seleccione **Añadir un EtherChannel / Agregación de enlace** en la lista y pulse Intro.
3. Seleccione el adaptador Ethernet primario y pulse Intro. Éste es el adaptador que se utilizará hasta que se produzca alguna anomalía.

**Nota:** El campo **Adaptadores de red disponibles** muestra todos los adaptadores Ethernet. Si selecciona un adaptador Ethernet que ya se esté utilizando, obtendrá un mensaje de error y deberá desconectar esta interfaz antes de poder utilizarlo. Consulte el apartado “[Realización de modificaciones en un EtherChannel con 5200-01 y versiones anteriores](#)” en la página 463 para obtener información sobre cómo desconectar una interfaz.

4. Escriba la información en los campos siguientes en función de las directrices siguientes:
  - **Adaptador padre:** Este campo proporciona información sobre el dispositivo padre de un EtherChannel (por ejemplo, cuando un EtherChannel pertenece a un adaptador Ethernet compartido). Este campo visualiza el valor NINGUNO si el EtherChannel no está incluido en otro adaptador (el valor predeterminado). Si el EtherChannel está contenido en otro adaptador, este campo visualiza el nombre del adaptador padre (por ejemplo, ent6). Este campo es sólo informativo y no puede modificarse. La opción del adaptador de seguridad está disponible en el sistema operativo AIX.
  - **Adaptadores de agregación de enlaces / EtherChannel:** Debería ver el adaptador primario que se ha seleccionado en el paso anterior.
  - **Habilitar dirección alternativa:** Este campo es opcional. Si se establece en sí, podrá especificar la dirección MAC que desee que utilice el EtherChannel. Si se establece esta opción en no, el EtherChannel utilizará la dirección MAC del adaptador principal.
  - **Dirección alternativa:** Si se establece **Habilitar dirección alternativa** en sí, especifique aquí la dirección MAC que desee utilizar. La dirección que especifique debe empezar por 0x y ser una dirección hexadecimal de 12 dígitos (por ejemplo, 0x001122334455).

- **Habilitar tramas de gran tamaño de Ethernet en gigabits:** Este campo es opcional. Para poder utilizarlo, el conmutador debe proporcionar soporte a las tramas de gran tamaño. Sólo funciona con una interfaz Ethernet estándar (en), no una interfaz IEEE 802.3 (et). Establézcalo en sí si desea utilizarlo.
- **Modalidad:** La modalidad operativa seleccionada es irrelevante porque sólo hay un adaptador en el EtherChannel principal. Todos los paquetes se envían a través de este adaptador hasta que se produzca una anomalía. No existe ninguna modalidad netif\_backup porque para emular esta modalidad debe utilizarse un adaptador de seguridad.
- **Modalidad hash:** La modalidad hash seleccionada es irrelevante porque sólo hay un adaptador en el EtherChannel principal. Todos los paquetes se envían a través de este adaptador hasta que se produzca una anomalía.
- **Adaptador de copia de seguridad:** Especifique una lista de uno o más adaptadores que desee incluir en el grupo de copia de seguridad del EtherChannel. Después de una migración tras error debida a la pérdida del grupo EtherChannel primario, se utilizan los adaptadores de copia de seguridad hasta que se recupere el grupo de EtherChannel primario.
- **Dirección Internet con la que realizar Ping:** Este campo es opcional. El EtherChannel realizará ping con la dirección IP o el nombre del sistema principal que se especifique aquí. Si el EtherChannel no puede realizar ping con esta dirección durante el número de veces especificado en el campo **Número de reintentos** y a los intervalos especificados en el campo **Tiempo de espera entre reintentos**, el EtherChannel comuta los adaptadores.
- **Número de reintentos:** Entre el número de fallos a la respuesta de ping que se permite antes de que el EtherChannel comute los adaptadores. El valor predeterminado es de 3. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.
- **Tiempo de espera entre reintentos:** Entre el número de segundos entre las veces en que el EtherChannel ejecutará ping con la **Dirección Internet con la que realizar ping**. El valor predeterminado es un segundo. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.

5. Pulse Intro después de cambiar los campos que desee para crear el EtherChannel.
6. Configure IP a través de la interfaz que acaba de crearse escribiendo smitty chinet en la línea de mandatos.
7. Seleccione la nueva interfaz de EtherChannel en la lista.
8. Rellene todos los campos necesarios y pulse Intro.

La copia de seguridad de la interfaz de la red ya está configurada.

#### **Opciones para el equilibrado de la carga en EtherChannel**

Existen dos métodos para el equilibrado de la carga para el tráfico de salida en EtherChannel, que son los siguientes: Round-robin, que distribuye el tráfico de salida de forma homogénea entre todos los adaptadores de EtherChannel y estándar, que selecciona el adaptador utilizando un algoritmo.

El parámetro Modalidad hash determina el valor numérico que se pasa al algoritmo.

La tabla siguiente resume las combinaciones de opciones de equilibrado de carga válidas que se ofrecen.

Tabla 81. Combinaciones de Modalidad y de Modalidad hash y la distribución del tráfico de salida que cada una genera.

Modalidad	Modalidad hash	Distribución del tráfico de salida
estándar o 8023ad	por omisión	El comportamiento de AIX tradicional. El algoritmo de selección de adaptador utiliza el último byte de la dirección IP de destino (para el tráfico <b>TCP/IP</b> ) o la dirección MAC (para ARP u otro tráfico que no sea IP). Esta modalidad suele ser una buena opción inicial para un servidor con un gran número de clientes.
estándar o 8023ad	src_dst_port	La vía de acceso del adaptador de salida se selecciona mediante un algoritmo utilizando los valores de los puertos TCP o UDP de origen y de destino combinados. Como cada conexión tiene un puerto TCP o UDP exclusivo, las tres modalidades hash basadas en puerto proporcionan flexibilidad de distribución de los adaptadores adicional cuando haya varias conexiones de TCP o UDP independientes entre un par de direcciones IP.
estándar o 8023ad	src_port	El algoritmo de selección del adaptador utiliza el valor del puerto TCP o UDP fuente. En la salida del mandato <b>netstat -an</b> , el puerto es el valor del sufijo de la dirección TCP/IP en la columna Local.
estándar o 8023ad	dst_port	La vía de acceso del adaptador de salida se selecciona mediante un algoritmo utilizando el valor del puerto del sistema de destino. En la salida del mandato <b>netstat -an</b> , el sufijo de la dirección TCP/IP de la columna Foreign (externo) es el valor del puerto TCP o UDP de destino.
round-robin	por omisión	El tráfico de salida se distribuye de forma homogénea entre los puertos de adaptadores de EtherChannel. Esta modalidad es la opción habitual para dos sistemas principales conectados de forma consecutiva (sin la intervención de un commutador).

### **Distribución round-robin**

Todo el tráfico de salida se distribuye de forma homogénea entre todos los adaptadores del EtherChannel. Proporciona la optimización más elevada del ancho de banda para el sistema de servidores en AIX. Aunque la distribución round-robin constituye la forma ideal para utilizar todos los enlaces de forma homogénea, piense que también conlleva la posibilidad de que los paquetes lleguen fuera de secuencia al sistema receptor.

En general, la modalidad round-robin resulta ideal para las conexiones consecutivas que se ejecutan a través de tramas de gran tamaño. En este entorno, no interviene ningún conector, por lo que no es posible que el proceso realizado en el conmutador altere la vía de acceso del adaptador, la hora o el orden de entrega de los paquetes. En esta vía de acceso de red por cable directo, los paquetes se reciben exactamente tal como se envían. Las tramas de gran tamaño (MTU de 9000 byte) siempre proporcionan un mejor rendimiento durante la transferencia de archivos que las MTU tradicionales de 1500 bytes. Sin embargo, en este caso, añaden otra ventaja. Estos paquetes más grandes tardan más en enviarse por lo que es menor probable que el sistema principal receptor se vea continuamente interrumpido con paquetes fuera de secuencia.

La modalidad round-robin puede implementarse en otros entornos pero con un mayor riesgo de que lleguen paquetes fuera de secuencia en el sistema receptor. Este riego es especialmente elevado cuando se trata de pocas conexiones TCP en modalidad continua que duran mucho. Cuando existen muchas conexiones de este tipo entre un par de sistemas principales, es posible que los paquetes de las distintas conexiones se entremezclen, disminuyendo con ello la posibilidad de que los paquetes de la misma conexión lleguen fuera de secuencia. Compruebe las estadísticas de paquetes fuera de secuencia en la sección `tcp` de la salida del mandato **netstat -s**. Un valor que aumenta de forma regular indica un problema en potencia en el tráfico enviados desde un EtherChannel.

Si los paquetes fuera de secuencia constituyen un problema en un sistema donde deben utilizarse MTU de Ethernet tradicionales que deba conectarse a través de un conmutador, intente las distintas modalidades hash que se ofrecen en el funcionamiento en modalidad estándar. Cada modalidad tiene un punto fuerte en concreto, pero el punto de partida lógica son la modalidad `src_dst_port` y la modalidad por omisión, ya que son las que pueden aplicarse de forma más generalizada.

### **Algoritmo estándar o 802.3ad**

La utilización del algoritmo estándar del EtherChannel presenta ventajas.

El algoritmo estándar se utiliza para las agregaciones tanto de tipo IEEE 802.3ad como estándar. AIX divide el último byte del "valor numérico" entre el número de adaptadores del EtherChannel y utiliza el resto para identificar el enlace de salida. Si el resto es cero, se selecciona el primer adaptador del EtherChannel; si el resto es uno, se selecciona el segundo adaptador y así sucesivamente (los adaptadores se seleccionan en el orden en el que se listan en el atributo **adapter\_names**).

La selección de la modalidad hash determina el valor numérico utilizado en el cálculo. De forma predeterminada, en el cálculo se utiliza el último byte de la dirección IP de destino o la dirección MAC pero también es posible utilizar los valores de los puertos TCP o UDP tanto de origen como de destino. Estas alternativas permiten un mejor ajuste de la distribución del tráfico de salida a través de los adaptadores reales del EtherChannel.

En la modalidad hash predeterminada, el algoritmo de selección de adaptador se aplica al último byte de la dirección IP de destino para el tráfico IP. Para ARP y otro tráfico que no es IP, se aplica la misma fórmula al último byte de la dirección MAC de destino. A menos que una anomalía del adaptador provoque una recuperación tras error, todo el tráfico entre un par de sistemas principales en la modalidad estándar predeterminada se envía a través del mismo adaptador. La modalidad hash predeterminada puede resultar idónea cuando el sistema principal local establece conexiones con muchas direcciones IP distintas.

Sin embargo, si el sistema principal local establece conexiones largas con pocas direcciones IP, observará que algunos adaptadores deben soportar una carga mucho mayor que los otros, porque todo el tráfico enviado a un destino en concreto se enviará a través del mismo adaptador. Aunque esto impide que los paquetes lleguen desordenados, es posible que el ancho de banda no se utilice de la forma más eficaz en todos los casos. Las modalidades hash basadas en puertos continúan enviando los paquetes en orden, pero permiten que los paquetes que pertenecen a conexiones UDP o TCP distintas, aunque se envíen al

mismo destino, se envíen a través de adaptadores distintos utilizando mejor de este modo el ancho de banda de todos los adaptadores.

En modalidad hash **src\_dst\_port**, los valores de los puertos TCP o UDP de origen y destino del paquete de salida se añaden y entonces se dividen entre dos. El número total resultante (sin decimales) se introduce en el algoritmo estándar. El tráfico TCP o UDP se envía a través del adaptador seleccionado por el algoritmo estándar y el valor de la modalidad hash seleccionada. El tráfico que no es TCP ni UDP utilizará la modalidad hash predeterminada, es decir, el último byte de la dirección IP o la dirección MAC de destino. La opción de la modalidad hash **src\_dst\_port** tiene en cuenta los valores de los puertos TCP o UDP tanto de origen como de destino. En esta modalidad, todos los paquetes de una conexión TCP o UDP se envían a través de un solo adaptador para que se garantice que lleguen en orden pero el tráfico todavía se distribuye porque las conexiones (incluso con el mismo sistema principal) pueden enviarse a través de distintos adaptadores. La dirección del establecimiento de la conexión no desvía los resultados de esta modalidad hash, ya que ésta utiliza los valores de puertos TCP o UDP tanto de origen como de destino.

En modalidad hash **src\_port**, se utiliza el valor del puerto TCP o UDP de origen del paquete de salida. En modalidad hash **dst\_port** se utiliza el valor del puerto TCP o UDP de destino del paquete de salida. Utilice las opciones de la modalidad hash **src\_port** o **dst\_port** si los valores de los puertos cambian de una conexión a otra y si la opción **src\_dst\_port** no proporciona la distribución que se desea.

### Listado de los EtherChannels o de las agregaciones de enlaces

Siga este procedimiento para listar los EtherChannels o las agregaciones de enlaces.

1. En la línea de mandatos, escriba smitty etherchannel.
2. Seleccione **Listar todas agregaciones de enlaces / EtherChannels** y pulse Intro.

### Modificación de la dirección alternativa

Para especificar una dirección MAC para el EtherChannel o la Agregación de enlaces, realice los pasos siguientes.

1. En función de la versión de AIX que se ejecute, es posible que deba desconectar la interfaz:
  - En AIX 5.2 con 5200-01 y versiones anteriores, escriba smitty chinet y seleccione la interfaz que pertenezca al EtherChannel. Cambie el atributo **ESTADO actual a desconectar** y pulse Intro.
  - En AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03. y versiones posteriores es posible cambiar la dirección alternativa del EtherChannel sin desconectar la interfaz.
2. En la línea de mandatos, escriba smitty etherchannel.
3. Seleccione **Cambiar/Mostrar características de un EtherChannel** y pulse Intro.
4. Si tiene varios EtherChannels, seleccione el EtherChannel para el que desee crear una dirección alternativa.
5. Cambie el valor de **Habilitar dirección de EtherChannel alternativa** a sí.
6. Escriba la dirección alternativa en el campo **Dirección de EtherChannel alternativa**. La dirección debe empezar por 0x y debe ser una dirección hexadecimal de 12 dígitos (por ejemplo, 0x001122334455).
7. Pulse Intro para completar el proceso.

**Nota:** Al cambiar la dirección MAC del EtherChannel en tiempo de ejecución puede provocarse una pérdida de conectividad temporal. Esto es debido a que es necesario restablecer los adaptadores para que aprendan la nueva dirección de hardware y algunos adaptadores tardan unos segundos en inicializarse.

### Pertenencia dinámica de los adaptadores (DAM)

Con anterioridad a AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03., para añadir o eliminar un adaptador de un EtherChannel, primero era necesario desconectar la interfaz, interrumpiendo temporalmente todo el tráfico de los usuarios. Para solucionar esta limitación, se añadió la Pertenencia dinámica de adaptadores (DAM) en AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03..

Permite añadir o eliminar adaptadores en el EtherChannel sin interrumpir las conexiones del usuario. También es posible añadir o eliminar un adaptador de seguridad; un EtherChannel puede crearse inicialmente sin un adaptador de seguridad y añadirlo más tarde si se considera necesario.

No sólo es posible añadir y eliminar los adaptadores sin interrumpir las conexiones de los usuarios, sino que también pueden modificarse la mayoría de atributos del EtherChannel durante la ejecución. Por ejemplo, es posible empezar a utilizar la función "ping" de la seguridad de la interfaz de red mientras se está utilizando el EtherChannel o cambiar el sistema principal remoto al que se realiza ping en cualquier momento.

También puede convertir un EtherChannel normal en una Agregación de enlaces IEEE 802.3ad (o viceversa), permitiendo que los usuarios experimenten con esta función sin tener que eliminar el EtherChannel y volver a crearlo.

Además, con DAM, puede optar por crear un EtherChannel de un adaptador. El comportamiento de un EtherChannel de un adaptador es exactamente el mismo que el de un adaptador normal; sin embargo, en caso de que se produjera una anomalía en este adaptador, sería posible sustituirlo durante la ejecución sin tener que perder la conexión. Para ello, es necesario añadir un adaptador temporal al EtherChannel, eliminar el adaptador defectuoso del EtherChannel, sustituir el adaptador defectuoso por uno que funcione bien utilizando una inserción en caliente (Hot Plug), añadir el adaptador nuevo al EtherChannel y eliminar entonces el adaptador temporal. Durante este proceso, no se aprecia ninguna pérdida de conectividad. Sin embargo, si el adaptador estaba funcionando como adaptador autónomo, debe desconectarse antes de su eliminación utilizando una inserción en caliente (Hot Plug) y durante este tiempo se perderá el tráfico que pase a través del mismo.

#### **Adición, eliminación o modificación de adaptadores en un EtherChannel o una Agregación de enlaces**

Existen dos formas de añadir, eliminar o modificar un adaptador en un EtherChannel o una Agregación de enlaces.

Un método requiere que la interfaz de la Agregación de enlaces o el EtherChannel esté desconectada, mientras que el otro no (utilizando la Pertenencia dinámica de los adaptadores, que está disponible en AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03. y versiones posteriores).

#### ***Realización de modificaciones en un EtherChannel utilizando la Pertenencia dinámica de los adaptadores***

Al realizar modificaciones utilizando la Pertenencia dinámica de los adaptadores no es necesario detener todo el tráfico que pasa a través del EtherChannel desconectando la interfaz.

Tenga en cuenta los aspectos siguientes antes de continuar:

1. Al añadir un adaptador en tiempo de ejecución, observe que distintos adaptadores Ethernet proporcionan soporte a distintas funciones (por ejemplo, la posibilidad de realizar la descarga de la suma de comprobación, de utilizar segmentos privados, de realizar grandes envíos, etc). Si se utilizan distintos tipos de adaptadores en el mismo EtherChannel, las funciones que se indican al nivel de la interfaz son aquellas a las que todos los adaptadores proporcionan soporte (por ejemplo, si todos los adaptadores excepto uno proporcionan soporte a la utilización de segmentos privados, el EtherChannel indicará que no proporciona soporte a los segmentos privados; si todos los adaptadores proporcionan soporte a los grandes envíos, el canal indicará que proporciona soporte a los grandes envíos). Cuando añada un adaptador a un EtherChannel durante la ejecución, asegúrese de que proporcione soporte por lo menos a las mismas funciones que los otros adaptadores que ya estén en el EtherChannel. Si intenta añadir un adaptador que no proporcione soporte a todas las funciones a las que el EtherChannel proporcione soporte, la adición fallará. Observe, sin embargo, que si la interfaz del EtherChannel está desconectada, es posible añadir un adaptador (con independencia de las funciones a las que proporcione soporte) y cuando la interfaz se reactive el EtherChannel volverá a calcular las funciones a las que proporciona soporte en función de la nueva lista de adaptadores.
2. Si no utiliza una dirección alternativa y piensa suprimir el adaptador cuya dirección MAC se haya utilizado para el EtherChannel (la dirección MAC utilizada para el EtherChannel es "propiedad" de uno de los adaptadores), el EtherChannel utilizará la dirección MAC del siguiente adaptador disponible. En otras palabras, la del que pase a ser el primer adaptador tras la supresión o la del adaptador de seguridad en caso de que se supriman muchos adaptadores. Por ejemplo, si un EtherChannel tiene los adaptadores principales ent0 y ent1 y un adaptador de seguridad ent2, que utiliza la dirección MAC

ent0 predeterminada (se considerará que ent0 es el "propietario" de la dirección MAC). Si se suprime ent0, el EtherChannel utilizará la dirección MAC de ent1. Si entonces se suprime ent1, el EtherChannel utilizará la dirección MAC de ent2. Si más tarde vuelve a añadirse ent0 al EtherChannel, éste continuará utilizando la dirección MAC de ent2, porque ent2 será entonces el propietario de la dirección MAC. Si ent2 se suprime del EtherChannel, volverá a utilizar la dirección MAC de ent0 otra vez.

Si se suprime el adaptador cuya dirección MAC se ha utilizado para el EtherChannel puede provocar una pérdida temporal de la conectividad, ya que es necesario restablecer todos los adaptadores del EtherChannel para que aprendan la nueva dirección de hardware. Algunos adaptadores tardan unos segundos en inicializarse.

Si el EtherChannel utiliza una dirección alternativa (una dirección MAC que haya especificado), continuará utilizando esta dirección MAC con independencia de los adaptadores que se añadan o supriman. Además, ello significa que no se producirá ninguna pérdida temporal de la conectividad al añadir o suprimir los adaptadores, ya que ninguno de los adaptadores es el "propietario" de la dirección MAC del EtherChannel.

3. Casi todos los atributos del EtherChannel pueden modificarse ahora en tiempo de ejecución. La única excepción la constituye **Habilitar tramas de gran tamaño Ethernet en gigabits**. Para modificar el atributo **Habilitar tramas de gran tamaño Ethernet en gigabits**, deberá desconectar la interfaz del EtherChannel antes de intentar modificar este valor.
4. Para los atributos que no pueden modificarse en tiempo de ejecución(actualmente sólo **Habilitar tramas de gran tamaño Ethernet en gigabits**), existe un campo denominado **Aplicar el cambio únicamente a la BASE DE DATOS**. Si este atributo se establece en sí, es posible cambiar, en tiempo de ejecución, el valor de un atributo que normalmente no pueda modificarse en tiempo de ejecución. Cuando el campo **Aplicar el cambio únicamente a la BASE DE DATOS** se establece en sí, el atributo sólo se cambiará en el ODM y no se reflejará en el EtherChannel que está en ejecución hasta que vuelva a cargarse en memoria(para lo que se deberá desconectar la interfaz y utilizar los mandatos `rmdev -l EtherChannel_device` y `mkdev -l EtherChannel_device`) o hasta que se rearranje la máquina. Esto es una forma útil de asegurarse de qué atributo se modificará la próxima vez que se rearranje la máquina sin necesidad de interrumpir el EtherChannel que está en ejecución.
5. En una partición lógica, cuando se elimina un adaptador de un EtherChannel, debe eliminar también el puerto de conmutador asociado del EtherChannel del conmutador. De lo contrario, se podría perder la conectividad porque el conmutador podría estar utilizando el mismo puerto de conmutador para las comunicaciones.

Para realizar modificaciones en el EtherChannel o en la Agrupación de enlaces utilizando la Pertenencia dinámica de los adaptadores, siga los pasos siguientes:

1. En la línea de mandatos, escriba `smitty etherchannel`.
2. Seleccione **Cambiar/Mostrar características de una Agregación de enlaces / EtherChannel**.
3. Seleccione el EtherChannel o la Agregación de enlaces que desee modificar.
4. Rellene los campos necesarios de acuerdo con las directrices siguientes:
  - En el campo **Añadir adaptador** o **Eliminar adaptador**, seleccione el adaptador Ethernet que desee añadir o eliminar.
  - En los campos **Añadir adaptador de seguridad** o **Eliminar adaptador de seguridad**, seleccione el adaptador Ethernet que desee iniciar o detener utilizando una copia de seguridad.
  - Todos los atributos del EtherChannel pueden modificarse en tiempo de ejecución a excepción del atributo **Habilitar tramas de gran tamaño Ethernet en gigabits**.
  - Para convertir un EtherChannel normal en una Agregación de enlaces IEEE 802.3ad, cambie el atributo **Modalidad** a 8023ad. Para convertir una Agrupación de enlaces IEEE 802.3ad en un EtherChannel, cambie el atributo **Modalidad** a **estándar** o **round\_robin**.
5. Rellene los datos necesarios y pulse Intro.

## **Realización de modificaciones en un EtherChannel con 5200-01 y versiones anteriores**

Utilice este procedimiento para desconectar la interfaz y realizar cambios en un EtherChannel con 5200-01 y versiones anteriores.

1. Escriba smitty chinet y seleccione la interfaz que pertenezca al EtherChannel. Cambie el atributo **ESTADO actual a desconectar** y pulse Intro.
2. En la línea de mandatos, escriba smitty etherchannel.
3. Seleccione **Cambiar / Mostrar características de una Agregación de enlaces / EtherChannel** y pulse Intro.
4. Seleccione el EtherChannel o la Agregación de enlaces que desee modificar.
5. Modifique los atributos que desee modificar en el EtherChannel o la Agregación de enlaces y pulse Intro.
6. Rellene los campos necesarios y pulse Intro.

## **Eliminación de un EtherChannel o una Agregación de enlaces**

Siga este procedimiento para eliminar un EtherChannel o una Agregación de enlaces.

1. Escriba smitty chinet y seleccione la interfaz que pertenezca al EtherChannel. Cambie el atributo **ESTADO actual a desconectar** y pulse Intro.
2. En la línea de mandatos, escriba smitty etherchannel.
3. Seleccione **Eliminar un EtherChannel** y pulse Intro.
4. Seleccione el EtherChannel que deseé eliminar y pulse Intro.

## **Configuración o eliminación de un adaptador de seguridad en un EtherChannel o una Agregación de enlaces existente**

El procedimiento siguiente configura o elimina un adaptador de seguridad en un EtherChannel o una Agregación de enlaces.

1. Escriba smitty chinet y seleccione la interfaz que pertenezca al EtherChannel. Cambie el atributo **ESTADO actual a desconectar** y pulse Intro.
2. En la línea de mandatos, escriba smitty etherchannel.
3. Seleccione **Cambiar/Mostrar características de una Agregación de enlaces / EtherChannel**.
4. Seleccione el EtherChannel o la Agregación de enlaces donde esté añadiendo o modificando el adaptador de seguridad.
5. Entre el adaptador que deseé utilizar como adaptador de seguridad en el campo **Adaptador de seguridad** o seleccione **NINGUNO** si desea dejar de utilizar el adaptador de seguridad.

## **Configuración de la Agregación de enlaces IEEE 802.3ad**

IEEE 802.3ad constituye una forma estándar de realizar la Agregación de enlaces. Conceptualmente, funciona igual que EtherChannel, pero en este caso varios adaptadores Ethernet se agregan a un solo adaptador virtual, proporcionando mayor ancho de banda y protección contra anomalías.

Por ejemplo, es posible agregar ent0 y ent1 a una Agregación de enlaces 802.3ad denominada ent3; entonces, la interfaz ent3 se configuraría con una dirección IP. El sistema considera estos adaptadores agregados como un solo adaptador. Por lo tanto, IP se configura a través de ellos como cualquier adaptador Ethernet.

IEEE 802.3ad requiere soporte en el conmutador.

Las ventajas de utilizar la Agregación de enlaces IEEE 802.3ad en lugar de EtherChannel son que puede utilizar conmutadores que son compatibles con el estándar IEEE 802.3ad pero que no lo son con EtherChannel y que proporciona protección contra anomalías del adaptador.

Cuando se configura una agregación IEEE 802.3ad, las unidades de datos del Protocolo de control de Agregación de enlaces (LACPDU) se intercambian entre la máquina del servidor (sistema principal) y el conmutador adyacente. Sólo el canal activo, lo que puede ser el canal primario o el adaptador de seguridad, intercambia LACPDU con el conmutador adyacente.

Para poder agregar adaptadores (lo que significa que el conmutador permite que formen parte de la misma agregación) deben tener la misma velocidad de línea (por ejemplo, todos 100 Mbps, o todos 1 Gbps) y todos deben ser dúplex. Si intenta colocar adaptadores de velocidades de línea distintas o modalidades dúplex diferentes, la creación de la agregación en el sistema AIX se llevará a cabo correctamente, pero es posible que el conmutador no agregue juntos los adaptadores. Si el conmutador no agrega los adaptadores juntos satisfactoriamente, es posible que observe una reducción en el rendimiento de la red. Para obtener información sobre cómo determinar si una agregación en un conmutador ha sido satisfactoria, consulte el apartado “[Resolución de problemas con la Agregación de enlaces IEEE 802.3ad](#)” en la página 466.

Según la especificación IEEE 802.3ad, los paquetes que se envían a la misma dirección IP se envían a través del mismo adaptador. Por lo tanto, cuando se utiliza en la modalidad 802.3ad, los paquetes siempre se distribuyen de la forma estándar, nunca en una forma cíclica.

La función de adaptador de seguridad está disponible para las agregaciones de enlaces IEEE 802.3ad, al igual que para EtherChannel. El adaptador de seguridad también sigue la LACP IEEE 802.3ad. El puerto del conmutador conectado al adaptador de seguridad también debe tener IEEE 802.3ad habilitado.

**Nota:** Los pasos necesarios para permitir la utilización de IEEE 802.3ad varían de un conmutador a otro. Debe consultar la documentación de su conmutador para determinar los pasos iniciales, si hay alguno, que se deben realizar para habilitar LACP en el conmutador.

Para obtener información sobre cómo configurar una agregación IEEE 802.3ad, consulte el apartado “[Configuración de la Agregación de enlaces IEEE 802.3ad](#)” en la página 464.

Tenga en cuenta lo siguiente antes de configurar una Agregación de enlaces IEEE 802.3ad:

- Aunque carece de soporte oficial, la implementación de AIX de IEEE 802.3ad permite a la Agregación de enlaces que contenga adaptadores de distintas velocidades de líneas. Sin embargo, debe agregar sólo los adaptadores que estén establecidos en la misma velocidad de línea y dúplex. Esto ayuda a evitar los problemas potenciales al configurar la Agregación de enlaces en el conmutador. Para obtener más información sobre los tipos de agregación permitidos por el conmutador, consulte la documentación del conmutador.
- Si utiliza adaptadores Ethernet 10/100 en la Agregación de enlaces, debe habilitar el sondeo de enlaces en estos adaptadores antes de añadirlos a la agregación. Escriba smitty chgenet en la línea de mandatos. Cambie el valor de **Habilitar sondeo de enlaces** a sí y pulse Intro. Realice esta acción para cada adaptador Ethernet 10/100 que vaya a añadir a la Agregación de enlaces.

**Nota:** En AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03. y versiones posteriores, no es necesario el mecanismo de sondeo de enlaces. En sondeador de enlaces se inicia automáticamente.

#### [\*\*Configuración de la Agregación de enlaces IEEE 802.3ad\*\*](#)

Siga los pasos siguientes para configurar una Agregación de enlaces IEEE 802.3ad.

1. Escriba smitty etherchannel en la línea de mandatos.
2. Seleccione **Añadir un EtherChannel / Agregación de enlace** en la lista y pulse Intro.
3. Seleccione los adaptadores primarios de Ethernet que desee utilizar en la Agregación de enlaces y pulse Intro.

Si piensa utilizar un adaptador de seguridad, no seleccione el adaptador que piensa utilizar para la copia de seguridad todavía.

**Nota: Adaptadores de red disponibles** visualiza todos los adaptadores Ethernet. Si selecciona un adaptador Ethernet que ya se esté utilizando (que tenga definida una interfaz), obtendrá un mensaje de error. Si desea utilizar estos adaptadores, deberá desconectar estas interfaces primero.

4. Escriba la información en los campos en función de las directrices siguientes:

- **Adaptador padre:** Proporciona información sobre el dispositivo padre de un EtherChannel (por ejemplo, cuando un EtherChannel pertenece a un adaptador Ethernet compartido). Este campo visualiza el valor NINGUNO si el EtherChannel no está incluido en otro adaptador (el valor predeterminado). Si el EtherChannel está contenido en otro adaptador, este campo visualiza el

nombre del adaptador padre (por ejemplo, ent6). Este campo es sólo informativo y no puede modificarse. La opción del adaptador padre está disponible en AIX 5.3 y versiones posteriores.

- **Adaptadores de agregación de enlaces/EtherChannel:** Debería ver todos los adaptadores primarios que se utilicen en la Agregación de enlaces. Estos adaptadores se han seleccionado en el paso anterior.
- **Habilitar dirección alternativa:** Este campo es opcional. Si se establece en sí, podrá especificar la dirección MAC que desee que utilice la Agregación de enlaces. Si se establece esta opción en no, la agrupación de enlaces utilizará la dirección MAC del primer adaptador.
- **Dirección alternativa:** Si se establece **Habilitar dirección alternativa** en sí, especifique aquí la dirección MAC que desee utilizar. La dirección que especifique debe empezar por 0x y ser una dirección hexadecimal de 12 dígitos (por ejemplo, 0x001122334455).
- **Habilitar tramas de gran tamaño de Ethernet en gigabits:** Este campo es opcional. Para poder utilizarlo, el conmutador debe proporcionar soporte a las tramas de gran tamaño. Sólo funciona con una interfaz Ethernet estándar (en), no una interfaz IEEE 802.3 (et). Establézcalo en sí si desea habilitarlo.
- **Modalidad:** Escriba 8023ad.
- **Modalidad hash:** Elija entre las siguientes modalidades hash, que determinan el valor de los datos que el algoritmo utilizará para determinar el adaptador de salida:
  - **valor predeterminado:** En esta modalidad hash, se utilizará la dirección IP de destino del paquete para determinar el adaptador de salida. Para el tráfico que no es IP (como, por ejemplo, ARP), se utiliza el último byte de la dirección MAC de destino para efectuar el cálculo. Esta modalidad garantizará que los paquetes se envíen a través del EtherChannel en el orden en el que se hayan recibido pero es posible que el ancho de banda no se utilice completamente.
  - **src\_port:** Se utiliza el valor del puerto UDP o TCP de origen para determinar el adaptador de salida. Si el paquete no es tráfico UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino.
  - **dst\_port:** Se utiliza el valor del puerto UDP o TCP de destino del paquete para determinar el adaptador de salida. Si el paquete no es tráfico UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino.
  - **src\_dst\_port:** Se utilizan los valores tanto del puerto UDP o TCP de origen como de destino del paquete para determinar el adaptador de salida (de hecho, se añaden los puertos de origen y de destino y, a continuación, se dividen entre dos antes de pasarse al algoritmo). Si el paquete no es tráfico UDP ni TCP, se utiliza el último byte de la dirección IP de destino. Si el paquete no es tráfico IP, se utiliza el último byte de la dirección MAC de destino. Esta modalidad puede proporcionar una buena distribución de los paquetes en la mayoría de situaciones, tanto para los clientes como para los servidores.

Para saber más acerca de la distribución de paquetes y el equilibrado de la carga, consulte el apartado "Opciones para el equilibrado de la carga en EtherChannel" en la página 457.

- **Adaptador de seguridad:** Este campo es opcional. Entre el adaptador que deseé utilizar como copia de seguridad.
- **Dirección Internet con la que realizar ping:** Este campo es opcional y está disponible si tiene uno o más adaptadores en la agregación principal y un adaptador de seguridad. La Agregación de enlaces realizará ping con la dirección IP o el nombre del sistema principal que se especifique aquí. Si la agrupación de enlaces no puede realizar ping con esta dirección durante el número de veces especificado en el campo **Número de reintentos** y a los intervalos especificados en el campo **Tiempo de espera entre reintentos**, la Agregación de enlaces conmutará los adaptadores.
- **Número de reintentos:** Entre el número de fallos a la respuesta de ping que se permite antes de que la agrupación de enlaces conmute los adaptadores. El valor predeterminado es de 3. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.
- **Tiempo de espera entre reintentos:** Entre el número de segundos entre las veces en que la agrupación de enlaces ejecutará pings con la **Dirección Internet con la que realizar ping**. El valor

predeterminado es un segundo. Este campo es opcional y sólo es válido si se ha establecido una **Dirección Internet para realizar ping**.

5. Pulse Intro después de cambiar los campos que desee para crear la Agregación de enlaces.
6. Configure IP a través del dispositivo de Agregación de enlaces que acaba de crearse escribiendo smitty chinet en la línea de mandatos.
7. Seleccione la nueva interfaz de Agregación de enlaces en la lista.
8. Rellene todos los campos necesarios y pulse Intro.

#### **Resolución de problemas con la Agregación de enlaces IEEE 802.3ad**

Utilice el mandato **entstat** para solucionar los problemas con la Agregación de enlaces IEEE 802.3ad.

Si observa problemas con la Agregación de enlaces IEEE 802.3ad, utilice el mandato siguiente para verificar la modalidad de funcionamiento de la Agregación de enlaces:

```
entstat -d dispositivo
```

donde *dispositivo* es el dispositivo de Agregación de enlaces.

Esto también proporcionará una determinación lo más acertada posible del estado del progreso del LACP en base a las LACPDU que se reciban desde el conmutador. Son posibles los valores de estado siguientes:

- **Inactivo:** LACP no se ha inicializado. Éste es el estado cuando una Agregación de enlaces todavía no se ha configurado, porque todavía no se le ha asignado una dirección IP o porque la interfaz se ha desconectado.
- **Negociación:** LACP está en curso pero el conmutador todavía no ha agregado los adaptadores. Si la Agregación de enlaces sigue en este estado durante más de un minuto, compruebe si el conmutador está configurado correctamente. Por ejemplo, debe verificar que LACP esté habilitado en los puertos.
- **Agregado:** LACP ha sido satisfactorio y el conmutador ha agregado los adaptadores juntos.
- **Anómalo:** LACP presenta anomalías. Algunas de las causas posibles son que los adaptadores de la agregación estén establecidos en velocidades de línea o modalidades de dúplex distintas o que estén conectados a conmutadores distintos. Verifique la configuración de los adaptadores.

Además, algunos conmutadores sólo permiten la agregación de puertos contiguos y puede haber alguna limitación en el número de adaptadores que pueden agregarse. Consulte la documentación del conmutador para determinar las posibles limitaciones que el conmutador puede tener y verifique la configuración del conmutador.

**Nota:** El estado de la Agregación de enlaces es un valor de diagnóstico y no afecta la parte de la configuración de AIX. Este valor de estado se ha derivado utilizando un intento lo más acertado posible. Para depurar algún problema de agregación, es mejor verificar la configuración del conmutador.

Las siguientes estadísticas de la Agregación de enlaces IEEE 802.3ad representan el estado de LACP en cada puerto de la agregación.

Se muestran tanto para el actor (la Agregación de enlaces IEEE 802.3ad) como para el asociado (el puerto del conmutador).

**Prioridad del sistema:** valor de prioridad de este sistema

**Sistema:** valor que identifica este sistema de forma exclusiva

**Clave Operacional:** valor que indica los puertos que pueden agregarse juntos

**Prioridad del puerto:** valor de prioridad para este puerto

**Puerto:** valor exclusivo que identifica este puerto en la agregación

**Estado:**

**Actividad de LACP:** Activa o Pasiva - si debe iniciarse el envío de las LACPDU siempre o sólo en respuesta a otra  
    LACPDU: la Agregación de enlaces IEEE 802.3ad siempre funcionará en modalidad activa.

**Tiempo de espera LACP:** Largo o corto - tiempo que debe esperarse antes de enviar las LACPDU: la Agregación de enlaces

IEEE 802.3ad siempre utilizará el tiempo de espera largo

**Agregación:** Individual o Agregable - si este puerto puede formar una agregación con otros puertos o si sólo puede formar una agregación con sigo mismo:  
el puerto de una Agregación de enlaces IEEE 802.3ad de un adaptador se marcará como Individual o Agregable si existe más de un puerto

**Sincronización IN\_SYNC o OUT\_OF\_SYNC** - si la agregación ha determinado que se ha alcanzado la sincronización con el asociado

**Recopilando:** Habilitado o Inhabilitado - si la agregación de enlaces IEEE 802.3ad está recopilando (recibiendo) paquetes

**Distribuyendo:** Habilitado o Inhabilitado - si la agregación de enlaces IEEE 802.3ad está distribuyendo (enviando) paquetes

**Por omisión:** Verdadero o Falso - si la agregación de enlaces IEEE 802.3ad está utilizando los valores predeterminados para la información del asociado

**Caducado:** Verdadero o Falso - si la Agregación de enlaces IEEE 802.3ad se utiliza en modalidad caducada

Las estadísticas siguientes se muestran tanto para cada puerto como de forma agregada:

**LACPDU recibidas:** Paquetes LACPDU recibidos

**LACPDU transmitidas:** Paquetes LACPDU enviados

**PDU de marcador recibidas:** PDU de marcador recibidas

**PDU de marcador transmitidas:** PDU de marcador enviadas:  
esta versión del protocolo no implementa el protocolo de marcador, por lo que las estadísticas siempre estarán a cero

**PDU de respuesta de marcador recibidas:** PDU de marcador recibidas

**PDU de respuesta de marcador transmitidas:** PDU de respuesta de marcador enviadas:  
esta versión del protocolo no implementa el protocolo de marcador, por lo que las estadísticas siempre estarán a cero

**PDU desconocidas recibidas:** PDU de tipo desconocido recibidas

**PDU no válidas recibidas:** PDU de tipo desconocido recibidas  
mal formadas o con una longitud inesperada o un subtipo desconocido

### Ejemplos de interoperabilidad

Tenga en cuenta los siguientes ejemplos de interoperatividad al configurar el EtherChannel o la Agregación de enlaces IEEE 802.3ad.

Después de la tabla se proporciona información adicional sobre cada ejemplo.

<i>Tabla 82. Distintas combinaciones de AIX y de configuración del conmutador y de los resultados que generará cada combinación.</i>		
<b>Modalidad EtherChannel</b>	<b>Configuración del conmutador</b>	<b>Resultado</b>
8023ad	LACP IEEE 802.3ad	Correcto - AIX inicia las LACPDU, lo que desencadena una Agregación de enlaces IEEE 802.3ad en el conmutador.
estándar o round_robin	EtherChannel	Correcto - Se obtiene el comportamiento tradicional del EtherChannel.

*Tabla 82. Distintas combinaciones de AIX y de configuración del conmutador y de los resultados que generará cada combinación. (continuación)*

Modalidad EtherChannel	Configuración del conmutador	Resultado
8023ad	EtherChannel	No deseado - AIX y el Comutador no pueden agregarse. AIX inicia las LACPDU, pero el conmutador no las tiene en cuenta y no envía las LACPDU a AIX. Debido a la falta de LACPDU, AIX no distribuye los paquetes en el enlace/puerto. El resultado es la pérdida de la conectividad de red.
estándar o round_robin	LACP IEEE 802.3ad	No deseado - El conmutador no puede agregarse. El resultado podría ser un rendimiento bajo, ya que el conmutador mueve la dirección MAC entre los puertos del conmutador

A continuación se proporciona una descripción breve de cada combinación de configuración:

- 8023ad con EtherChannel:

En este caso, AIX enviará las LACPDU pero no obtendrán respuesta porque el conmutador funciona como un EtherChannel. El resultado es que, debido a la falta de LACPDU, AIX no utilizará el enlace/puerto para la distribución de paquetes. Esto causará la pérdida de la conectividad de red.

**Nota:** En este caso, el mandato `entstat -d` siempre indicará que la agregación se encuentra en el estado Negociando. Asimismo, en la salida `entstat`, la sección IEEE 802.3ad Port Statistics mostrará que la **Distribución** está inhabilitada para el **Actor**.

- estándar o round\_robin con EtherChannel:

Ésta es la configuración de EtherChannel más frecuente.

- estándar o round\_robin con LACP IEEE 802.3ad:

Esta configuración no es válida. Si el conmutador utiliza LACP para crear una agregación, la agregación nunca se llevará a cabo porque AIX nunca contestará a las LACPDU. Para que funcione correctamente, debería establecerse la modalidad 8023ad en AIX.

### Adaptadores soportados

La Agregación de enlaces IEEE 802.3ad y EtherChannel se soportan en los adaptadores Ethernet de IBM Power Systems Peripheral Component Interconnect-X (PCI-X) y PCI Express (PCIe).

Debe tener en cuenta las siguientes consideraciones adicionales:

- Adaptador Ethernet de E/S virtual

Sólo se proporciona soporte a los adaptadores Ethernet de E/S virtuales en dos configuraciones posibles del EtherChannel:

- Un adaptador Ethernet de E/S virtual como principal y un adaptador Ethernet de E/S virtual como seguridad. En esta configuración, el atributo **Dirección Internet para realizar ping** debe estar habilitado para que el EtherChannel pueda detectar las anomalías en la conectividad remota. Para Virtual I/O Server (VIOS) 2.2.3.0, o posterior, y AIX versión 7.1 con nivel de tecnología 3, o posterior, puede utilizar la característica de estado de enlace ascendente de Ethernet virtual, para detectar el error del adaptador Ethernet compartido (SEA) o el VIOS de servicio, estableciendo el atributo **poll\_uplink** del dispositivo Ethernet virtual en yes.

- Un adaptador Ethernet físico soportado como principal y un adaptador Ethernet de E/S virtual como seguridad. En esta configuración, el atributo **Dirección Internet para realizar ping** debe estar habilitado para que el EtherChannel pueda detectar las anomalías en la conectividad remota.
- Adaptador Ethernet de sistema principal (HEA - Host Ethernet Adapter)

Los puertos lógicos HEA están soportados en EtherChannel si todos los adaptadores dentro de EtherChannel son puertos lógicos HEA. En un puerto HEA dedicado, se da soporte a la agregación con el adaptador PCI/PCI-E. Además, se da soporte a un adaptador Ethernet virtual PCI/PCI-E como adaptador de copia de seguridad (cuando el adaptador primario contenga HEA).

Al utilizar varios puertos lógicos de HEA como adaptadores primarios en un EtherChannel, los puertos físicos asociados con los puertos lógicos de HEA también se deben ubicar en un EtherChannel en el conmutador de Ethernet. En consecuencia, todas las particiones que utilicen puertos lógicos de HEA que van a los mismos puertos físicos de HEA también se deben ubicar en un EtherChannel.

Por ejemplo, supongamos que la Partición 1 está configurada de la siguiente manera:

- Un puerto lógico de HEA fuera del puerto físico de HEA 0
- Un puerto lógico de HEA fuera del puerto físico de HEA 1
- Un EtherChannel creado utilizando los puertos lógicos de HEA anteriores

Si otra partición en el mismo sistema necesita utilizar un puerto lógico de HEA fuera del puerto físico de HEA 0 o fuera del puerto físico de HEA 1, debe crear un EtherChannel para la partición mediante ambos puertos lógicos de HEA, similar a la configuración de la Partición 1. Intentar utilizar cualquiera de dichos puertos lógicos de HEA como puertos autónomos en otras particiones podría generar problemas de conectividad, ya que los paquetes podrían no entregarse al puerto lógico de HEA correcto.

La restricción no existe al utilizar puertos lógicos de HEA en una copia de seguridad de la interfaz de red de configuración (1 primario y 1 de copia de seguridad), debido a que los puertos físicos de HEA no requieren una configuración específica en el conmutador de Ethernet.

**Nota:** Si los puertos lógicos de los puertos físicos HEA están configurados como parte de la agregación LACP (802.3ad), dichos puertos físicos deberán ser exclusivos en dicha LPAR. HMC no impide que se asignen los puertos a otras LPAR, pero no da soporte a la configuración.

- Canal de fibra en Ethernet en adaptadores de red convergentes

La agregación de un enlace, entre un puerto compartido (un puerto que se utiliza para el tráfico Ethernet y para el canal de fibra) y otros adaptadores admitidos, sólo se admite si el conmutador está conectado en el puerto compartido y admite la agregación de enlace sin tener ningún impacto en el tráfico del canal de fibra.

- Adaptadores de virtualización E/S de con una sola raíz (SR-IOV)

La agregación de enlaces con puertos lógicos SR-IOV se puede conseguir utilizando uno de los métodos siguientes:

- Agregación de enlaces IEEE 802.3ad, también conocido como Protocolo de control de agregación de enlaces (LCAP)
- Copia de seguridad de la interfaz de red (NIB)
- Tanto LACP como NIB

Para aplicaciones de red donde el ancho de banda de más de un puerto único es requerido, la agregación de enlace IEEE 802.3ad, se puede utilizar para agregar varios puertos lógicos SR-IOV. Un puerto lógico SR-IOV agregado utilizando la agregación de enlaces IEEE 802.3ad, debe ser el único puerto lógico configurado para el puerto físico. Es posible que el conmutador no gestione adecuadamente varios puertos lógicos SR-IOV configurados para el mismo puerto físico, donde uno de los puertos lógicos SR-IOV está configurado como parte de una configuración de agregación de enlaces IEEE 802.3ad, porque más de un socio LACP puede estar comunicándose a través del puerto físico.

Para evitar la configuración de un segundo puerto lógico SR-IOV en el mismo puerto físico como puerto lógico SR-IOV en una configuración de agregación de enlaces IEEE 802.3ad, el valor de capacidad del puerto lógico debe establecerse en 100 (100%) cuando se configure el puerto lógico.

Para aplicaciones de red donde el ancho de banda de menos de un puerto único es requerido además de protección contra un único error de red, los puertos lógicos SR-IOV pueden ser parte de la configuración NIB. Cuando un puerto lógico SR-IOV se configura como adaptador de copia de seguridad o primario en una configuración NIB, el puerto físico lo pueden compartir otros puertos lógicos SR-IOV. En esta configuración, el atributo **Dirección Internet para realizar ping**, puede estar habilitado para detectar anomalías en la conectividad remota. Los puertos lógicos SR-IOV pueden ser el adaptador de copia de seguridad o el primario para otro puerto lógico SR-IOV, un adaptador Ethernet virtual o un puerto de adaptador físico.

Para obtener información adicional sobre el release relativo a los nuevos adaptadores, consulte las AIXNotas del release que correspondan a su nivel de AIX.

**Importante:** No se proporciona soporte a la combinación de adaptadores de distintas velocidades en el mismo EtherChannel, ni siquiera aunque uno de ellos funcione como adaptador de seguridad. Esto *no* significa que dichas configuraciones no funcionen. El controlador del EtherChannel realiza todos los esfuerzos posibles para funcionar aunque se trate de un caso de distintas velocidades.

### Información relacionada

[Virtualización de E/S con una raíz única](#)

### Resolución de problemas en EtherChannel

Los problemas con EtherChannel pueden deberse a muchas causas.

Puede utilizar el rastreo y las estadísticas como ayuda para el diagnóstico del problema, que puede deberse a temas relativos a la recuperación tras error y las tramas de gran tamaño.

#### Rastreo en EtherChannel

Utilice **tcpdump** y **iptrace** la resolución de problemas con EtherChannel.

El ID de enganche de rastreo es 2FA para los paquetes de transmisión y 2FB para los otros sucesos. No es posible rastrear los paquetes de recepción de EtherChannel en bloque, pero sí rastrear los enganches de rastreo de recepción de cada adaptador.

#### Estadísticas de EtherChannel

Utilice el mandato **entstat** para obtener las estadísticas de agregación de todos los adaptadores de EtherChannel.

Por ejemplo, **entstat ent3** mostrará las estadísticas de agregación de ent3. Si se añade el distintivo **-d**, también se visualizarán las estadísticas de cada adaptador por separado. Por ejemplo, si se escribe **entstat -d ent3** aparecerán las estadísticas de agregación de EtherChannel, así como las estadísticas de cada uno de los distintos adaptadores de EtherChannel.

**Nota:** En la sección Estadísticas generales, el número que aparece en Número de restauraciones del adaptador es el número de recuperaciones. En la copia de seguridad de EtherChannel no se cuenta como una anomalía el retorno al EtherChannel principal desde el adaptador de seguridad. Sólo se cuenta el paso del canal principal a la copia de seguridad.

En el campo Número de adaptadores, el adaptador de seguridad se incluye en el número que aparece.

#### Recuperación tras error lento

Si la recuperación tras error al utilizar la copia de seguridad del EtherChannel o la modalidad de seguridad de la interfaz de red se realiza con lentitud, verifique que no se esté ejecutando el Protocolo de árbol de expansión (STP).

Cuando el conmutador detecta una modificación en la correlación entre el puerto de conmutación y la dirección MAC, ejecuta el algoritmo del árbol de expansión para ver si hay algún bucle en la red. La copia de seguridad del EtherChannel y la copia de seguridad de la interfaz de la red puede provocar un cambio en la correlación entre el puerto y la dirección MAC.

Los puertos de conmutación tienen un contador de retardos de reenvío que determina el tiempo que cada puerto debe esperar tras la inicialización para empezar a reenviar y enviar paquetes. Por este motivo, cuando el canal principal vuelve a habilitarse, se produce un retardo antes de que la conexión vuelva a

establecerse, mientras que la recuperación tras error en el adaptador de seguridad resulta más rápida. Compruebe el contador de retardos de reenvío del conmutador y establezcalo en el valor más pequeño posible para que el retorno al canal principal se produzca con la mayor rapidez posible.

Para que la función de copia de seguridad del EtherChannel funcione correctamente, el contador de retardos de reenvío no debe superar los 10 segundos o es posible que el retorno al EtherChannel principal no funcione correctamente. Es aconsejable establecer el contador de retardos de reenvío en el valor más bajo que el conmutador permita.

#### **Adaptadores sin recuperación tras error**

Si las anomalías de los adaptadores no desencadenan recuperaciones y ejecuta AIX 5.2 con 5200-01 o versiones anteriores, compruebe si la tarjeta del adaptador necesita tener habilitado el sondeo de enlaces para detectar las anomalías en los enlaces.

Algunos adaptadores no pueden detectar el estado de enlace de forma automática. Para detectar esta condición, estos adaptadores deben habilitar un mecanismo de sondeo de enlaces que inicia un temporizador que verifica el estado del enlace periódicamente. El sondeo de enlaces está inhabilitado por omisión. Sin embargo, para que EtherChannel funcione correctamente con estos adaptadores, el mecanismo de sondeo de enlaces debe estar habilitado en cada uno de los adaptadores antes de que se cree el EtherChannel. Si ejecuta AIX 5L Versión 5.2 con el paquete de mantenimiento recomendado 5200-03. y versiones posteriores, el sondeo de enlaces se inicia automáticamente y no hay ningún problema.

Los adaptadores que tienen un mecanismo de sondeo de enlaces cuentan con un atributo del ODM denominado **poll\_link**, que debe estar establecido en **sí** para que se habilite el sondeo de enlaces. Antes de crear el EtherChannel, utilice el mandato siguiente en cada adaptador que deba incluirse en el canal:

```
smitty chgenet
```

Cambie el valor de **Habilitar sondeo de enlaces** a **sí** y pulse Intro.

#### **Tramas de gran tamaño**

Aparte de habilitar el atributo **use\_jumbo\_frame** en el EtherChannel, también debe habilitar las tramas de gran tamaño en cada adaptador antes de crear el EtherChannel.

Para ello, ejecute el mandato siguiente:

```
smitty chgenet
```

Las tramas de gran tamaño se habilitan de forma automática en todos los adaptadores subyacentes cuando el atributo **use\_jumbo\_frame** de un EtherChannel se establece en yes.

#### **Vuelco remoto**

El vuelco remoto no está soportado a través de un EtherChannel.

### **Protocolo Internet a través de InfiniBand (IPoIB)**

Los paquetes IP (Protocolo Internet) pueden enviarse a través de una interfaz InfiniBand (IB). Este transporte se realiza encapsulando los paquetes IP de los paquetes IB utilizando una interfaz de red.

Para utilizar IP a través de IB, debe instalar y configurar en el sistema el controlador del gestor de conexiones de InfiniBand (ICM) y por lo menos un dispositivo IB. Para ver si un dispositivo IB ya está instalado, ejecute el mandato `lsdev -C | grep iba`. El nombre del archivo que contiene la interfaz IB es: `devices.common.IBM.ib`. El archivo `devices.chrp.IBM.lhca` es un ejemplo de un archivo de adaptador al que se proporciona soporte actualmente.

Para configurar un controlador ICM, consulte el apartado “[Configuración de un controlador del Gestor de comunicaciones InfiniBand](#)” en la página 474.

Para poder crear la interfaz InfiniBand (IB IF), IB IF deberá poder unirse a un grupo de difusión general-multidifusión con una clave facilitada por el usuario PKEY (o bien se utiliza un valor predeterminado PKEY = 0xFFFF si el usuario no ha facilitado ninguna clave) y una clave Q\_Key facilitada por el usuario (o se

utiliza un valor predeterminado Q\_Key = 0x1E si el usuario no ha facilitado ninguna clave). Un grupo de difusión general-multidifusión es un grupo de multidifusión al que la interfaz debe unirse para enviar paquetes **ARP** y de difusión general. Si no existe ningún grupo de difusión general-multidifusión o no se puede crear mediante la interfaz, la creación de IB IF no se realizará correctamente.

Es posible crear o modificar una IF IB utilizando la interfaz de la línea de mandatos o la interfaz del usuario de SMIT. Los parámetros necesarios para crear una IF IB son los siguientes:

- *nombre de la interfaz*
- *nombre del adaptador*
- *número de puerto*
- *dirección IP de la interfaz*

Los parámetros siguientes sirven para modificar la IF IB:

- *dirección Internet*
- *máscara de red*
- *tamaño de MTU* (igual a la MTU que se desee menos 4 bytes para la cabecera de IB)
- *estado*
- *Tamaño de cola de envío y recepción (el valor predeterminado es 4000)*
- *Clave de cola de multidifusión*
- *Superpaquete activado o desactivado*

A continuación se proporciona un ejemplo del mandato utilizado para crear una IF IB desde la línea de mandatos:

```
$ /usr/sbin/mkiba -i ib0 -p 1 -A iba0 -a 1.2.3.8 [-P -1 -S "up" -m "255.255.254.0" -M 2044]
```

donde:

Item	Descripción
-M 2044	Unidad de transmisión máxima.
-m "255.255.254.0"	Máscara de red.
-p 1	Número de puerto (si no se proporciona, el valor predeterminado es 1).
-A iba0	Nombre del dispositivo de IB.
-a 1.2.3.8	Dirección IP de IF.
-i ib0	Nombre de la interfaz.
-P -1	Clave de partición (si no se proporciona, el valor predeterminado es PKEY. Una vez creada la interfaz no es posible modificar PKEY; el usuario debe conseguir del administrador de la red una PKEY que no tenga el valor predeterminado.)
-S "up"	Estado de la interfaz.
-q 8000	Tamaño de colas de recepción y transmisión (cada uno).
-Q 0x1E	Clave de cola de multidifusión asignada al grupo de multidifusión (adopta el valor predeterminado de Q_KEY = 0x1E si no se ha facilitado).
-k "on"	El superpaquete permitirá que MTU sea de 64KB. Para poder funcionar no tiene que estar habilitado en el sistema principal remoto.

A continuación se proporciona un ejemplo del mandato utilizado para crear una IF IB desde la interfaz del usuario de SMIT:

```
$ smitty inet
```

Cuando aparezca el menú Selección de interfaz de red, siga el procedimiento siguiente:

1. Seleccione **Añadir una interfaz de red** o **Modificar/Mostrar características de una interfaz de red**.  
Aparece el menú Añadir una interfaz de red.
2. En el menú Añadir una interfaz de red, seleccione **Añadir una interfaz de red IB**. Aparecer el menú Añadir una interfaz de red IB.
3. En el menú Añadir una interfaz de red IB, efectúe las modificaciones necesarias y pulse Intro.

#### **Creación, visualización, adición, supresión de entradas ARP y modificación de temporizadores**

Una entrada **ARP (Protocolo de resolución de direcciones)** permite que una interfaz se comunique con otra interfaz aunque no estén en el mismo grupo de multidifusión.

Una entrada **ARP** puede crearse manualmente utilizando el mandato `arp -t ib`.

Para visualizar todas las entradas **ARP**, ejecute el mandato `$ arp -t ib -a`. Si desea visualizar un número concreto de entradas **ARP**, puede especificar el número. Por ejemplo, `$ arp -t ib -a 5` muestra 5 entradas **ARP**.

El mandato siguiente añade una entrada **ARP**:

```
$ arp -t ib -s nombre de interfaz IB dlid <DLID de 16 bits> dgq  
Número de par de cola de destino hex de 16 bits  
ipaddr <Dirección IP de destino>
```

donde:

Item	Descripción
<i>DLID</i>	es el ID local de destino.
<i>DGID</i>	es el ID global de destino.

El mandato siguiente elimina una entrada **ARP**:

```
$ arp -t ib -d Dirección IP
```

Los siguientes valores modifican los valores de temporizador de la entrada ARP para entradas ARP completas e incompletas. Estos valores se utilizan para eliminar las entradas ARP tras un periodo de tiempo:

```
arp -t ib -i <número en minutos completos para eliminar las entradas ARP incompletas>  
-c <número en minutos completos para eliminar las entradas ARP completas>
```

El tiempo predeterminado actual para que se eliminan las entradas ARP incompletas es de 3 minutos. Para las entradas ARP completas, el tiempo predeterminado es 24 horas. Si se tienen que cambiar los valores, la ejecución del mandato sólo cambiará para todas las interfaces actuales configuradas (o en un estado definido). Si se configuran interfaces nuevas, deberá volverse a ejecutar el mandato. Los valores también cambian en ODM.

Los valores pueden cambiar dinámicamente a una interfaz específica ejecutando el mandato **ifconfig**:

```
Para cambiar el temporizador de entrada ARP incompleta  
ifconfig ib0 inc_timer 4  
ifconfig ib0 com_timer 60
```

#### **Modificación de los parámetros de una interfaz InfiniBand**

Para modificar los parámetros de una IF IB, utilice la interfaz del usuario de SMIT o los mandatos de la línea de mandatos.

Para modificar los parámetros de una IF IB utilizando SMIT:

1. Ejecute el mandato `$ smitty inet`.  
Aparece el menú Selección de interfaz de red.

2. En el menú Selección de interfaz de red, seleccione **Modificar/Mostrar características de una interfaz de red**.

Aparece el menú Interfaces de red disponibles.

3. En el menú Interfaces de red disponibles, seleccione **Interfaz InfiniBand**.

Aparece el menú Modificar/Mostrar una interfaz IB.

4. Modifique los parámetros que desee.

Para modificar los parámetros de la IF en la línea de mandatos, ejecute el mandato \$ ifconfig. El mandato siguiente modifica los parámetros de la IF IB desde la línea de mandatos:

```
$ ifconfig ib0 [ib_port número de puerto mtu unidad de transmisión máxima p_key  
clave de partición hex de 16 bits ib_adapter nombre de adaptador InfiniBand netmask  
decimales con puntos]
```

```
$ ifconfig ib0 inc_timer 3 com_timer 60
```

- *inc\_timer* es el tiempo en minutos que una entrada ARP incompleta tardará en caducar. El valor predeterminado es 2 minutos.
- *com\_timer* es el tiempo en minutos que una entrada ARP incompleta tardará en caducar. El valor predeterminado es 24 horas.

### Configuración de un controlador del Gestor de comunicaciones InfiniBand

Siga este procedimiento para configurar un Gestor de comunicaciones InfiniBand.

1. Ejecute el mandato \$ smitty icm.

Aparece el menú Gestor de comunicaciones InfiniBand.

2. En el menú Gestor de comunicaciones InfiniBand, seleccione **Añadir un Gestor de comunicaciones InfiniBand**.

3. En el menú Añadir un Gestor de comunicaciones InfiniBand, seleccione **Añadir un Gestor de comunicaciones InfiniBand**.

Aparece el menú Nombre del Gestor de comunicaciones IB a añadir.

4. En el menú Nombre del gestor de comunicaciones IB a añadir, seleccione **icm InfiniBand de gestión**.

5. Utilice los valores predeterminados o modifique los parámetros necesarios y, a continuación, pulse Intro.

## Iniciador de software iSCSI y destino del software

El iniciador de software iSCSI permite a AIX acceder a dispositivos de almacenamiento utilizando TCP/IP en adaptadores de red Ethernet. El software iSCSI permite a AIX exportar almacenamiento local para que otros iniciadores iSCSI accedan al mismo utilizando el protocolo iSCSI definido en la RFC 3720.

La utilización de la tecnología iSCSI, que normalmente se conoce como tecnología SAN sobre IP, permite el despliegue de red de área de almacenamiento sobre una red IP. iSCSI es un planteamiento abierto basado en estándares mediante el cual **TCP/IP** encapsula la información SCSI para permitir el transporte a través de redes Ethernet y Gigabit Ethernet. iSCSI permite que una red Ethernet existente transfiera datos y mandatos SCSI con total independencia de la ubicación. Las soluciones iSCSI utilizan los siguientes componentes diferentes, pero integralmente relacionados:

- Iniciadores

Son los controladores de dispositivo que residen en el cliente. Encapsulan mandatos SCSI y los direccionan a través de la red IP al dispositivo de destino.

- Software de destino

El software recibe los mandatos SCSI encapsulados a través de la red IP. El software también puede proporcionar soporte de configuración y soporte de gestión de almacenamiento.

- Hardware de destino

El hardware puede ser un equipo de almacenamiento que contiene almacenamiento incorporado. El hardware también puede ser un producto de pasarela o puente que no contenga almacenamiento interno propio.

### Configuración del iniciador de software iSCSI

El iniciador de software se configura utilizando SMIT, como se ve en este procedimiento.

1. Seleccione **Dispositivos**.
2. Seleccione **iSCSI**.
3. Seleccione **Configurar dispositivo de protocolo iSCSI**.
4. Seleccione **Cambiar/Mostrar características de un dispositivo de protocolo iSCSI**
5. Verifique que el valor de **Nombre de iniciador** sea correcto.

El dispositivo de destino iSCSI utiliza el valor **Nombre de iniciador** durante la operación de inicio de sesión.

**Nota:** Un nombre de iniciador predeterminado se asigna cuando se instala el software. Puede cambiar el nombre del iniciador para que se ajuste a los convenios de denominación de la red local. Si utiliza varios dispositivos de iniciador iSCSI, debe asignar un nombre exclusivo a cada dispositivo de iniciador.

6. El campo **Destinos máximos permitidos** indica el número máximo de dispositivos de destinos iSCSI que se pueden configurar.  
Si reduce este número, también reducirá la cantidad de memoria de red asignada previamente para el controlador de protocolo iSCSI durante la configuración.
7. Configure el método de descubrimiento iSCSI utilizando el campo **Política de descubrimiento** para descubrir los dispositivos de destino iSCSI.

El software iniciador de iSCSI da soporte a los siguientes métodos de descubrimiento:

#### archivo

La información sobre los dispositivos de destino se almacena en un archivo de configuración.

**Nota:** Si el campo **Política de descubrimiento** se establece en **file**, los nombres de los dispositivos de destino iSCSI se leen desde el archivo especificado en el atributo **Nombre de archivo de descubrimiento**. Si utiliza varias instancias del iniciador de software iSCSI, debe crear varios archivos de descubrimiento si los dispositivos de iniciador acceden a distintos dispositivos de destino iSCSI.

#### odm

La información sobre los destinos se almacena en los objetos Gestor de datos de objeto (ODM). Al utilizar un disco iSCSI como un disco de arranque o como parte del arranque **rootvg**, debe utilizarse el método de descubrimiento **odm**. Consulte [Adición de un destino iSCSI descubierto estadísticamente en ODM](#).

#### isns

La información sobre destinos se almacena en un servidor iSNS (internet Storage Name Service) y se recupera automáticamente durante la configuración del iniciador iSCSI.

#### slp

La información sobre los destinos se almacena en un agente de servidores de Service Location Protocol (SLP) o en un agente de directorios y se recupera automáticamente durante la configuración del iniciador de iSCSI.

8. Seleccione un valor para el atributo **isw\_err\_recov**, o **delayed\_fail** o **fast\_fail**. Este atributo le permite definir cuántas veces intentará el iniciador iSCSI recuperarse de errores de red. El valor **delayed\_fail** representa el comportamiento predeterminado que utiliza el iniciador iSCSI. El valor **delayed\_fail** se recomienda para entornos que tienen una sola vía de acceso iSCSI a los dispositivos. El valor **fast\_fail** reduce varios valores de tiempo de espera y reintentos que utiliza el iniciador de software iSCSI. Este valor se recomienda cuando se utilizan varias vías de acceso al dispositivo iSCSI (MPIO), o cuando los dispositivos iSCSI están utilizando duplicación LVM. En estas situaciones, si se utiliza el valor **fast\_fail** value, el sistema operativo AIX comuta más rápidamente a otra vía de acceso que funcione cuando una vía de acceso tiene un corte de red.

9. Seleccione los valores requeridos para los atributos **initial\_r2t** y **immediate\_data**. De forma predeterminada, el atributo **initial\_r2t** se establece en yes y el atributo **immediate\_data** se establece en no. Puede conmutar estos valores.

Si establece el atributo **initial\_r2t** en no, el dispositivo de iniciador de software iSCSI puede negociar con el dispositivo de destino iSCSI para que no utilice una unidad de datos de protocolo (PDU) inicial preparada para transferencia mientras se graban datos en el disco iSCSI. Si establece el atributo **immediate\_data** en yes, el dispositivo de iniciador de software iSCSI puede negociar con el dispositivo de destino iSCSI para enviar los datos de inmediato al disco iSCSI. Si selecciona los valores adecuados para los atributos **initial\_r2t** e **immediate\_data**, mejorará el rendimiento de la grabación de datos en los discos iSCSI.

Después de que el iniciador de software se haya configurado, realice lo siguiente:

1. Si la política de descubrimiento es **archivo**, edite el archivo /etc/iscsi/targets para incluir los destinos iSCSI necesarios durante la configuración del dispositivo.

Cada línea no comentada del archivo representa un destino iSCSI. Para obtener más información, consulte el [Archivo targets](#) en la publicación *Referencia de archivos*.

Si la política de descubrimiento es **odm**, utilice el mandato **mkiscsi** o los paneles de smit para crear las definiciones de destino en ODM. Para obtener más información, consulte [Adición de un destino iSCSI descubierto estadísticamente en ODM](#).

Si la política de descubrimiento es **isns** o **slp**, asegúrese de que el servidor iSNS o SLP esté adecuadamente configurado y accesible mediante el iniciador de iSCSI.

La configuración de dispositivo iSCSI necesita que se puedan alcanzar los destinos iSCSI mediante una interfaz de red configurada adecuadamente. Si bien el iniciador de software iSCSI puede trabajar con una LAN de Ethernet 10/100, está diseñado para ser utilizado con una red Ethernet gigabit separada de otro tráfico de red.

2. Tras definir los destinos, escriba el mandato siguiente:

```
cfgmgr -l iscsi0
```

Este mandato vuelve a configurar el controlador del iniciador de software. Hace que el controlador intente comunicarse con los destinos listados en el archivo /etc/iscsi/targets y defina un nuevo hdisk para cada LUN de los destinos que se encuentran. Para obtener más información, consulte la descripción del mandato **cfgmgr**.

**Nota:** Si no se han definido los discos apropiados, revise la configuración del iniciador, el destino y las pasarelas iSCSI para asegurarse de que son correctos y, a continuación, vuelva a ejecutar el mandato **cfgmgr**.

Si desea configurar adicionalmente los parámetros para los dispositivos de iniciador de software iSCSI, utilice SMIT como se indica a continuación:

1. Seleccione **Dispositivos**.

2. Seleccione **Disco fijo**.

Un dispositivo iniciador de software típico se muestra de una manera similar a la del ejemplo siguiente:

hdisk2	Disponible	Otras unidades de disco iSCSI
--------	------------	-------------------------------

Si el disco iSCSI soporta colas de códigos de mandato y NACA=1 en el byte de control, tenga en cuenta la posibilidad de cambiar el valor de profundidad de cola del disco por un valor mayor. Un valor más grande podría ayudar a mejorar el rendimiento del dispositivo. El valor de profundidad de cola óptima no puede exceder el tamaño de cola real en la unidad. Si se establece la profundidad de cola en un valor mayor que el del tamaño de cola de la unidad, posiblemente se degradará el rendimiento. Para determinar el tamaño de cola de la unidad, consulte la documentación de la unidad.

## **Configuración de varios dispositivos de iniciador de software iSCSI**

El software iSCSI (Internet Small Computer Systems Interface) crea un dispositivo que representa el iniciador de software iSCSI. De forma predeterminada, el dispositivo se denomina `iscsi0`. Este dispositivo tiene un atributo **initiator\_name** que contiene el nombre iSCSI asociado al dispositivo.

Puede crear varios dispositivos de iniciador de software iSCSI en una única instancia del sistema operativo AIX. Disponer de varios dispositivos de iniciador de software iSCSI ofrece las ventajas siguientes:

- Puede crear con facilidad varias vías de acceso de E/S de multivía de acceso (MPIO) para un disco iSCSI que admite MPIO. Cada vía de acceso MPIO crea su propia conexión del socket TCP/IP, de manera que el tráfico de datos de iSCSI se distribuye entre más conexiones para mejorar el rendimiento incrementando el procesamiento simultáneo.
- Las distintas solicitudes de E/S de iSCSI se pueden separar de forma lógica. Los discos del dispositivo `iscsi0` pueden ser utilizados por una aplicación, mientras que los discos del dispositivo `iscsi1` pueden ser utilizados por otra aplicación. En estos casos, separar las solicitudes de E/S reduce la posibilidad de conflictos de solicitudes de E/S entre aplicaciones.

Para crear un dispositivo de iniciador de software iSCSI, ejecute el mandato siguiente:

```
mkdev -c driver -s node -t iscsi -d
```

Este mandato crea el un dispositivo de iniciador de software iSCSI e imprime el nombre en el dispositivo. Para crear varios dispositivos de iniciador, utilice el mandato **mkdev**. Se sugiere que no cree ni utilice más de 8 dispositivos de iniciador iSCSI.

Una vez creado el dispositivo, tiene que asignar un nombre exclusivo al dispositivo. Puede utilizar el mandato **chdev** para establecer el atributo **initiator\_name** del nuevo dispositivo. También tiene que configurar el nuevo dispositivo para que acceda a determinados dispositivos de destino de iSCSI, de una manera similar a la configuración aplicada al dispositivo `iscsi0`. Si crea varios dispositivos de iniciador de software iSCSI, puede configurar los dispositivos para que accedan a los mismos dispositivos de destino de iSCSI o a distintos dispositivos de destino de iSCSI.

Si dos dispositivos de iniciador acceden a los mismos dispositivos de destino y utilizan la política de descubrimiento de archivos (es decir, si el atributo **disc\_policy** se ha establecido en `file`), los dos dispositivos de iniciador podrían apuntar al mismo nombre de archivo. Si dos dispositivos de iniciador acceden a distintos dispositivos de destino, los dos dispositivos de iniciador deberán apuntar a nombres de archivos diferentes. Si dos dispositivos de iniciador acceden a los mismos dispositivos de destino y utilizan la política de descubrimiento del Gestor de Datos Objeto (ODM) (es decir, si el atributo **disc\_policy** se ha establecido en `odm`), es necesario duplicar las entradas de ODM para el primer dispositivo de iniciador, a fin de que aparezcan en la lista del segundo dispositivo de iniciador. Puede utilizar el mandato **cpiscsi** para duplicar la configuración del dispositivo de destino iSCSI.

## **Configuración del destino de software iSCSI**

El controlador de destino de software iSCSI permite que AIX funcione como un dispositivo de destino o como varios dispositivos de destino iSCSI. El controlador de destino iSCSI exporta discos locales, volúmenes lógicos o archivos locales a iniciadores iSCSI que se conectan a AIX mediante el protocolo iSCSI y TCP/IP.

Cada dispositivo de destino tiene un nombre completo iSCSI y un conjunto de números de unidad lógica (LUN) que están a disposición de los iniciadores que se conectan al destino iSCSI virtual. Para cada dispositivo de destino, puede especificar qué números de interfaz de red y de puerto TCP/IP puede utilizar el controlador de destino para aceptar conexiones entrantes.

**Nota:** Es necesario tener instalado el conjunto de archivos de destino iSCSI. El nombre de conjunto de archivos es `devices.tmisccsw.rte` y el conjunto de archivos está incluido en el paquete de expansión de AIX.

Para configurar un controlador de destino iSCSI, complete los pasos siguientes:

1. Cree una instancia única del controlador de destino iSCSI utilizando la siguiente vía de acceso de SMIT. Esta instancia funciona como un contenedor para los otros objetos iSCSI.

**Dispositivos > iSCSI > Dispositivo de destino iSCSI > Dispositivo de protocolo de destino iSCSI > Añadir un dispositivo de protocolo de destino iSCSI**

2. Cree un dispositivo de destino iSCSI para cada destino iSCSI virtual que esté asignado por el controlador de dispositivo iSCSI. Utilice la siguiente vía de acceso de SMIT para crear cada dispositivo de destino iSCSI:

**Dispositivos > iSCSI > Dispositivo de destino iSCSI > Destinos iSCSI > Añadir un destino iSCSI**

3. Defina uno o varios LUN para cada dispositivo de destino utilizando la siguiente vía de acceso de SMIT:

**Nota:** Los LUN son accesibles mediante iniciadores que se conectan a un destino virtual. En el destino iSCSI, cada LUN puede estar asociado a un volumen lógico definido previamente, a un volumen físico o a un archivo creado previamente en un sistema de archivos local. El sistema AIX no puede utilizar de ninguna otra manera el volumen físico que esté asociado a una unidad lógica de destino iSCSI.

**Dispositivos > iSCSI > Dispositivo de destino iSCSI > LUN de destino iSCSI**

Por lo general, con este paso se completa la configuración. Pero si utiliza el protocolo de autenticación por desafío mutuo (CHAP) o bien si utiliza Listas de control de accesos (ACL) para indicar qué iniciadores pueden acceder a qué LUN, será necesario un paso adicional para completar la configuración de destino.

- Si utiliza la autenticación CHAP de los iniciadores, edite el archivo /etc/tmiscsi/autosecrets y añada los secretos utilizados por los iniciadores para iniciar la sesión. El archivo /etc/tmiscsi/autosecrets contiene una entrada por destino. Cada entrada contiene el formato siguiente:

*nombre\_destino nombre\_chap secreto\_chap*

- Si va a utilizar las ACL para indicar qué iniciadores pueden acceder a qué LUN, edite el archivo /etc/tmiscsi/access\_lists y añada una entrada por destino. Cada entrada contiene el formato siguiente:

*nombre\_destino/nombre\_lun nombre\_iSCSI, nombre\_iSCSI,...*

**Información relacionada**

[/etc/tmiscsi/autosecrets](#)

[/etc/tmiscsi/access\\_lists](#)

[/etc/tmiscsi/isns\\_servers](#)

**Consideraciones sobre el iniciador de software iSCSI**

Tenga en cuenta lo siguiente cuando trate con iniciadores de software iSCSI.

- Descubrimiento de destino

El iniciador de software de iSCSI da soporte a los siguientes cuatro formatos de descubrimientos de destino:

**archivo**

Se utiliza un archivo de texto para configurar cada destino.

**odm**

Los objetos ODM se utilizan para configurar cada destino. Al utilizar un disco iSCSI como un disco de arranque o como parte del arranque rootvg, debe utilizarse el método de descubrimiento **odm**.

**isns**

Cada destino se registra en uno o más de los servidores de Internet Storage Name Service (iSNS).

**slp**

Cada destino se registra en uno o más de los agentes de directorios o de agentes de servicios de Service Location Protocol (SLP).

- Autentificación iSCSI

El iniciador de software iSCSI utiliza el nombre calificado iSCSI local como nombre del Protocolo de autenticación por desafío mutuo (CHAP) si el nombre CHAP no se especifica. Es posible que el archivo targets o la configuración de ODM especifiquen un nombre CHAP alternativo. Para obtener más

información sobre cómo especificar el nombre CHAP, consulte la información de referencia del archivo `targetso` el mandato [`mkiscsi`](#).

Sólo se puede utilizar CHAP (MD5) para configurar la autenticación de iniciador. La autenticación de destino no se implementa.

- Iniciador de software iSCSI MPIO

El iniciador de software iSCSI de AIX da soporte a múltiples vías de acceso de E/S (MPIO). Si está utilizando el archivo o bien la política de descubrimiento ODM, añada entradas para conectar con varios puertos de un dispositivo de almacenamiento, utilizando varias interfaces de red de AIX. El controlador iSCSI reconoce varias vías de acceso al mismo dispositivo y las configura en una configuración MPIO. Esto es similar a la configuración MPIO para otros protocolos de dispositivos de almacenamiento.

Si está utilizando definiciones ODM de discos iSCSI de terceros, asegúrese de que estén instaladas las versiones más recientes disponibles de esas definiciones para utilizar múltiples vías de acceso a los discos iSCSI.

- Número de LUN configurados

El número máximo de LUN configurados probados utilizando el iniciador de software iSCSI es de 128 por destino iSCSI. El iniciador de software utiliza una sola conexión TCP para cada destino iSCSI (una conexión por sesión iSCSI). Esta conexión TCP se comparte entre todos los LUN configurados para un destino. Los espacios de envío y de recepción de socket TCP del iniciador de software se establecen ambos en el máximo de almacenamiento intermedio de socket del sistema. El máximo lo establece la opción de red **`sb_max`**. El valor predeterminado es 1 MB.

- Grupos de volúmenes

Para evitar problemas de configuración y entradas del registro de errores al crear grupos de volúmenes utilizando dispositivos iSCSI, siga estas directrices:

- Configure grupos de volúmenes que se crean utilizando dispositivos iSCSI para que estén en estado inactivo después del rearranque. Cuando los dispositivos iSCSI estén configurados, active manualmente los grupos de volúmenes respaldados por iSCSI. A continuación, monte los sistemas de archivo asociados.

Los grupos de volúmenes se activan durante una fase de arranque diferente de la del controlador de software iSCSI. Por esta razón, no es posible de activar los grupos de volúmenes iSCSI durante el proceso de arranque.

- No fragmente grupos de volúmenes en dispositivos no iSCSI.

- Anomalías de E/S

Si se pierde la conectividad con los dispositivos de destino iSCSI, se producen anomalías de E/S. Para evitar anomalías de E/S y que se corrompa el sistema de archivos, detenga toda la actividad de E/S y desmonte los sistemas de archivos respaldados por iSCSI antes de realizar cualquier acción que produzca una pérdida de conectividad a largo plazo a los destinos iSCSI activos.

Si se produce una pérdida de conectividad a los destinos iSCSI mientras las aplicaciones intentan actividades de E/S con dispositivos iSCSI, finalmente se producirán errores de E/S. Es posible que no se puedan desmontar los sistemas de archivos respaldados por iSCSI porque el dispositivo iSCSI subyacente permanece ocupado.

Se deberá realizar el mantenimiento del sistema de archivos si se producen anomalías de E/S debido a la pérdida de conectividad a los destinos iSCSI activos. Para realizar el mantenimiento del sistema de archivos, ejecute el mandato **`fsck`**.

- No utilice el iniciador de software iSCSI de AIX ni el destino de software de iSCSI de AIX con la interfaz de bucle de retorno (1o0). El proceso de la interrupción de la interfaz de bucle de retorno se diferencia del proceso de la interrupción de interfaz de red del adaptador Ethernet virtual o físico. El sistema operativo AIX debe detener operaciones si la interfaz de bucle de retorno se utiliza con los controladores de software iSCSI.

## Información relacionada

[Adición de un destino iSCSI descubierto estáticamente a ODM](#)

### **Consideraciones acerca de la seguridad iSCSI**

El directorio /etc/iscsi, el directorio /etc/tmisco y los ficheros de dichos directorios están protegidos de los usuarios sin privilegios mediante el permiso y la propiedad de archivos.

Los secretos CHAP se guardan en el archivo /etc/iscsi/targets y en el archivo /etc/tmisco/autosecrets como texto claro.

**Nota:** No cambie el permiso de archivo y la propiedad originales de estos archivos.

### **Consideraciones acerca del rendimiento de iSCSI**

Establezca las configuraciones siguientes para obtener el mejor rendimiento de iSCSI.

Para asegurar el mejor rendimiento:

- Habilite las características de Gran envío de TCP, de control de flujo de envío y recepción TCP y de Tramas de gran tamaño del Adaptador Gigabit Ethernet de AIX y la interfaz de Destino iSCSI.
- Ajuste las opciones de red y los parámetros de interfaz para el máximo rendimiento de E/S iSCSI en el sistema AIX como se indica a continuación:
  - Habilite la opción de red RFC 1323.
  - Configure las opciones de red **tcp\_sendspace**, **tcp\_recvspace**, **sb\_max** y **mtu\_size** y las opciones de interfaz de red a los valores apropiados.

El tamaño de transferencia máximo del Iniciador de software iSCSI es de 256 KB. Suponiendo que los máximos de sistemas para **tcp\_sendspace** y **tcp\_recvspace** se establezcan en 262144 bytes, un mandato **ifconfig** utilizado para configurar una interfaz Gigabit Ethernet puede tener el aspecto siguiente:

```
ifconfig en2 10.1.2.216 mtu 9000 tcp_sendspace 262144 tcp_recvspace 262144
```

- Establezca la opción de red **sb\_max** en un mínimo de 524288 y, preferiblemente, en 1048576.
- Establezca **mtu\_size** en 9000.
- Para algunos destinos iSCSI, se debe inhabilitar el algoritmo TCP Nagle para obtener un rendimiento óptimo. Utilice el mandato **no** para establecer el parámetro **tcp\_nagle\_limit** en 0, lo que inhabilitará el algoritmo Nagle.

Para obtener más información y parámetros de ajuste adicionales, consulte el [ajuste de rendimiento de TCP y UDP](#).

### **Consideraciones sobre el destino del software iSCSI**

Cuando vaya a definir un destino de software iSCSI y vaya a exportar números de unidad lógica (LUN), tenga en cuenta lo siguiente:

- El nombre completo iSCSI (IQN) de cada destino virtual se especifica en la herramienta SMIT cuando se ha definido un destino de software. El panel de la herramienta SMIT no restringe el formato del nombre. Sin embargo, algunos iniciadores de software iSCSI precisan que se especifique el IQN en el formato definido por el protocolo iSCSI. Si se utiliza un formato de nombre incorrecto, ello podría impedir que el iniciador iniciara la sesión en el destino y accediera a los discos exportados por el destino.

Para mostrar el nombre actual de un dispositivo de destino iSCSI, complete los pasos siguientes:

1. Ejecute un mandato similar al siguiente. Para este ejemplo, se presupone que el dispositivo de destino iSCSI es **target0**.

```
lsattr -E -l target0
```

2. Compruebe el atributo **iscsi\_name**.

- Los datos de consulta devueltos para un LUN exportado contienen los valores siguientes:

- ID de proveedor: AIX
- ID de producto: **iSCSI\_VDASD**
- Número de versión ANSI: 3

- No utilice el iniciador de software iSCSI de AIX ni el destino de software de iSCSI de AIX con la interfaz de bucle de retorno (lo0). El proceso de la interrupción de la interfaz de bucle de retorno se diferencia del proceso de la interrupción de interfaz de red del adaptador Ethernet virtual o físico. El sistema operativo AIX debe detener operaciones si la interfaz de bucle de retorno se utiliza con los controladores de software iSCSI.

## Protocolo de transmisión de control de corriente (Stream Control Transmission Protocol)

**SCTP (Stream Transmission Control Protocol - Protocolo de control de transmisiones de corrientes)** es un protocolo orientado a las conexiones, similar a TCP, pero proporciona la transferencia de datos orientada a mensajes, similar a **UDP**. El sistema operativo AIX cumple con RFC 4960.

La tabla siguiente describe las diferencias generales del comportamiento entre SCTP y los protocolos de transporte existentes, TCP y UDP.

Tabla 83. Diferencias entre TCP, UDP y SCTP			
Atributo	TCP	UDP	SCTP
Fiabilidad	Fiable	No fiable	Fiable
Gestión de conexiones	Orientado a conexión	Sin conexión	Orientado a conexión
Transmisión	Orientado a bytes	Orientado a mensaje	Orientado a mensaje
Control de flujo	Sí	No	Sí
Control de congestión	Sí	No	Sí
Tolerancia de errores	No	No	Sí
Entrega de datos	Estrictamente ordenada	Desordenada	Parcialmente ordenada
Seguridad	Sí	Sí	Mejorada

En general, **SCTP** puede proporcionar más flexibilidad para determinadas aplicaciones, por ejemplo **Voice over IP (VoIP)**, que requieren la transferencia de datos fiable pero orientada a mensajes. Para esta categoría de aplicaciones, probablemente **SCTP** es más adecuado que **TCP** o **UDP**.

- **TCP** proporciona entrega de datos de orden de transmisión fiable y estricta. Para aplicaciones que necesitan fiabilidad, pero pueden tolerar la entrega de datos no ordenados o parcialmente ordenados, **TCP** puede producir algún retardo innecesario debido al bloqueo de cabecera de línea. Con el concepto de varias corrientes en una sola conexión, **SCTP** puede proporcionar entrega estrictamente ordenada en una corriente mientras se aislan los datos de forma lógica de las corrientes diferentes.
- **SCTP** está orientado a mensajes, a diferencia de **TCP**, que está orientado a bytes. Debido a la naturaleza orientada a bytes de **TCP**, la aplicación tiene que añadir su propia marca de registro para mantener los límites de mensaje.
- **SCTP** proporciona cierto grado de tolerancia a errores utilizando la característica de varios inicios. Se considera que un sistema principal tiene varios inicios cuando tiene conectada más de una interfaz de red, en la misma red o en redes diferentes. Se puede establecer una asociación **SCTP** establecida entre dos sistemas principales de varios inicios. En este caso, todas las direcciones IP de ambos puntos finales se intercambian en el arranque de asociación; esto permite que cada punto final utilice cualquiera de estas direcciones durante el tiempo de vida de la conexión si una de las interfaces está inactiva por cualquier razón, a condición de que se pueda alcanzar el igual mediante las interfaces alternativas.
- **SCTP** proporciona características de seguridad adicionales que **TCP** y **UDP** no proporcionan. En **SCTP**, la asignación de recursos durante la configuración de asociación se retarda hasta que la identidad del cliente se puede verificar utilizando un mecanismo de intercambio cookie, reduciendo de este modo la posibilidad de ataques de rechazo de servicio.

### Arranque y cierre de asociación SCTP

Aquí se describen las directrices de arranque y cierre de asociación **SCTP**.

La asociación **SCTP** consta de un reconocimiento de cuatro direcciones que tiene lugar en el orden siguiente:

1. El cliente envía una señal **INIT** al servidor para iniciar una asociación.
2. Al recibir la señal **INIT**, el servidor envía una respuesta **INIT-ACK** al cliente. Esta señal **INIT-ACK** contiene un cookie de estado. Este cookie de estado debe contener un Código de autentificación de mensaje (MAC), junto con una indicación de la hora correspondiente a la creación del cookie, el periodo de vida del cookie de estado y la información necesaria para establecer la asociación. El MAC lo calcula el servidor basándose en una clave secreta que sólo él conoce.
3. Al recibir esta señal **INIT-ACK**, el cliente envía una respuesta **COOKIE-ECHO**, que simplemente hace eco del cookie de estado.
4. Después de verificar la autenticidad del cookie de estado utilizando la clave secreta, el servidor asigna los recursos para la asociación, envía una respuesta **COOKIE-ACK** reconociendo la señal **COOKIE-ECHO** y mueve la asociación al estado **ESTABLISHED**.

**SCTP** también soporta el cierre ordenado de una asociación activa cuando lo solicita el usuario **SCTP**. Se produce la siguiente secuencia de sucesos:

1. El cliente envía una señal **SHUTDOWN** al servidor, que indica al servidor que el cliente está preparado para cerrar la conexión.
2. El servidor responde enviando un reconocimiento **SHUTDOWN-ACK**.
3. Entonces el cliente devuelve una señal **SHUTDOWN-COMPLETE** al servidor.

**SCTP** también soporta el cierre repentino (señal **ABORT**) de una asociación activa cuando lo solicita el cliente **SCTP** o debido a un error de la pila **SCTP**. Sin embargo, **SCTP** no soporta conexiones medio abiertas. Se puede encontrar más información sobre el protocolo y sus características internas en RFC 4960.

Además de las diferencias especificadas más arriba entre **SCTP** y los protocolos de transporte existentes, **SCTP** proporciona las características siguientes:

- **Entrega en secuencias en las corrientes:** Una corriente en el contexto de **SCTP** hace referencia a una secuencia de mensajes de usuario que se transfieren entre puntos finales. Una asociación **SCTP** puede soportar varias corrientes. En el momento de configurar la asociación, el usuario puede especificar el número de las corrientes. El valor efectivo del número de corriente se fija después de negociar con el igual. Dentro de cada corriente, el orden de la entrega de datos se mantiene de forma estricta. Sin embargo, entre corrientes, la entrega de datos es independiente. De este modo, la pérdida de datos de una corriente no impide que los datos se entreguen en otra corriente. Esto permite a una aplicación de usuario utilizar diferentes corrientes para datos lógicamente independientes. También se pueden entregar datos de un modo no ordenado utilizando una opción especial. Esto puede ser útil para enviar datos urgentes.
- **Fragmentación de datos de usuario:** **SCTP** puede fragmentar mensajes de usuario para asegurar que el tamaño de paquete pasado a la capa inferior no excede la MTU de vía de acceso. En el momento de la recepción, los fragmentos se vuelven a ensamblar en un mensaje completo y se pasan al usuario. Aunque la fragmentación también se puede realizar a nivel de red, la fragmentación de capa de transporte proporciona varias ventajas respecto a la fragmentación de capa de IP. De lo contrario, algunas de estas ventajas, que incluyen no tener que volver a enviar mensajes enteros cuando se pierden fragmentos en la red y reducir el peso en los direccionadores, posiblemente tendrían que realizar la fragmentación de IP.
- **Reconocimiento y control de congestión:** El reconocimiento de paquetes es necesario para la entrega de datos fiable. Cuando, al cabo de un periodo de tiempo especificado, **SCTP** no obtiene un reconocimiento de un paquete que envía, desencadena una retransmisión del mismo paquete. **SCTP** sigue algoritmos de control de congestión similares a los utilizados por **TCP**. Además de utilizar los reconocimientos acumulativos como **TCP**, **SCTP** utiliza el mecanismo SACK (Selective Acknowledgment - Reconocimiento selectivo) que le permite reconocer los paquetes de forma selectiva.
- **Empaquetado de fragmentos:** Un fragmento puede contener datos de usuario o información de control de **SCTP**. Se pueden empaquetar juntos varios fragmentos bajo la misma cabecera **SCTP**. Para

empaquetar los fragmentos es necesario reunir los fragmentos en un paquete **SCTP** en el extremo remitente y posteriormente deshacer en paquete en fragmentos en el extremo destinatario.

- **Validación de paquete:** Cada paquete **SCTP** tiene un campo de código de verificación que cada punto final establece durante el tiempo de arranque de asociación. Todos los paquetes se envían con el mismo código de verificación durante todo el tiempo de vida de la asociación. Si, durante el tiempo de vida de la asociación, se recibe un paquete con un código de verificación inesperado, se descarta el paquete. Asimismo, el remitente de cada paquete **SCTP** debe establecer la suma de comprobación de CRC-32 para proporcionar una mayor protección frente a la corrupción de datos en la red. Se descarta cualquier paquete recibido con una suma de comprobación de CRC-32 no válida.
- **Gestión de vía de acceso:** En el momento de realizar la configuración de asociación, cada punto final puede anunciar una lista de direcciones de transporte que tiene. Sin embargo, sólo se define una vía de acceso primaria para la asociación **SCTP** y se utiliza dicha vía para la transferencia de datos normal. Si la vía de acceso primaria quede desactivada, se utilizan las demás direcciones de transporte. Durante el tiempo de vida de la asociación, se envían latidos a intervalos regulares a través de todas las vías de acceso a fin de supervisar el estado de la vía de acceso.

#### API de socket **SCTP**

Las características de las API de socket **SCTP** incluyen coherencia, accesibilidad y compatibilidad.

Las API de socket **SCTP** se han diseñado para proporcionar las características siguientes:

- Mantener la coherencia con las API de socket existentes
- Proporcionar una base para acceder a las nuevas características de **SCTP**
- Proporcionar compatibilidad para que la mayoría de las aplicaciones **TCP** y **UDP** existentes se puedan migrar a **SCTP** con pocos cambios

Para facilitar la migración fácil de las aplicaciones **TCP** y **UDP** existentes, se han formulado dos estilos diferentes de API **SCTP**:

- API de estilo **UDP** – La semántica es similar a la definida para los protocolos sin conexión como **UDP**
- API de estilo **TCP** – La semántica es similar a la definida para los protocolos orientados a conexión como **TCP**

Aunque **SCTP** permite que se defina y se utilice el estilo **TCP** y **UDP** de API de socket, en AIX 5.3, sólo se proporciona soporte para la sintaxis de socket de estilo **UDP** porque la API de estilo **UDP** proporciona más flexibilidad para acceder a las características nuevas de **SCTP**. Con la API de estilo **UDP**, un servidor típico utiliza la secuencia de llamadas siguiente durante el tipo de vida de una asociación.

1. `socket()`
2. `bind()`
3. `listen()`
4. `recvmsg()`
5. `sendmsg()`
6. `close()`

Un cliente típico utiliza la secuencia siguiente de llamadas de API de socket:

1. `socket()`
2. `sendmsg()`
3. `recvmsg()`
4. `close()`

Las asociaciones creadas utilizando la secuencia de llamadas anterior se denominan asociaciones creadas explícitamente. Una asociación se puede crear implícitamente después de crear un socket, simplemente llamando a `sendmsg()`, `recvmsg()` o `sendto()` y `recvto()`. En el caso de asociación implícita, las llamadas `bind()` y `listen()` no son necesarias. La sintaxis de todas estas llamadas de sistema son similares a las utilizadas con los sockets **UDP**. Para la subrutina de socket, el campo **Type** (**Tipo**) se debe establecer en **SOCK\_SEQPACKET** y el campo **Protocol** (**Protocolo**) debe ser

IPPROTO\_SCTP. Además de estas API de socket estándares **SCTP** proporciona dos nuevas API: **sctp\_peeloff()** y **sctp\_opt\_info()**. Se puede encontrar más información sobre el uso de la API de socket para **SCTP** en el borrador de API de socket SCTP. **SCTP** se ha implementado como una extensión de kernel en AIX 5.3. Un usuario puede utilizar el mandato **sctpctrl** para cargar y descargar la extensión de kernel **SCTP**.

Además, este mandato también se puede utilizar para ver y cambiar otras estadísticas y otros parámetros ajustables diversos de la extensión de kernel **SCTP** utilizando diferentes opciones como get y set.

### **Subrutina sctp\_bindx**

Añade o elimina la dirección de enlace en un socket.

#### **Biblioteca**

```
/usr/lib/libssctp.a
```

#### **Sintaxis**

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/sctp.h>

int sctp_bindx(int sd, struct sockaddr * addrs, int addrcnt, int flags);
```

#### **Descripción**

La subrutina **sctp\_bindx** añade o elimina un conjunto de direcciones de enlace pasadas en la batería de **addrs** o desde el socket **sd**. El parámetro **addrcnt** es el número de direcciones de la batería, y el parámetro **flags** especifica si las direcciones necesitan añadirse o eliminarse.

Si el socket **sd** es un socket IPv4, las direcciones que se pasan deben ser direcciones IPv4. Si el socket **sd** es un socket IPv6, las direcciones que se pasan pueden ser direcciones IPv4 o IPv6.

El parámetro **addrs** es un puntero a una batería de una o más direcciones de socket. Cada dirección se contiene en su estructura adecuada, es decir, **struct sockaddr\_in** o **struct sockaddr\_in6**. La familia del tipo de dirección debe utilizarse para distinguir la longitud de la dirección. El emisor especifica el número de direcciones de la batería además de **addrcnt**.

El parámetro **flags** puede ser **SCTP\_BINDEX\_ADD\_ADDR** o **SCTP\_BINDEX\_REMOVE\_ADDR**. Una aplicación puede utilizar **SCTP\_BINDEX\_ADD\_ADDR** para asociar direcciones adicionales con un punto final tras llamar al mandato **bind**. El parámetro **SCTP\_BINDEX\_REMOVE\_ADDR** se dirige a SCTP para eliminar las direcciones determinadas desde la asociación. Un emisor puede no eliminar todas las direcciones de una asociación. El mandato fallará, dando como resultado el código de error **EINVAL**.

#### **Valores de retorno**

Una vez que se hayan completado satisfactoriamente, el mandato **sctp\_bindx()** devolverá 0. Al fallar, el mandato **sctp\_bindx()** devuelve -1 y establece el parámetro **errno** en el código de error apropiado.

Códigos de error

Error	Descripción
<b>EINVAL</b>	El código de error <b>EINVAL</b> indica que el puerto o la dirección no es válido o que el mandato está intentando eliminar todas las direcciones de una asociación.
<b>EOPNOTSUPP</b>	El código de error <b>EOPNOTSUPP</b> indica que el mandato está intentando añadir o eliminar direcciones de una asociación conectada.

### **Subrutinas sctp\_getladdrs y sctp\_freeladdrs**

Devuelve todas las direcciones vinculadas localmente en un socket.

## Biblioteca

```
/usr/lib/libscpt.a
```

## Sintaxis

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/scpt.h>

int scpt_getladdrs(int sd, scpt_assoc_t assoc_id, struct sockaddr **addrs);
void scpt_freeladdrs(struct sockaddr *addrs);
```

## Descripción

La subrutina **scpt\_getladdrs** devuelve todas las direcciones vinculadas localmente en un socket. A su vez, el parámetro **addrs** apunta a una batería empaquetada asignada dinámicamente de las estructuras de **sockaddr** del tipo apropiado para cada dirección local. Debe utilizar el parámetro **scpt\_freeladdrs** para liberar la memoria.

**Nota:** El parámetro de entrada o salida **addrs** no debe ser NULL.

Si el parámetro **sd** es un socket IPv4, las direcciones devueltas son todas las direcciones IPv4. Si el parámetro **sd** es un socket IPv6, las direcciones devueltas pueden ser una mezcla de direcciones IPv4 o IPv6.

Para sockets de estilo uno a varios, el campo **id** especifica la asociación que se va a consultar. Para sockets de estilo uno a uno, el campo **id** se ignorará. Si el campo **id** se establece en 0, las direcciones vinculadas localmente se devuelven sin tener en cuenta ninguna asociación particular.

La subrutina **scpt\_freeladdrs** libera todos los recursos asignados por la subrutina **scpt\_getladdrs**.

## Valor de retorno

Al finalizar satisfactoriamente, la subrutina **scpt\_getladdrs** devuelve el número de direcciones locales vinculadas al socket. Si el socket no está vinculado, se devuelve 0 y el valor del campo **\*addrs** no estará definido. Si hay un error, la subrutina **scpt\_getladdrs** devuelve -1, y el valor del campo **\*addrs** no estará definido.

## Subrutinas **scpt\_getpaddrs** y **scpt\_freepaddrs**

Devuelve todas las direcciones iguales en una asociación.

## Biblioteca

```
/usr/lib/libscpt.a
```

## Sintaxis

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/scpt.h>

int scpt_getpaddrs(int sd, scpt_assoc_t assoc_id, struct sockaddr **addrs);
void scpt_freepaddrs(struct sockaddr *addrs);
```

## Descripción

La subrutina **scpt\_getpaddrs** devuelve todas las direcciones iguales de una asociación. A su vez, el parámetro **addrs** apunta a una batería empaquetada asignada dinámicamente de las estructuras de **sockaddr** del tipo apropiado para cada dirección. Debe utilizar la subrutina **scpt\_freepaddrs** para liberar la memoria.

**Nota:** El parámetro de entrada o salida **addrs** no debe ser NULL.

Si el parámetro **sd** es un socket IPv4, las direcciones devueltas son todas las direcciones IPv4. Si el parámetro **sd** es un socket IPv6, las direcciones devueltas pueden ser una mezcla de direcciones IPv4 o IPv6. Para sockets de estilo uno a varios, el campo **id** especifica la asociación que se va a consultar. Para sockets de estilo uno a uno, el campo **id** se ignorará.

La subrutina **sctp\_freepaddrs** libera todos los recursos asignados por la subrutina **sctp\_getpaddrs**.

### Valor de retorno

Al finalizar satisfactoriamente, la subrutina **sctp\_getpaddrs** devuelve el número de direcciones iguales de la asociación. Si no hay una asociación en este socket, se devuelve 0 y el valor del campo **\*addrs** no estará definido. Si hay un error, la subrutina **sctp\_getpaddrs** devuelve -1, y el valor del campo **\*addrs** no estará definido.

## Descubrimiento de MTU de vía de acceso

Para dos sistemas principales que se comunican a través de una vía de acceso de varias redes, se fragmenta un paquete transmitido si su tamaño es mayor que la MTU más pequeña de cualquier red de la vía de acceso. Puesto que la fragmentación de paquete puede hacer que disminuya el rendimiento de red, es deseable evitar la fragmentación transmitiendo paquetes con un tamaño que no sea mayor que la MTU más pequeña de la vía de acceso de red. Este tamaño se denomina MTU de vía de acceso.

El sistema operativo soporta un algoritmo de descubrimiento de MTU de vía de acceso tal como se describe en la RFC 1191. Se puede habilitar el descubrimiento de MTU de vía de acceso para las aplicaciones **TCP** y **UDP** modificando las opciones **tcp\_pmtu\_discover** y **udp\_pmtu\_discover** del mandato **no**. Cuando se habilita para **TCP**, el descubrimiento de MTU de vía de acceso forzará automáticamente que el tamaño de todos los paquetes transmitidos por las aplicaciones **TCP** no exceda la MTU de vía de acceso. Puesto que las propias aplicaciones **UDP** determinan el tamaño de los paquetes transmitido, las aplicaciones **UDP** se deben escribir específicamente para que utilicen la información de MTU de vía de acceso usando la opción de socket **IP\_FINDPMTU**, incluso si se habilita la opción **udp\_pmtu\_discover no**. De forma predeterminada, **tcp\_pmtu\_discover** y **udp\_pmtu\_discover** están habilitados.

Cuando se intenta el descubrimiento de MTU de vía de acceso para un destino, se creará una entrada de pmtu en una tabla de MTU de vía de acceso (PMTU). Esta tabla se puede visualizar utilizando el mandato de visualización **pmtu**. Se puede evitar la acumulación de entradas pmtu permitiendo que las entradas pmtu no utilizadas caduquen y se supriman. La caducidad de entrada PMTU la controla la opción **pmtu\_expire** del mandato **no**. **pmtu\_expire** se establece en 10 minutos de forma predeterminada.

Puesto que las rutas pueden cambiar dinámicamente, el valor de MTU de una vía de acceso puede cambiar también con el tiempo. Dado que si se reduce el valor de MTU de vía de acceso, se produce la fragmentación de paquetes, se comprueba periódicamente si los valores de MTU de vía de acceso descubiertos disminuyen. De forma predeterminada, las disminuciones se comprueban cada 10 minutos y este valor se puede cambiar modificando el valor de la opción **pmtu\_default\_age** del mandato **no**.

Las aplicaciones **UDP** siempre necesitarán establecer la opción de socket **IP\_DONTFRAG** para detectar las disminuciones en PMTU. Esto habilitará la detección inmediata de las disminuciones de MTU de vía de acceso en lugar de comprobar las disminuciones cada **pmtu\_default\_age** minutos.

Los incrementos del valor de MTU de vía de acceso pueden producir un aumento potencial en el rendimiento de la red, de modo que se comprueban periódicamente los aumentos en los valores de MTU de vía de acceso descubiertos. De forma predeterminada, se comprueban los aumentos cada 30 minutos y este valor se puede cambiar modificando el valor de la opción **pmtu\_rediscover\_interval** del mandato **no**.

Si no todos los direccionadores de la vía de acceso de red soportan la RFC 1191, puede que no sea posible determinar un valor de MTU de vía de acceso exacto. En estos casos, se puede utilizar el mandato **mmtu** para añadir o suprimir los valores de MTU de vía de acceso que se intentan.

**Nota:**

1. El direccionamiento de MTU de vía de acceso no se puede utilizar en rutas duplicadas, incluidas las configuradas para el direccionamiento de grupos (consulte el apartado “[Restricciones de uso de rutas](#)” en la página 438). El descubrimiento de MTU de vía de acceso se puede utilizar en rutas duplicadas
2. Al habilitar el descubrimiento de MTU de vía de acceso, se establece el valor de la opción **arpqsize** del mandato **no** en un valor mínimo de 5. Este valor no disminuye si posteriormente se inhabilita el descubrimiento de MTU de vía de acceso.

## Calidad de servicio de TCP/IP

QoS (Quality of Service - Calidad de servicio) es una familia de estándares de Internet en desarrollo que proporcionan procedimientos para dar un trato preferente a determinados tipos de tráfico IP.

Con el soporte adecuado para QoS a lo largo de una ruta, esto puede mejorar los efectos de la congestión y los retardos de colas variables que contribuyen a que el rendimiento de la red sea deficiente. El sistema operativo proporciona soporte de sistema principal para QoS a fin de clasificar el tráfico de salida en clases diferenciadas de servicio y anunciar y establecer reservas de recursos según las soliciten las aplicaciones cliente.

Una institución puede utilizar QoS para desplegar e imponer políticas de red que controlan el uso del ancho de banda de red. Con QoS, un sistema principal puede:

- Regular la cantidad de tráfico de un determinado tipo inyectado en la red;
- Marcar paquetes seleccionados de acuerdo con alguna política para que los direccionadores subsiguientes puedan entregar el servicio indicado;
- Soportar servicios tales como el servicio de línea alquilada virtual con soporte de QoS correcto a lo largo de la ruta y
- Participar en las peticiones de reserva de recursos de los destinatarios y anunciar las sesiones de remitente disponibles para las peticiones de reserva de recursos.

El soporte de QoS proporciona las funciones siguientes:

- Servicios diferenciados definidos en la RFC 2474
- Políticas de tráfico
- Marcado de paquetes en el perfil y fuera del perfil
- Definición de tráfico
- Medición
- Servicios integrados para aplicaciones cliente y servidor tal como se definen en la RFC 1633
- Señalización de RSVP (RFC 2205)
- Servicio garantizado (RFC 2212)
- Servicio de carga controlada (RFC 2211)
- Redes basadas en políticas
- Biblioteca compartida RAPI para aplicación

El subsistema QoS consta de cuatro componentes:

### Extensión de kernel de QoS (**/usr/lib/drivers/qos**)

La extensión de kernel de QoS reside en **/usr/lib/drivers/qos** y se carga y descarga utilizando los métodos de configuración **cfgqos** y **ucfgqos**. Esta extensión de kernel habilita el soporte de QoS.

### Agente de política (**/usr/sbin/policyd**)

El agente de política es un daemon a nivel de usuario que reside en **/usr/sbin/policyd**.

Proporciona soporte para la gestión de política y las interfaces con la extensión de kernel de QoS para instalar, modificar y suprimir normas de política. Las normas de política se puede definir en el archivo de configuración local (**/etc/policyd.conf**) y/o recuperar de un servidor de políticas de red central utilizando LDAP.

### **Agente RSVP (/usr/sbin/rsvpd)**

El agente RSVP es un daemon de nivel de usuario que reside en /usr/sbin/rsvpd. Implementa la semántica de protocolo de señalización RSVP.

### **Biblioteca compartida RAPI (/usr/lib/librapi.a)**

Las aplicaciones pueden utilizar la API RSVP (RAPI) para solicitar la calidad de servicio ampliada tal como define el modelo de QoS de Servicios integrados de Internet. Esta biblioteca interactúa con el agente RSVP local para propagar la petición de QoS a lo largo de la vía de acceso del flujo de datos utilizando el protocolo RSVP. Esta API es un estándar abierto.

**Nota:** Esta implementación de QoS se basa en un conjunto de estándares de Internet en desarrollo y de estándares de borrador que actualmente están siendo desarrollados por IETF (Internet Engineering Task Force - Grupo de trabajo de ingeniería de Internet) y sus diversos grupos de trabajo. Esta tecnología será más coherente y estará mejor definida a medida que progresen estos esfuerzos de estandarización en el IETF. También es importante tener en cuenta que QoS es una tecnología de Internet en desarrollo que acaba de empezar a desplegarse en Internet. Existen muchas ventajas de QoS en todas las etapas del desarrollo. Sin embargo, los verdaderos servicios de extremo a extremo sólo se pueden llevar a cabo cuando existe soporte de QoS a lo largo de toda una ruta determinada.

### **Modelos QoS**

Los modelos QoS para Internet son estándares abiertos definidos por IETF.

Existen dos modelos QoS de Internet que actualmente se están estandarizando en IETF: *servicios integrados* y *servicios diferenciados*. Estos dos modelos QoS de Internet amplían el modelo de servicio tradicional de máximo esfuerzo descrito en RFC 1812.

#### **Servicios integrados**

IS (Integrated Services - Servicios integrados) es un modelo de reserva de recurso dinámico para Internet que se describe en RFC 1633.

Los sistemas principales utilizan un protocolo de señalización denominado Resource ReSerVation Protocol (RSVP) para solicitar dinámicamente una calidad de servicio específica de la red. Los parámetros de QoS se transportan en estos mensajes RSVP y cada nodo de red junto con la vía de acceso instala los parámetros para obtener la calidad de servicio solicitada. Estos parámetros QoS describen uno de dos servicios definidos actualmente, el servicio garantizado y el servicio de carga controlada. Una característica importante de IS es que esta señalización se realiza para cada flujo de tráfico y las reservas se instalan en cada salto a lo largo de la ruta. Aunque este modelo es adecuado para satisfacer las necesidades dinámicamente cambiantes de las aplicaciones, existen algunos problemas de escala significativos que implican que no se pueda desplegar en una red en la que direcciones individuales pueden manejar muchos flujos simultáneos.

#### **Servicios diferenciados**

Los Servicios diferenciados (DS) eliminan los problemas de escalabilidad por flujo y por salto, sustituyéndolos por un mecanismo simplificado de clasificación de paquetes.

En lugar de utilizar una propuesta de señalización dinámica, DS utiliza los bits del byte de tipo de servicio (TOS) IP para separar los paquetes en clases. El patrón de bit particular del byte TOS de IP se denomina punto de código DS y lo utilizan los routers para definir la calidad de servicio proporcionada en ese determinado salto, de la misma forma que los routers realizan el reenvío de IP utilizando búsquedas de tabla de dirección. El trato dado a un paquete con un punto de código DS determinado se denomina comportamiento por salto (PHB) y se administra independientemente en cada nodo de red. Cuando se concatenan los efectos de estos PHB individuales independientes, se produce un servicio de extremo a extremo.

Los Servicios diferenciados están siendo estandarizados por un grupo de trabajo de IETF, que ha definido tres PHB: el PHB de EF (Expedited Forwarding - Reenvío urgente), el grupo de PHB de AF (Assured Forwarding - Reenvío asegurado) y el PHB de DE (Default - Valor predeterminado). El PHB de EF se puede utilizar para implementar una frecuencia baja, una fluctuación baja, una pérdida baja, un servicio de extremo a extremo, por ejemplo una línea alquilada virtual (VLL). AF es una familia de PHB, denominada grupo de PHB, que se utiliza para clasificar paquetes en diversos niveles de prioridad para soltarlos. La prioridad asignada a un paquete para soltarlo determina la importancia relativa del paquete en la clase

AF. Se puede utilizar para implementar el servicio llamado *Olímpico*, que consta de tres clases: bronce, plata y oro. El PHB de DE es el modelo de servicio tradicional de esfuerzo óptimo que se ha estandarizado en la RFC 1812.

### Estándares soportados y estándares de borrador

Estas RFC y borradores de Internet describen los estándares en los que se basa esta implementación de QoS.

Item	Descripción
RFC 2474	Definición del campo de Servicios diferenciados (campo DS) en las cabeceras de IPv4 e IPv6
RFC 2475	Una arquitectura para Servicios diferenciados
RFC 1633	Servicios integrados en la arquitectura de Internet: una visión general
RFC 2205	Resource ReSerVation Protocol (RSVP)
RFC 2210	El uso de RSVP con Servicios integrados de IETF
RFC 2211	Especificación del servicio de elementos de red de carga controlada
RFC 2212	Especificación de calidad de servicio garantizada
RFC 2215	Parámetros de caracterización generales para elementos de red de servicios integrados

Item	Descripción
draft-ietf-diffserv-framework-01.txt, octubre de 1998	Una infraestructura para servicios diferenciados
draft-ietf-diffserv-rsvp-01.txt, noviembre de 1998	Una infraestructura para uso de RSVP con redes DIFF-serv
draft-ietf-diffserv-phb-ef-01.txt	Un PHB de reenvío urgente
draft-ietf-diffserv-af-04.txt	Grupo PHB de reenvío asegurado
draft-rajan-policy-qosschema-00.txt, octubre de 1998	Esquema para servicios diferenciados y servicios integrados en redes
draft-ietf-rap-framework-01.txt, noviembre de 1998	Una infraestructura para control de admisión basado en políticas [25]
draft-ietf-rap-rsvp-ext-01.txt, noviembre de 1998	Extensiones de RSVP para control de políticas

**Nota:** QoS es una tecnología emergente de Internet. QoS ofrece muchas ventajas en todas las etapas del despliegue. Sin embargo, los verdaderos servicios de extremo a extremo sólo se pueden llevar a cabo cuando existe soporte de QoS a lo largo de toda una ruta determinada.

### Instalación de QoS

QoS se empaqueta con bos.net.tcp.server. Este catálogo de archivos se debe instalar a fin de utilizar QoS.

Para utilizar la biblioteca compartida RAPI, también se debe instalar bos.adt.include.

### Detención e inicio del subsistema QoS

QoS se puede iniciar o detener mediante SMIT con la vía de acceso rápida smit qos o con los mandatos **mkqos** y **xmqos**.

1. Para inhabilitar el subsistema QoS ahora y en el siguiente reinicio del sistema:

```
/usr/sbin/xmqos -B
```

2. Para inhabilitar el subsistema QoS ahora solamente:

```
/usr/sbin/mkqos -N
```

Consulte las descripciones de los mandatos **mkqos** y **xmqos** para conocer los distintivos de mandato de arranque y eliminación.

Los daemons **policyd** y **rsvpd** se configuran mediante los archivos de configuración */etc/policyd.conf* y */etc/rsvpd.conf*, respectivamente. Estos archivos de configuración se *deben* editar para personalizar el subsistema QoS en el entorno local. QoS no funciona correctamente con las configuraciones de ejemplo proporcionadas.

### Configuración de agente RSVP

El agente RSVP es necesario si el sistema principal debe soportar el protocolo RSVP.

Se utiliza el archivo de configuración */etc/rsvpd.conf* para configurar el agente RSVP. La sintaxis del archivo de configuración se describe en el archivo de configuración de ejemplo instalado en */etc/rsvpd.conf*.

El ejemplo siguiente ilustra una posible configuración de RSVP en la que el sistema principal tiene 4 interfaces (virtual o física) proporcionadas por las 4 direcciones IP, 1.2.3.1, 1.2.3.2, 1.2.3.3 y 1.2.3.4.

```
interface 1.2.3.1
interface 1.2.3.2 disabled
interface 1.2.3.3 disabled
interface 1.2.3.4
{
    trafficControl
}

rsvp 1.2.3.1
{
    maxFlows 64
}

rsvp 1.2.3.4
{
    maxFlows 100
}
```

La interfaz 1.2.3.1 se ha habilitado para RSVP. Sin embargo, no se ha especificado control de tráfico y los mensajes RESV RSVP de entrada no producen reserva de recursos en el subsistema TCP. Esta interfaz puede soportar un máximo de 64 sesiones RSVP simultáneas.

Las interfaces 1.2.3.2 y 1.2.3.3 se han inhabilitado. El agente RSVP no puede utilizar esta interfaz para transmitir o recibir mensajes RSVP.

La interfaz 1.2.3.4 se ha habilitado para RSVP. Además, puede instalar reservas de recursos en el subsistema **TCP** en respuesta a un mensaje RESV RSVP. Esta interfaz puede soportar un máximo de 100 sesiones RSVP.

Otras interfaces presentes en el sistema principal pero no mencionadas explícitamente en */etc/rsvpd.conf* están inhabilitadas.

### Configuración de agente de política

El agente de política es un componente necesario del subsistema QoS.

Se utiliza el archivo de configuración */etc/policyd.conf* para configurar el agente de política. La sintaxis de este archivo de configuración se describe en el archivo de configuración de ejemplo instalado en */etc/policyd.conf*.

El agente de política se puede configurar editando */etc/policyd.conf*. Adicionalmente, se proporcionan los mandatos siguientes para ayudar en la configuración de políticas:

- **qosadd**
- **qosmod**

- **qoslist**
- **qosremove**

En el ejemplo siguiente, se crea una categoría de servicio máximo que se utiliza en la norma de política `tcptraffic`. Esta categoría de servicio tiene una velocidad máxima de 110000 Kbps, una profundidad de cubeta de señales de 10000 bits y un valor TOS de IP de salida de 11100000 en binario. La norma de política `tcptraffic` proporciona este servicio máximo a todo el tráfico con la dirección IP de origen proporcionada por 1.2.3.6, la dirección de destino 1.2.3.3 y el puerto de destino en el rango de 0 a 1024.

```
ServiceCategories premium
{
    PolicyScope     DataTraffic
    MaxRate        110000
    MaxTokenBucket 10000
    OutgoingTOS    11100000
}

ServicePolicyRules tcptraffic
{
    PolicyScope     DataTraffic
    ProtocolNumber 6 # tcp
    SourceAddressRange 1.2.3.6-1.2.3.6
    DestinationAddressRange 1.2.3.3-1.2.3.3
    DestinationPortRange 0-1024
    ServiceReference   premium
}
```

Las sentencias siguientes configuran una categoría de servicio predeterminada y la utilizan para restringir el tráfico UDP que fluye de las interfaces 1.2.3.1 a 1.2.3.4 hasta las direcciones IP 1.2.3.6 a 1.2.3.10, puerto 8000.

```
ServiceCategories default
{
    MaxRate        110000
    MaxTokenBucket 10000
    OutgoingTOS    00000000
}

ServicePolicyRules udptraffic
{
    ProtocolNumber 17 # udp
    SourceAddressRange 1.2.3.1-1.2.3.4
    DestinationAddressRange 1.2.3.6-1.2.3.10
    DestinationPortRange 8000-8000
    ServiceReference   default
}
```

Se puede utilizar la siguiente configuración de ejemplo para descargar normas de un servidor LDAP utilizando el nombre de subárbol distinguido, con el fin buscar las políticas en el sistema principal de servidor LDAP.

```
ReadFromDirectory
{
    LDAP_Server      1.2.3.27
    Base             ou=NetworkPolicies,o=myhost.mydomain.com,c=us
}
```

### **Resolución de problemas de QoS**

Se puede utilizar el mandato **qosstat** para visualizar información de estado sobre las políticas instaladas y activas en el subsistema QoS. Esta información puede ser útil para ayudarle a determinar dónde existe un problema si está solucionando problemas de la configuración de QoS.

Se puede utilizar **qosstat** para generar el siguiente informe.

```
Action:
Token bucket rate (B/sec): 10240
Token bucket depth (B): 1024
Peak rate (B/sec): 10240
Min policed unit (B): 20
Max packet size (B): 1452
```

```

Type: IS-CL
Flags: 0x00001001 (POLICE,SHAPE)

Statistics:
Compliant packets: 1423 (440538 bytes)

Conditions:
Source address      Dest address      Protocol
192.168.127.39:8000 192.168.256.29:35049  tcp      (1 connection)

Action:
Token bucket rate (B/sec): 10240
Token bucket depth (B): 1024
Peak rate (B/sec): 10240
Outgoing TOS (compliant): 0xc0
Outgoing TOS (non-compliant): 0x00
Flags: 0x00001011 (POLICE,MARK)
Type: DS

Statistics:
Compliant packets: 335172 (20721355 bytes)
Non-compliant packets: 5629 (187719 bytes)

Conditions:
Source address      Dest address      Protocol
192.168.127.39:80  *:*               tcp      (1 connection)
192.168.127.40:80  *:*               tcp      (5 connections)

```

## Especificación de política de QoS

Aquí se describen las clases y los atributos de objeto utilizados por el agente de política para especificar las políticas para la calidad de servicio (QoS) en el tráfico de salida.

Se definen las clases y los atributos de objeto, seguidos de directrices para habilitar las marcas, las políticas y las formas.

En las explicaciones siguientes se utilizan estos convenios.

```

p : elegir uno del conjunto de parámetros permitido
B : valor de entero de un byte (es decir 0 <= B <= 255)
b : serie de bits empezando por el bit situado más a la izquierda (por ejemplo 101
     equivale a 10100000 en un campo de byte)
i : valor de entero
s : serie de caracteres
a : formato de dirección IP B.B.B.B
(R) : parámetro necesario
(O) : parámetro opcional

```

## Sentencia ReadFromDirectory

Esta sentencia especifica parámetros para establecer una sesión LDAP.

La sentencia ReadFromDirectory se utiliza en el archivo /etc/policyd.conf para establecer la sesión LDAP.

```

ReadFromDirectory
{
    LDAP_Server   a  # Dirección IP de servidor de directorios que ejecuta LDAP
    LDAP_Port     i  # Número de puerto en el que escucha el servidor LDAP
    Base          s  # Nombre distinguido para el uso de LDAP
    LDAP_SelectedTag s # Código para comparar SelectorTag en clases de objeto
}

```

donde

```

LDAP_Server (R): dirección IP de servidor LDAP
LDAP_Port (O): Número de puerto exclusivo, el puerto predeterminado es 389
Base (R): El ejemplo es o=ibm, c=us donde o es la organización y c es el país
LDAP_SelectedTag (R): Serie exclusiva que coincide con el atributo
                      SelectorTag en la clase de objeto

```

## Sentencias ServiceCategories

Esta sentencia especifica el tipo de servicio que un flujo de paquetes IP (por ejemplo, de una conexión **TCP** o de datos **UDP**) debe recibir de extremo a extremo a medida que atraviesa la red.

ServiceCategories se puede repetir, teniendo cada uno de ellos un nombre diferente para poder hacer referencia a los mismos posteriormente. Un objeto ServiceCategories necesita que ServicePolicyRules complete la definición de política.

```
ServiceCategories s
{
    SelectorTag      s  # Código necesario para la búsqueda LDAP
    MaxRate          i  # Velocidad destino para tráfico en esta clase servicio
    MaxTokenBucket  i  # La profundidad de cubeta
    OutgoingTOS     b  # Valor TOS de tráfico salida para esta clase servicio
    FlowServiceType   p # Tipo de tráfico
}
```

donde

s (R)	: es el nombre de esta categoría de servicio
SelectorTag (R)	: Sólo necesario para que LDAP busque clases de objeto
MaxRate (0)	: en Kbps (K bits por segundo), el valor predeterminado es 0
MaxTokenBucket(0)	: en Kb, valor predeterminado es máximo definido por sistema
OutgoingTOS (0)	: el valor predeterminado es 0
FlowServiceType (0)	: ControlledLoad   Guaranteed, el valor predeterminado es ControlledLoad

### **Sentencia ServicePolicyRules**

Esta sentencia especifica las características de los paquetes IP que se utilizan para realizar la comparación con una categoría de servicio correspondiente.

En otras palabras, define un conjunto de datagramas IP que deben recibir un servicio determinado. ServicePolicyRules se asocia con ServiceCategories mediante el atributo ServiceReference. Si dos normas hacen referencia a la misma ServiceCategory, cada norma se asocia con una instancia exclusiva de ServiceCategory.

```
ServicePolicyRules s
{
    SelectorTag      s  # Código necesario para la búsqueda LDAP
    ProtocolNumber   i  # ID de protocolo de transporte para la norma de política
    SourceAddressRange a1-a2
    DestinationAddressRange a1-a2
    SourcePortRange   i1-i2
    DestinationPortRange i1-i2
    PolicyRulePriority i  # El valor más alto se impone primero
    ServiceReference    s # Nombre de categoría de servicio para
                           # esta norma de política
}
```

donde

s (R):	es el nombre de la norma de política
SelectorTag (R):	sólo necesario para que LDAP busque la clase de objeto
ProtocolNumber (R):	valor predet. 0 no produce coincidencias, especificar explícitamente
SourceAddressRange (0):	de a1 a a2 donde a2 >= a1, valor predeterminado es 0, cualquier dirección origen
SourcePortRange (0):	de i1 a i2 donde i2 >= i1, valor predeterminado es 0, cualquier puerto origen
DestinationAddressRange (0):	igual que SourceAddressRange
DestinationPortRange (0):	igual que SourcePortRange
PolicyRulePriority (0):	Importante especificarlo cuando existen políticas que se solapan
ServiceReference (R):	categoría de servicio que esta norma utiliza

### **Directrices para entornos DiffServ**

A continuación se proporcionan directrices para especificar políticas de creación de marcas, formas y/o políticas en un entorno DiffServ.

#### **1. Sólo marcas**

```

OutgoingTOS      : Tipo de servicio deseado
FlowServiceType : ControlledLoad
MaxRate         : Tomar valor predeterminado de 0

```

## 2. Sólo formas

```

OutgoingTOS      : Tomar valor predeterminado de 0
FlowServiceType : Garantizado
MaxRate         : Velocidad de destino desea para el tráfico como entero positivo

```

## 3. Marcas y políticas (ver nota)

```

OutgoingTOS      : Tipo de servicio deseado
FlowServiceType : ControlledLoad
MaxRate         : Velocidad de destino desea para el tráfico como entero positivo

```

## 4. Marcas y formas

```

OutgoingTOS      : Tipo de servicio deseado
FlowServiceType : Garantizado
MaxRate         : Velocidad de destino desea para el tráfico como entero positivo

```

**Nota:** El tipo de servicio establecido para la salida de los paquetes de perfil se establece en cero en el caso de la creación de políticas.

### Archivo de configuración policyd de ejemplo

A continuación se proporciona un ejemplo completo del archivo de configuración /etc/policyd.conf.

```

#loglevel 511    # Registro cronológico detallado
#####
#
# Marcar tráfico rsh en los puertos de origen TCP 513 y 514.
ServiceCategories      tcp_513_514_svc
{
    MaxRate          0          # Marcar sólo
    OutgoingTOS     00011100   # binario
    FlowServiceType ControlledLoad
}

ServicePolicyRules      tcp_513_514_flt
{
    ProtocolNumber    6  # TCP
    SourceAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección origen IP
    DestinationAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección destino IP
    SourcePortRange    513-514
    DestinationPortRange 0-0          # Cualquier puerto destino
    ServiceReference   tcp_513_514_svc
}
#
#####
#
# Definir tráfico UDP conectado en puerto de origen 9000.
ServiceCategories      udp_9000_svc
{
    MaxRate          8192      # kilobits
    MaxTokenBucket   64        # kilobits
    FlowServiceType  Guaranteed
}

ServicePolicyRules      udp_9000_flt
{
    ProtocolNumber    17  # UDP
    SourceAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección origen IP
    DestinationAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección destino IP
    SourcePortRange    9000-9000
    DestinationPortRange 0-0          # Cualquier puerto destino
    ServiceReference   udp_9000_svc
}
#
#####
#
# Marcar y vigilar tráfico finger en el puerto de origen TCP 79.
ServiceCategories      tcp_79_svc
{

```

```

        MaxRate          8      # kilobits
        MaxTokenBucket  32     # kilobits
        OutgoingTOS     00011100   # binario
        FlowServiceType ControlledLoad
    }

    ServicePolicyRules      tcp_79_flt
    {
        ProtocolNumber      6      # TCP
        SourceAddressRange  0.0.0.0-0.0.0.0 # Cualquier dirección origen IP
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección destino IP
        SourcePortRange     79-79
        DestinationPortRange 0-0      # Cualquier puerto destino
        ServiceReference    tcp_79_svc
    }
#
#####
# Marcar y definir tráfico de datos ftp en el puerto de origen TCP 20.
ServiceCategories      tcp_20_svc
{
    MaxRate          81920    # kilobits
    MaxTokenBucket  128      # kilobits
    OutgoingTOS     00011101   # binario
    FlowServiceType Guaranteed
}

    ServicePolicyRules      tcp_20_flt
    {
        ProtocolNumber      6      # TCP
        SourceAddressRange  0.0.0.0-0.0.0.0 # Cualquier dirección origen IP
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Cualquier dirección destino IP
        SourcePortRange     20-20
        DestinationPortRange 0-0      # Cualquier puerto destino
        ServiceReference    tcp_20_svc
    }
#
#####
# Entrada de servidor LDAP.
#ReadFromDirectory
#{
#    LDAP_Server          9.3.33.138  # Dirección IP de servidor LDAP
#    Base                 o=ibm,c=us  # Nombre distinguido base
#    LDAP_SelectedTag     myhost    # Normalmente nombre de sistema principal de cliente
#}
#
#####

```

### Cargas de políticas de IBM SecureWay Directory Server

Si se utiliza el daemon de política con el Servidor LDAP IBM SecureWay Directory, utilice este esquema como guía para actualizar /etc/ldapschema/V3.modifiedschema antes de iniciar el servidor LDAP.

Consulte el apartado “[Planificación y configuración para la resolución de nombres de LDAP \(esquema de IBM SecureWay Directory\)](#)” en la página 215 para obtener detalles.

```

objectClasses {
( ServiceCategories-OID NAME 'ServiceCategories' SUP top MUST
( objectClass $ SelectorTag $ serviceName ) MAY
( description $ FlowServiceType $ MaxRate $ MaxTokenBucket $ OutgoingTos ) )
( ServicePolicyRules-OID NAME 'ServicePolicyRules' SUP top MUST
( objectClass $ PolicyName $ SelectorTag ) MAY
( description $ DestinationAddressRange $ DestinationPortRange $
ProtocolNumber $ ServiceReference $ SourceAddressRange $ SourcePortRange ) )
}

attributeTypes {
( DestinationAddressRange-OID NAME 'DestinationAddressRange' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( DestinationPortRange-OID NAME 'DestinationPortRange' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( FlowServiceType-OID NAME 'FlowServiceType'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( MaxRate-OID NAME 'MaxRate' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( MaxTokenBucket-OID NAME 'MaxTokenBucket' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( OutgoingTos-OID NAME 'OutgoingTos' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( PolicyName-OID NAME 'PolicyName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( ProtocolNumber-OID NAME 'ProtocolNumber' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SelectorTag-OID NAME 'SelectorTag' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

```

```

( ServiceReference-OID NAME 'ServiceReference' SYNTAX
  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SourceAddressRange-OID NAME 'SourceAddressRange' SYNTAX
  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SourcePortRange-OID NAME 'SourcePortRange' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
}

IBMattributeTypes {
( DestinationAddressRange-OID DBNAME ( 'DestinationAddressRange' 'DestinationAddressRange' ) )
( DestinationPortRange-OID DBNAME ( 'DestinationPortRange' 'DestinationPortRange' ) )
( FlowServiceType-OID DBNAME ( 'FlowServiceType' 'FlowServiceType' ) )
( MaxRate-OID DBNAME ( 'MaxRate' 'MaxRate' ) )
( MaxTokenBucket-OID DBNAME ( 'MaxTokenBucket' 'MaxTokenBucket' ) )
( OutgoingTos-OID DBNAME ( 'OutgoingTos' 'OutgoingTos' ) )
( PolicyName-OID DBNAME ( 'PolicyName' 'PolicyName' ) )
( ProtocolNumber-OID DBNAME ( 'ProtocolNumber' 'ProtocolNumber' ) )
( SelectorTag-OID DBNAME ( 'SelectorTag' 'SelectorTag' ) )
( ServiceReference-OID DBNAME ( 'ServiceReference' 'ServiceReference' ) )
( SourceAddressRange-OID DBNAME ( 'SourceAddressRange' 'SourceAddressRange' ) )
( SourcePortRange-OID DBNAME ( 'SourcePortRange' 'SourcePortRange' ) )
}

ldapSyntaxes {
}

matchingRules {
}

```

## Configuración del sistema QoS

Las políticas que se solapan se instalan en el Gestor QoS en un orden no determinante. En el caso de políticas de solapamiento, se deberá especificar el atributo `PolicyRulePriority` de `ServicePolicyRules` para determinar el orden de imposición de las políticas. El atributo `PolicyRulePriority` toma un entero como parámetro y, en el caso de políticas de solapamiento, se impone la norma con el valor de entero más alto.

Para QoS sólo se soportan sockets **UDP** conectados.

La política y los agentes RSVP son independientes entre ellos. Por consiguiente, se debe tener cuidado de no especificar una política que esté en conflicto con una reserva RSVP existente o que quede cubierta por ella. En presencia de tales conflictos, el sistema acepta la primera política o reserva mientras señala una violación para las demás.

Para el funcionamiento correcto, el atributo `MaxTokenBucket` se debe establecer al menos en la MTU máxima de todas las interfaces configuradas en el sistema.

Las modificaciones de política las maneja el agente de políticas suprimiendo automáticamente las políticas existentes e instalando las nuevas. Esto puede hacer que durante un breve periodo de tiempo el tráfico correspondiente reciba el servicio predeterminado (normalmente el esfuerzo óptimo).

## Conformidad con los estándares de IETF para los modelos IntServ y DiffServ

Este release es compatible con los estándares de Internet Engineering Task Force (IETF) en desarrollo para DiffServ (Differentiated Services - Servicios diferenciados) e IntServ (Integrated Services - Servicios integrados) en Internet.

Las siguientes RFC describen diversos componentes del modelo IntServ:

- El uso de RSVP con Servicios integrados de IETF (RFC 2210)
- Especificación del servicio de elementos de red de carga controlada (RFC 2211)
- Especificación de calidad de servicio garantizada (RFC 2212)

Las siguientes RFC describen diversos componentes del modelo DiffServ:

- Definición del campo de Servicios diferenciados (campo DS) en las cabeceras de IPv4 e IPv6 (RFC 2474)
- Una arquitectura para Servicios diferenciados (RFC 2475)

La RFC siguiente describe el uso actual del octeto TOS de IP:

- Tipo de servicio en el conjunto de protocolos Internet (RFC 1349)

Las RFC siguientes describen las futuras prácticas que controlarán el uso del octeto TOS de IP:

- Definición del campo de Servicios diferenciados (campo DS) en las cabeceras de IPv4 e IPv6 (RFC 2474)
- Grupo PHB de reenvío asegurado (RFC 2597)
- Un PHB de reenvío urgente (RFC 2598)

### Soporte de IPv6

QoS sólo da soporte a IPv4. No se soporta IPv6.

### Control de daemon de política

Puede controlar el daemon de política utilizando el SRC (Controlador de recursos del sistema).

Por ejemplo, el mandato:

```
startsrc -s policyd -a "-i 60"
```

inicia el agente de política con un intervalo de renovación de 60 segundos.

El mandato

```
stopsrc -s policyd
```

detiene el daemon de política.

**Nota:** La detención del daemon de política no elimina las políticas instaladas en el kernel. Al iniciar el daemon de política otra vez, se suprimen las políticas antiguas (instaladas anteriormente en el kernel) y las políticas definidas en el archivo /etc/policyd.conf se vuelven a instalar.

Actualmente no se soporta el mandato **refresh** de SRC.

### Mandatos y métodos de QoS

Aquí se listan los mandatos y métodos de calidad de servicio de **TCP/IP**.

Para conocer las actualizaciones importantes de esta documentación, consulte el archivo README en /usr/samples/tcpip/qos.

Se soportan los mandatos de QoS siguientes:

- **qosadd**
- **qoslist**
- **qosmod**
- **qosremove**
- **qosstat**
- **mkqos**
- **rmqos**

Se soportan los métodos de QoS siguientes:

- **cfgqos**
- **ucfgqos**

## Resolución de problemas de TCP/IP

El mandato **netstat** es una buena herramienta para diagnosticar problemas comunes en un entorno de red **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

El mandato **netstat** le permite determinar qué área de la red tiene un problema. Después de haber aislado el problema en un área, puede utilizar herramientas más sofisticadas para continuar. Por ejemplo, puede utilizar **netstat -i** y **netstat -v** para determinar si tiene un problema con una interfaz de hardware determinada y, a continuación, ejecutar diagnósticos para aislar el problema adicionalmente. O,

si el mandato **netstat -s** muestra que hay errores de protocolo, puede utilizar entonces los mandatos **trpt** o **iptrace**.

### Problemas de comunicaciones

Los problemas comunes de comunicaciones de **TCP/IP** incluyen la imposibilidad de comunicarse con un sistema principal de la red y problemas de direccionamiento. A continuación se proporciona algunas soluciones.

Si no se puede comunicar con un sistema principal de la red:

- Intente ponerse en contacto con el sistema principal, utilizando el mandato **ping**. Ejecute el mandato **ping** en el sistema principal local para verificar que la interfaz local a la red está activa y en ejecución.
- Intente resolver el nombre del sistema principal, utilizando el mandato **host**. Si el nombre no se resuelve, tiene un problema de resolución de nombres. Consulte el apartado “[Problemas de resolución de nombres](#)” en la página 498 para obtener más información.

Si el nombre se resuelve y está intentando ponerse en contacto con un sistema principal de otra red, es posible que tenga un problema de direccionamiento. Consulte el apartado “[Problemas de direccionamiento de TCP/IP](#)” en la página 499 para obtener más información.

- Si la red es una Red en anillo, compruebe si el sistema principal de destino está en otro anillo. Si es así, probablemente el campo **allcast** está establecido incorrectamente. Utilice la vía de acceso rápida System Management Interface Tool (SMIT) smit chinet para acceder al menú Interfaces de red. A continuación, establezca el campo Confinar difusión a la red en anillo local en **no** en el diálogo de la Red en anillo.
- Si hay un gran número de paquetes de **ARP (Protocolo de resolución de direcciones)** en la red, verifique que la máscara de subred esté establecida correctamente. Esta condición se conoce como tormenta de difusión y puede afectar el rendimiento del sistema.

### Problemas de resolución de nombres

Las rutinas de resolución de sistemas principales que ejecutan **TCP/IP** intentan resolver los nombres, utilizando estas fuentes en el orden listado.

1. Servidor de nombres de DOMINIO (**named**)
2. NIS (Network Information Service - Servicio de información de red)
3. Archivo /etc/hosts local

### Resolución de problemas de sistema principal de cliente

Si no puede resolver un nombre de sistema principal y está utilizando la resolución de nombres normales (utilizando el archivo /etc/hosts), verifique que en el archivo /etc/hosts estén el nombre de sistema principal y la información de dirección IP (Protocolo Internet) correcta.

Si no logra resolver un nombre de sistema principal y está utilizando un servidor de nombres, siga estos pasos:

1. Verifique que tiene un archivo **resolv.conf** que especifica el nombre de dominio y la dirección Internet de un servidor de nombres.
2. Verifique que el servidor de nombres local está activo emitiendo el mandato **ping** con la dirección IP del servidor de nombres (que se encuentra en el archivo local **resolv.conf**).
3. Si el servidor de nombres local está activo, verifique que el daemon **named** del servidor de nombres local está activo emitiendo el mandato **lssrc -s named** en el servidor de nombres.
4. Si está ejecutando **syslogd**, compruebe los mensajes registrados.  
La salida de estos mensajes se define en el archivo /etc/syslog.conf.

Si estos pasos no identifican el problema, compruebe el sistema principal de servidor de nombres.

### Resolución de problemas de sistema principal de servidor de nombres

Utilice este procedimiento para resolver problemas de servidor de nombres de sistema principal.

Si no logra resolver un nombre de sistema principal:

1. Verifique que el daemon **named** esté activo emitiendo el mandato siguiente:

```
lssrc -s named
```

2. Verifique que la dirección del sistema principal de destino exista y sea correcta en la base de datos de servidor de nombres.

Envíe una señal **SIGINT** al daemon **named** para volcar la base de datos y almacenarla en antememoria en el archivo `/var/tmp/named_dump.db`. Verifique que la dirección que está intentando resolver se encuentre allí y sea correcta.

Añada o corrija la información de resolución de nombre en dirección en el archivo de datos de sistemas principales **named** para el servidor de nombres maestro del dominio. A continuación, emita el siguiente mandato **SRM** para volver a leer los archivos de datos:

```
refresh -s named
```

3. Verifique que las peticiones de resolución de nombres se estén procesando.

Para ello, entre el daemon **named** desde la línea de mandatos y especifique un nivel de depuración. Los niveles de depuración válidos son 1 a 9. Cuando más alto es el nivel, más información registra el mecanismo de depuración.

```
startsrc -s named -a "-d NivelDepuración"
```

4. Compruebe los problemas de configuración en los archivos de datos **named**.

Para obtener más información, consulte el apartado “Resolución de servidor de nombres” en la página 192. Además, consulte “DOMAIN Data File Format,”, “DOMAIN Reverse Data File Format,” “DOMAIN Cache File Format,” y “DOMAIN Local Data File Format” en la sección *Referencia de archivos*.

**Nota:** Un error común es el uso incorrecto de . (punto) y de @ (signo de arroba) en los archivos de datos DOMAIN.

Si los usuarios externos no pueden alcanzar los dominios, asegúrese de que todos los servidores de nombres no maestros (esclavo, intermedio) tengan información de tiempo de vida (TTL) igual en los archivos de datos DOMAIN.

Si las rutinas de resolución externas consultan los servidores constantemente, asegúrese de que los servidores están distribuyendo archivos de datos DOMAIN con valores TTL razonables. Si el TTL es cero u otro valor pequeño, los datos que transfiere excederán el tiempo de espera muy rápidamente. Establezca el valor mínimo en los registros de inicio de autorización (SOA) en una semana o más para resolver este problema.

### Problemas de direccionamiento de TCP/IP

Si no puede alcanzar un sistema principal de destino, considere las soluciones a las siguientes situaciones.

- Si recibe un mensaje de error Red inalcanzable, asegúrese de que se ha definido una ruta al sistema principal de pasarela y de que dicha ruta es correcta. Compruébelo utilizando el mandato **netstat -r** para listar las tablas de direccionamiento de kernel.
- Si recibe un mensaje de error No hay ruta al sistema principal, verifique que la interfaz de red local esté activa emitiendo el mandato **ifconfig nombre\_interfaz**. La salida indica si la interfaz está activa o no. Utilice el mandato **ping** para intentar y alcanzar otro sistema principal de la red.
- Si recibe un mensaje de error Tiempo de espera de conexión excedido:
  - Verifique que la pasarela local esté activa utilizando el mandato **ping** con el nombre o la dirección Internet de la pasarela.
  - Asegúrese de que se ha definido una ruta al sistema principal de pasarela y de que dicha ruta es correcta. Compruébelo utilizando el mandato **netstat -r** para listar las tablas de direccionamiento de kernel.
  - Asegúrese de que el sistema principal con el que desea comunicarse tiene una entrada de tabla de direccionamiento en la máquina.

- Si está utilizando el direccionamiento estático, asegúrese de que se ha definido una ruta al sistema principal de destino y al sistema principal de pasarela. Compruébelo utilizando el mandato **netstat -r** para listar las tablas de direccionamiento de kernel.

**Nota:** Asegúrese de que el sistema principal con el que desea comunicarse tiene una entrada de tabla de direccionamiento en la máquina.

- Si está utilizando el direccionamiento dinámico, verifique que la pasarela esté listada y sea correcta en las tablas de direccionamiento de kernel emitiendo el mandato **netstat -r**.
- Si el sistema principal de pasarela está utilizando el RIP (**Routing Information Protocol - Protocolo de información de direccionamiento**) con el daemon **routed**, asegúrese de que se ha configurado una ruta estática al sistema principal de destino en el archivo /etc/gateways.

**Nota:** Sólo necesita realizar esta acción si el daemon de direccionamiento no puede identificar la ruta a un sistema principal distante mediante consultas a otras pasarelas.

- Si el sistema principal de pasarela utiliza **RIP** con el daemon **gated**, asegúrese de que se ha configurado una ruta estática al sistema principal de destino en el archivo **gated.conf**.
- Si está utilizando el direccionamiento dinámico con el daemon **routed**:
  - Si **routed** no puede identificar la ruta mediante consultas (por ejemplo, si el sistema principal de destino no ejecuta **RIP**, compruebe el archivo /etc/gateways para verificar que se ha definido una ruta al sistema principal de destino).
  - Asegúrese de que las pasarelas responsables de reenviar paquetes al sistema principal están activas y están ejecutando el **RIP**. De lo contrario, necesitará definir una ruta estática.
  - Ejecute el daemon **routed** utilizando la opción de depuración para registrar dicha información como paquetes incorrectos recibidos. Invoque el daemon desde la línea de mandatos utilizando el siguiente mandato:

```
startsrc -s routed -a "-d"
```

- Ejecute el daemon **routed** utilizando el distintivo **-t**, lo que hace que todos los paquetes enviados o recibidos se graben en la salida estándar. Cuando se ejecuta **routed** en esta modalidad, permanece bajo el control del terminal que lo ha iniciado. Por consiguiente, una interrupción del terminal de control mata el daemon.
- Si está utilizando el direccionamiento dinámico con el daemon **gated**:
  - Verifique que el archivo /etc/gated.conf esté configurado correctamente y que esté ejecutando los protocolos correctos.
  - Asegúrese de que la pasarela de la red de origen está utilizando el mismo protocolo que la pasarela de la red de destino.
  - Asegúrese de que la máquina con la que está intentando comunicarse tiene una ruta de retorno a la máquina de sistema principal.
  - Verifique que los nombres de pasarela del archivo **gated.conf** correspondan a los nombres de pasarela listados en el archivo /etc/networks.
- Si está utilizando los protocolos **RIP** o **HELLO** y no se pueden identificar rutas al destino mediante consultas de direccionamiento, compruebe el archivo **gated.conf** para verificar que se ha definido una ruta al sistema principal de destino. Establezca rutas estáticas bajo las siguientes condiciones:
  - El sistema principal de destino no está ejecutando el mismo protocolo que el sistema principal de origen, por consiguiente no puede intercambiar información de direccionamiento.
  - Una pasarela distante (una pasarela que está en un sistema autónomo diferente del sistema principal de origen) debe alcanzar el sistema principal. El **RIP** sólo se puede utilizar entre sistemas principales del mismo sistema autónomo.

Si falla todo lo demás, es aconsejable que active el rastreo para el daemon de direccionamiento (**routed** o **gated**). Utilice el mandato **traceson** de SRC desde la línea de mandatos o envíe una señal al daemon para especificar diferentes niveles de rastreo. Consulte el daemon **gated** o el daemon **routed** para obtener información específica sobre el envío de señales a estos daemons.

## Resolución de problemas con el soporte de SRC

Utilice estas sugerencias para resolver problemas comunes con el Controlador de recursos del sistema.

- Si no entran en vigor los cambios en el archivo /etc/inetd.conf:

Actualice el daemon **inetd** emitiendo el mandato **refresh -s inetd** o el mandato **kill -1 PIDInetd**.

- Si **startsrc -s [nombre subsistema]** devuelve el siguiente mensaje de error:

```
0513-00 El  
Controlador de recursos del sistema no está activo.
```

El subsistema Controlador de recursos del sistema no se ha activado. Emite el mandato **srcmstr &** para iniciar el SRC y, a continuación, vuelva a emitir el mandato **startsrc**.

Es posible que también desee intentar iniciar el daemon desde la línea de mandatos sin soporte de SRC.

- Si **refresh -s [nombre subsistema]** o **lssrc -ls [nombre subsistema]** devuelve el siguiente mensaje de error:

```
[nombre subsistema] no soporta  
esta opción.
```

El subsistema no soporta la opción SRC emitida. Compruebe la documentación del subsistema para verificar las opciones que el subsistema soporta.

- Si se visualiza el mensaje siguiente:

```
SRC no se ha encontrado,  
se continúa sin soporte de SRC.
```

Se ha invocado un daemon directamente desde la línea de mandatos en lugar de utilizar el mandato **startsrc**. Esto no es un problema. Sin embargo, los mandatos SRC, por ejemplo **stopsrc** y **refresh**, no manipularán un subsistema que se invoca directamente.

Si el daemon **inetd** está activo y en ejecución correctamente y parece que el servicio apropiado es correcto pero sigue sin poder conectarse, intente ejecutar los procesos de daemon **inetd** mediante un depurador.

1. Detenga el daemon **inetd** temporalmente:

```
stopsrc -s inetd
```

El mandato **stopsrc** detiene los subsistemas como el daemon **inetd**.

2. Edite el archivo **syslog.conf** para añadir una línea de depuración en la parte inferior. Por ejemplo:

```
vi /etc/syslog.conf
```

a. Añada la línea `*.debug /tmp/myfile` en la parte inferior del archivo y salga.

b. El archivo que especifique debe existir (/tmp/myfile en este ejemplo). Puede utilizar el mandato **touch** para hacer que exista el archivo.

3. Renueve el archivo:

- Si está utilizando SRC, entre:

```
refresh -s syslogd
```

- Si no está utilizando SRC, mate el daemon **syslogd**:

```
kill -1 `ps -e | grep /etc/syslogd | cut -c1-7`
```

4. Inicie la copia de seguridad del daemon **inetd** con la depuración habilitada:

```
startsrd -s inetd -a "-d"
```

El distintivo **-d** habilita la depuración.

5. Intente realizar una conexión para registrar los errores en el archivo de depuración /tmp/myfile. Por ejemplo:

```
tn bastet
Trying...
connected to bastet
login:>
Connection closed
```

6. Compruebe si hay algo que parezca un problema en el archivo de depuración. Por ejemplo:

```
tail -f /tmp/myfile
```

### Resolución de problemas de telnet o rlogin

Estas explicaciones pueden ser útiles en la resolución de problemas con el mandato **telnet** o **rlogin**.

Si tiene problemas con la distorsión de pantalla en aplicaciones de pantalla completa:

1. Compruebe la variable de entorno TERM emitiendo uno de los mandatos siguientes:

```
env
```

```
echo $TERM
```

2. Verifique que la variable TERM se establezca en un valor que coincida con el tipo de pantalla de terminal que está utilizando.

Los submandatos de **telnet** que pueden ayudar en la depuración de problemas incluyen:

Item	Descripción
<b>display</b>	Visualiza los valores de establecimiento y conmutación.
<b>toggle</b>	Conmuta la visualización de todos los datos de red en hexadecimal.
<b>toggle options</b>	Conmuta la visualización de opciones de proceso de <b>telnet</b> internas.

Si el daemon **inetd** puede ejecutar el servicio **telnet** pero aún no es posible conectarse utilizando el mandato **telnet**, es posible que haya algo incorrecto con la interfaz **telnet**.

1. Verifique que **telnet** esté utilizando el tipo de terminal correcto.

- a. Compruebe la variable \$TERM en la máquina:

```
echo $TERM
```

- b. Inicie la sesión en la máquina a la que está intentando conectarse y compruebe la variable \$TERM:

```
echo $TERM
```

2. Utilice las opciones de depuración de la interfaz de **telnet** entrando el mandato **telnet** sin distintivos.

```
telnet
tn>
```

- a. Escriba open *sistpral* donde *sistpral* es el nombre de la máquina.

- b. Pulse Control-T para obtener el indicador tn%gt;.

- c. En el indicador tn>, escriba debug para la modalidad de depuración.

3. Intente conectarse a otra máquina utilizando la interfaz **telnet**:

```
telnet bastet
Trying...
Connected to bastet
Escape character is '^T'.
```

Observe la pantalla mientras se desplazan hacia arriba en la pantalla los diversos mandatos. Por ejemplo:

```
SENT do ECHO
SENT do SUPPRESS GO AHEAD
SENT will TERMINAL TYPE (reply)
SENT do SUPPORT SAK
SENT will SUPPORT SAK (reply)
RCVD do TERMINAL TYPE (don't reply)
RCVD will ECHO (don't reply)
RCVD will SUPPRESS GO AHEAD (don't reply)
RCVD wont SUPPORT SAK (reply)
SENT dont SUPPORT SAK (reply)
RCVD do SUPPORT SAK (don't reply)
SENT suboption TELOPT_NAWS Width 80, Height 25
RCVD suboption TELOPT_TTYPE SEND
RCVD suboption TELOPT_TTYPE aixterm
...
```

4. Compruebe en /etc/termcap o /usr/lib/terminfo la definición de aixterm. Por ejemplo:

```
ls -a /usr/lib/terminfo
```

5. Si falta la definición de aixterm, añádala creando el archivo ibm.ti. Por ejemplo:

```
tic ibm.ti
```

El mandato **tic** es un compilador de información de terminal.

Se pueden producir problemas con las teclas de función y de flecha cuando se utilizan los mandatos **rlogin** y **telnet** con programas que utilizan curses ampliado. Las teclas de función y de flecha generan secuencias de escape, que se dividen si se asigna un tiempo excesivamente insuficiente para la secuencia de teclas entera. Curses espera una cantidad de tiempo específica para decidir si un Esc indica sólo la tecla de escape o el inicio de una secuencia de escape de varios bytes generada por otras teclas, por ejemplo teclas de cursor, la tecla de acción y las teclas de función.

Si, durante la cantidad de tiempo asignada, después del Esc no hay datos o hay datos que no son válidos, curses decide que Esc es la tecla de escape y se divide la secuencia de teclas. El retardo resultante del mandato **rlogin** o **telnet** depende de la red. A veces las teclas de flecha y de función funcionan y a veces no, según la velocidad de la red a la que se conecten. Si se establece la variable de entorno ESCDELAY en un valor grande (1000 a 1500), este problema se soluciona de forma efectiva.

### Problemas de configuración de TCP/IP

Las interfaces de red se configuran automáticamente durante el primer arranque del sistema después de haber instalado la tarjeta adaptadora. Sin embargo, todavía necesita establecer algunos valores iniciales para **TCP/IP** incluidos el nombre de sistema principal, la dirección de Internet y la máscara de subred.

Para ello, puede utilizar la interfaz de SMIT de las siguientes maneras:

- Utilice la vía de acceso rápida smit mktcpip para establecer los valores iniciales para el nombre de sistema principal, la dirección de Internet y la máscara de subred.
- Utilice la vía de acceso rápida smit mktcpip para especificar un servidor de nombres a fin de proporcionar el servicio de resolución de nombres. (Tenga en cuenta que smit mktcpip sólo configura una interfaz de red.)
- Utilice la vía de acceso rápida smit chinet para establecer otros atributos de red.

Es posible que también desee configurar rutas estáticas que el sistema principal necesite para enviar información de transmisión, por ejemplo una ruta a la pasarela local. Utilice la vía de acceso rápida de SMIT, smit mkroute, para establecer de forma permanente en la base de datos de configuración.

Si tiene otros problemas con la configuración, consulte el apartado “Configuración de TCP/IP” en la página 109 para obtener más información.

### Problemas comunes de TCP/IP con interfaces de red

Las interfaces de red se configuran automáticamente durante el primer arranque del sistema después de haber instalado la tarjeta adaptadora. Sin embargo, hay determinados valores que se deben establecer para que se inicie **TCP/IP**. Estos valores incluyen el nombre de sistema principal y la dirección de Internet y se pueden establecer utilizando la vía de acceso rápida de SMIT smit mktcpip.

Si elige el método de SMIT, utilice la vía de acceso rápida smit mktcpip para establecer estos valores permanentemente en la base de datos de configuración. Utilice las vías de acceso rápidas smit chinet y smit hostname para cambiarlos en un sistema en ejecución. La vía de acceso rápida smit mktcpip configura **TCP/IP** mínimamente. Para añadir adaptadores, utilice el menú Configuración avanzada, al que puede llegar mediante la vía de acceso rápida smit tcpip.

Si ya ha hecho estas comprobaciones para verificar la precisión y aún tiene problemas al enviar y recibir información, compruebe lo siguiente:

- Verifique que el adaptador de red tiene una interfaz de red ejecutando el mandato **netstat -i**. La salida debe listar una interfaz, por ejemplo **tr0**, en la columna Nombre. Si no es así, cree una interfaz de red especificando la vía de acceso rápida SMIT smit mkinet.
- Verifique que la dirección IP para la interfaz es correcta ejecutando el mandato **netstat -i**. La salida debe listar la dirección IP en la columna de Red. Si no es correcto, establezca la dirección IP especificando la vía de acceso rápida SMIT smit chinet.
- Utilice el mandato **arp** para asegurarse de que tiene la dirección IP completa para la máquina de destino. Por ejemplo:

```
arp -a
```

El mandato **arp** busca la dirección de adaptador físico. Es posible que este mandato muestre una dirección incompleta. Por ejemplo:

```
? (192.100.61.210) at (incomplete)
```

Esto puede deberse a que hay una máquina desenchufada, una dirección abandonada sin ninguna máquina en esa dirección determinada o a un problema de hardware (por ejemplo una máquina que se conecta y recibe paquetes pero no puede devolver paquetes).

- Busque errores en la tarjeta adaptadora. Por ejemplo:

```
netstat -v
```

El mandato **netstat -v** muestra estadísticas para los controladores de dispositivo de adaptador Ethernet, Token Ring, X.25 y 802.3. El mandato también muestra datos de registro de errores y de red de todos los controladores de dispositivo activos en una interfaz incluyendo: Sin error Mbuf, Sin error extensión Mbuf y Paqts Transmitidos y Errores Detectados Adaptador.

- Compruebe el registro cronológico de errores ejecutando el mandato **erprt** para asegurarse de que no hay problemas de adaptador.
- Verifique que la tarjeta adaptadora es correcta ejecutando los diagnósticos. Utilice la vía de acceso rápida smit diag o el mandato **diag**.

### Problemas de TCP/IP con una interfaz de red SLIP

En general, el método más efectivo para depurar problemas con una interfaz **SLIP (Serial Line Interface Protocol)** es volver a rastrear la configuración, verificando cada paso.

Sin embargo, también puede:

- Verificar que el proceso **slattach** se está ejecutando y está utilizando el puerto de tty correcto emitiendo el mandato **ps -ef**. Si no se ejecuta, ejecute el mandato **slattach**. Consulte el apartado “Configuración de SLIP a través de un módem” en la página 714 o el apartado “Configuración de SLIP

a través de un cable de módem nulo” en la página 715 para conocer la sintaxis exacta que debe utilizar).

- Verifique que las direcciones de punto a punto se especifican correctamente entrando la vía de acceso rápida smit chinet.

Seleccione la interfaz **SLIP**. Asegúrese de que los campos **DIRECCIÓN DE INTERNET** y **DIRECCIÓN DE DESTINO** sean correctos.

Si el módem no funciona correctamente:

- Asegúrese de que el módem se ha instalado correctamente. Consulte el manual de instalación del módem.
- Verifique que el control de flujo que realiza el módem esté desactivado.

Si la tty no funciona correctamente, verifique que la velocidad en baudios de tty y las características de módem estén establecidas correctamente en la base de datos de configuración entrando la vía de acceso rápida smit tty.

#### **Problemas de TCP/IP con una interfaz de red Ethernet**

Consulte esta lista de comprobación si persisten los problemas de **TCP/IP** en una interfaz de red Ethernet.

Si la interfaz de red se ha inicializado, las direcciones se han especificado correctamente y ha verificado que la tarjeta adaptadora es correcta:

- Verifique que está utilizando un conector en T enchufado directamente en el transmisor/receptor de entrada /salida.
- Asegúrese de que está utilizando un cable Ethernet. (El cable Ethernet es de 50 OHM.)
- Asegúrese de que está utilizando terminadores Ethernet. (Los terminadores de Ethernet son de 50 OHM.)
- Los adaptadores Ethernet se pueden utilizar con el transmisor/receptor que está en la tarjeta o con un transmisor/receptor externo. Hay un puente en el adaptador para especificar cuál se está utilizando. Verifique que el puente esté colocado correctamente (consulte el manual del adaptador para obtener instrucciones).
- Verifique esté utilizando el tipo de conector Ethernet correcto (fino es BNC; grueso es DIX). Si cambia este tipo de conector, utilice la vía de acceso rápida **smit chgenet** de SMIT para establecer el campo Aplicar cambio sólo a la base de datos. (Establezca Sí en SMIT). Reinicie la máquina para aplicar el cambio de configuración. (Consulte el apartado “Configuración y gestión de los adaptadores” en la página 170.)

#### **Problemas de TCP/IP con una interfaz de Red en anillo**

Utilice estas directrices para resolver problemas de comunicaciones con la interfaz de red.

Si no se puede comunicar con alguna de las máquinas de la red aunque se haya inicializado la interfaz de red, se haya especificado correctamente las direcciones y haya verificado que la tarjeta adaptadora es correcta:

- Compruebe si los sistemas principales con los que no se puede comunicar están en un anillo diferente. Si es así, utilice la vía de acceso rápida smit chinet de SMIT para comprobar el campo Confinar difusión a la Red en anillo local. Establezca No en SMIT.
- Compruebe si el adaptador de Red en anillo se ha configurado para ejecutarse a la velocidad correcta del anillo. Si no se ha configurado correctamente, utilice SMIT para cambiar el atributo de velocidad de anillo de adaptador (consulte el apartado “Configuración y gestión de los adaptadores” en la página 170). Cuando se reinicia **TCP/IP**, el adaptador de Red en anillo tiene la misma velocidad de anillo que el resto de la red.

#### **Problemas de TCP/IP con un puente de Red en anillo a Ethernet**

Si no se puede comunicar entre una Red en anillo y una red Ethernet utilizando un puente y ha verificado que el puente funciona correctamente, es posible que el adaptador Ethernet esté desactivando paquetes.

Una máquina desactiva los paquetes si el paquete de entrada (incluidas las cabeceras) es mayor que el valor de la unidad máxima de transmisión (MTU) del adaptador de red. Por ejemplo, un paquete de 1500 bytes enviado por un adaptador de Red en anillo a través de un puente recopila una cabecera de control de enlace lógico (LLC) de 8 bytes, haciendo que el tamaño total del paquete sea 1508. Si la MTU de adaptador Ethernet de recepción está establecida en 1500, se desactiva el paquete.

Compruebe los valores de MTU de ambos adaptadores de red. Para permitir la cabecera LLC de ocho bytes que el adaptador de Red en anillo conecta a los paquetes de salida, establezca el valor de MTU para el adaptador de Red en anillo en un valor que sea como mínimo el valor de MTU para el adaptador Ethernet menos ocho bytes. Por ejemplo, establezca la MTU para un adaptador de Red en anillo en 1492 para que se comunique con un adaptador Ethernet con una MTU de 1500.

### **Problemas de TCP/IP con un puente de Red en anillo a Red en anillo**

Cuando opere a través de un puente, cambie el valor predeterminado de 1500 para la Unidad máxima de transmisión (MTU) por un valor que sea igual al campo de información máxima (trama I máxima), anunciado por el puente en el campo de control de direccionamiento, menos ocho.

Para encontrar el valor de campo de control de direccionamiento, utilice el daemon **iptrace** para examinar los paquetes de entrada. Los bits 1, 2 y 3 del byte 1 son los bits de trama más grande, que especifican el campo de información máxima que se puede transmitir entre dos estaciones que se comunican en una ruta específica. Consulte lo siguiente para conocer el formato del campo de control de direccionamiento:



Figura 25. Campo de control de direccionamiento

Esta ilustración muestra el byte 0 y el byte 1 de un campo de control de direccionamiento. Los ocho bits del byte uno son B, B, B, B, L, L, L, L. Los ocho bits del byte 1 son D, F, F, F, r, r, r, r.

Los valores para los bits de trama más grande son los siguientes:

<b>Ítem</b>	<b>Descripción</b>
<b>00</b>	Especifica un máximo de 516 bytes en el campo de información.
<b>01</b>	Especifica un máximo de 1500 bytes en el campo de información.
<b>10</b>	Especifica un máximo de 2052 bytes en el campo de información.
<b>11</b>	Especifica un máximo de 4472 bytes en el campo de información.
<b>00</b>	Especifica un máximo de 8144 bytes en el campo de información.
<b>01</b>	Reservado.
<b>10</b>	Reservado.
<b>11</b>	Se utiliza en tramas de difusión de todas las rutas.

Por ejemplo, si el valor máximo de trama I es 2052 en el campo de control de direccionamiento, el tamaño de MTU se debe establecer en 2044. Esto sólo se aplica a interfaces de red en anillo.

**Nota:** Cuando se utiliza **iptrace**, el archivo de salida *no* debe estar en un NFS (Sistema de archivos de red).

### **Problemas de TCP/IP al comunicarse con un sistema principal remoto**

Si no se puede comunicar con un sistema principal remoto, intente seguir estas sugerencias.

- Ejecute el mandato **ping** en el sistema principal local para verificar que la interfaz local a la red está activa y en ejecución.
- Utilice el mandato **ping** para sistemas principales y pasarelas que son progresivamente más saltos desde el sistema principal local para determinar el punto en el que falla la comunicación.

Si tiene problemas con la pérdida de paquetes o tiene retardos en la entrega de paquetes, pruebe lo siguiente:

- Utilice el mandato **trpt** para rastrear paquetes a nivel de socket.
- Utilice el mandato **iptrace** para rastrear todas las capas de protocolo.

Si no se puede comunicar entre una Red en anillo y una red Ethernet utilizando un puente y ha verificado que el puente es correcto:

- Compruebe los valores de MTU de ambos adaptadores. Los valores de MTU deben ser compatibles para permitir las comunicaciones. Una máquina desactiva los paquetes si el paquete de entrada (incluidas las cabeceras) es mayor que los valores de MTU del adaptador. Por ejemplo, un paquete de 1500 bytes enviado a través de un puente recopila una cabecera LLC de 8 bytes, lo que hace que el tamaño total del paquete sea 1508. Si la MTU de máquina de recepción está establecida en 1500, un paquete de 1508 bytes se desactivará.

### **Problemas de TCP/IP con la respuesta de snmpd a las consultas**

Si **snmpd** no está respondiendo a las consultas y no se reciben mensajes de registro cronológico, es posible que el paquete sea demasiado grande para el manejador de paquetes de **UDP (User Datagram Protocol)** de kernel.

Si éste es el caso, incremente las variables de kernel, **udp\_sendspace** y **udp\_recvspace**, emitiendo los mandatos siguientes:

```
no -o udp_sendspace=64000  
no -o udp_recvspace=64000
```

El tamaño máximo para un paquete **UDP** es 64 K. Si la consulta tiene más de 64 K de tamaño, se rechazará. Parta el paquete en paquetes más pequeños para evitar este problema.

### **Problemas de TCP/IP con el Protocolo de configuración dinámica de sistemas principales**

En el caso de que no pueda obtener datos de configuración, intente las siguientes soluciones.

Si no puede obtener una dirección IP u otros parámetros de configuración:

- Compruebe si ha especificado que se debe configurar una interfaz. Esto puede realizarse utilizando la vía de acceso rápida de SMIT **smit dhcp**.
- Compruebe si hay un servidor en la red local o un agente de relé configurado para obtener las peticiones de la red local.
- Compruebe si el programa **dhcpcd** está en ejecución. Si no lo está, utilice el mandato **startsrc -s dhcpcd**.

## **Mandatos TCP/IP**

**TCP/IP** forma parte de la estructura subyacente del sistema. Le permite comunicarse con otro terminal o sistema simplemente ejecutando un mandato o programa.

**TCP/IP** forma parte de la estructura subyacente del sistema. Le permite comunicarse con otro terminal o sistema simplemente ejecutando un mandato o programa. El sistema se encarga del resto.

<b>Item</b>	<b>Descripción</b>
<b>chnamsv</b>	Cambia la configuración de servicio de nombres basada en <b>Transmission Control Protocol/Internet Protocol (TCP/IP)</b> en un sistema principal.

<b>Item</b>	<b>Descripción</b>
<b>chptrsv</b>	Cambia una configuración de servicio de impresión en una máquina de cliente o servidor.
<b>hostent</b>	Manipula directamente las entradas de correlación de direcciones de la base de datos de configuración del sistema.
<b>ifconfig</b>	Configura o visualiza parámetros de interfaz de red para una red, utilizando <b>TCP/IP</b> .
<b>mknamsv</b>	Configura el servicio de nombres basado en <b>TCP/IP</b> en un sistema principal para un cliente.
<b>mkptrsv</b>	Configura el servicio de impresión basado en <b>TCP/IP</b> en un sistema principal.
<b>mktcpip</b>	Establece los valores necesarios para iniciar <b>TCP/IP</b> en un sistema principal.
<b>no</b>	Configura opciones de red.
<b>rmnamsv</b>	Desconfigura el servicio de nombres basado en <b>TCP/IP</b> en un sistema principal.
<b>rmptrsv</b>	Desconfigura un servicio de impresión en una máquina de cliente o servidor.
<b>slattach</b>	Conecta líneas serie como interfaces de red.
<b>arp</b>	Visualiza o cambia la dirección de Internet en tablas de conversión de direcciones de hardware utilizadas por el <b>Protocolo de resolución de direcciones (ARP)</b> .
<b>gettable</b>	Obtiene tablas de sistema principal de formato NIC (Network Information Center - Centro de información de red) de un sistema principal.
<b>hostid</b>	Establece o visualiza el identificador del sistema principal local actual.
<b>hostname</b>	Establece o visualiza el nombre del sistema principal local actual.
<b>htable</b>	Convierte archivos de sistema principal a formato utilizado por las rutinas de biblioteca de red.
<b>ipreport</b>	Genera un informe de rastreo de paquetes desde el archivo de rastreo de paquetes especificado.
<b>iptrace</b>	Proporciona rastreo de paquetes a nivel de interfaz para los protocolos Internet.
<b>lsnamsv</b>	Muestra la información de servicio de nombres almacenada en la base de datos.
<b>lsprtsv</b>	Muestra la información de servicio de impresión almacenada en la base de datos.
<b>mhhosts</b>	Genera el archivo de tablas de sistema principal.
<b>namerslv</b>	Manipula directamente las entradas de servidor de nombres de dominio para las rutinas de resolución locales en la base de datos configuración de sistema.
<b>netstat</b>	Muestra el estado de la red.
<b>route</b>	Manipula manualmente las tablas de direccionamiento.
<b>ruser</b>	Manipula directamente las entradas en tres bases de datos de sistema independientes que controlan el acceso de sistemas principales externos a los programas.
<b>ruptime</b>	Visualiza el estado de cada sistema principal de una red.
<b>securetcpip</b>	Habilita la característica de seguridad de red.
<b>setclock</b>	Establece la hora y la fecha de un sistema principal en una red.
<b>timedc</b>	Devuelve información acerca del daemon <b>timed</b> .
<b>trpt</b>	Realiza el rastreo de protocolo en sockets <b>TCP (Transmission Control Protocol)</b> .

## Mandatos de SRC

Los mandatos de SRC pueden afectar a un daemon, a un grupo de daemons o a un daemon y los daemons que éste controla (subsistema con subservidores).

Además, algunos daemons **TCP/IP** no responden a todos los mandatos de SRC. A continuación se proporciona una lista de mandatos de SRC que se pueden utilizar para controlar los daemons **TCP/IP** y las excepciones.

Item	Descripción
<b>startsrc</b>	Inicia todos los subsistemas <b>TCP/IP</b> y los subservidores <b>inetd</b> . El mandato <b>startsrc</b> funciona para todos los subsistemas <b>TCP/IPP</b> y los subservidores <b>inetd</b> .
<b>stopsrc</b>	Detiene todos los subsistemas <b>TCP/IP</b> y los subservidores <b>inetd</b> . Este mandato también se denomina mandato <b>stop normal</b> . El mandato <b>stop normal</b> permite a los subsistemas procesar todo el trabajo pendiente y terminarlo ordenadamente. Para los subservidores <b>inetd</b> , se permite iniciar todas las conexiones pendientes y se permite completar todas las conexiones existentes. El mandato <b>stop normal</b> funciona para todos los subsistemas <b>TCP/IP</b> y los subservidores <b>inetd</b> .
<b>stopsrc -f</b>	Detiene todos los subsistemas <b>TCP/IP</b> y los subservidores <b>inetd</b> . Este mandato también se denomina <b>stop force</b> . El mandato <b>stop force</b> termina inmediatamente todos los subsistemas. Para los subservidores <b>inetd</b> , terminan inmediatamente todas las conexiones pendientes y las conexiones existentes.
<b>refresh</b>	Renueva los siguientes subsistemas y subservidores: los subsistemas <b>inetd</b> , <b>syslogd</b> , <b>named</b> , <b>dhcpsd</b> y <b>gated</b> .
<b>lssrc</b>	Proporciona un estado corto para los subsistemas, que es el estado del subsistema especificado (activo o inoperativo). También proporciona un estado corto para los subservidores <b>inetd</b> . El estado corto para los subservidores <b>inetd</b> incluye: nombre de subservidor, estado, descripción de subservidor, nombre de mandato y los argumentos con los que se ha invocado.

<b>Item</b>	<b>Descripción</b>
<b>lssrc -l</b>	Proporciona el estado corto más información adicional (estado largo) para los siguientes subsistemas:
<b>gated</b>	Estate de depuración o rastreo, protocolos de direccionamiento activos, tablas de direccionamiento, señales aceptadas y su función.
<b>inetd</b>	Estate de depuración, lista de subservidores activos y su estado corto; señales aceptadas y su función.
<b>named</b>	Estate de depuración, información de archivo named .conf.
<b>dhcpsd</b>	Estate de depuración, todas las direcciones IP controladas y el estado actual.
<b>routed</b>	Estate de depuración y rastreo, estado de suministro de información de direccionamiento, tablas de direccionamiento.
<b>syslogd</b>	Información de configuración de <b>syslogd</b> .
	El mandato <b>lssrc -l</b> también proporciona estado largo para subservidores <b>inetd</b> . El estado largo incluye información de estado corto e información de conexión activa. Algunos subservidores proporcionan información adicional. La información adicional proporcionada por el subservidor incluye:
<b>ftpd</b>	Estate de depuración o registro cronológico
<b>telnetd</b>	Tipo de emulación de terminal
<b>rlogind</b>	Estate de depuración
<b>fingerd</b>	Estate de depuración o registro cronológico
	Los subservidores <b>xwhod</b> y <b>timed</b> no proporcionan estado largo.
<b>traceson</b>	Activa la depuración de nivel de socket. Utilice el mandato <b>trpt</b> para formatear la salida. Los subsistemas <b>timed</b> e <b>iptraced</b> no soportan el mandato <b>traceson</b> .
<b>tracesoff</b>	Desactiva la depuración de nivel de socket. Utilice el mandato <b>trpt</b> para formatear la salida. Los subsistemas <b>timed</b> e <b>iptraced</b> no soportan el mandato <b>tracesoff</b> .

Para obtener ejemplos de cómo utilizar estos mandatos, consulte los temas sobre los mandatos individuales. Para obtener más información sobre el Controlador de recursos del sistema, consulte el apartado Controlador de recursos del sistema en la publicación *Sistema operativo y gestión de dispositivos*.

## Mandatos de transferencia de archivos

Aquí se listan descripciones breves de los mandatos de transferencia de archivos.

<b>Item</b>	<b>Descripción</b>
<b>ftp nombsistpral</b>	Transfiere archivos entre un sistema principal local y uno remoto.
<b>rcparchivo sistpral:archivo</b>	Transfiere archivos entre un sistema principal local y uno remoto, o entre dos sistemas principales remotos.

Item	Descripción
<b>tftp</b>	Transfiere archivos entre sistemas principales.

## Mandatos de inicio de sesión remoto

Aquí se listan descripciones breves de los mandatos de inicio de sesión remoto de **TCP/IP**.

Item	Descripción
<b>rexec</b> <i>mandato sistpral</i>	Ejecuta mandatos de uno en uno en un sistema principal remoto.
<b>rlogin</b> <i>sistpralremoto</i>	Conecta un sistema principal local con uno remoto.
<b>rsh</b> y <b>remsh</b> <i>mandato sistpralremoto</i>	Ejecuta el mandato especificado en el sistema principal remoto o inicia la sesión en el sistema principal remoto.
<b>telnet</b> , <b>tn</b> y <b>tn3270</b> <i>nombsistpral</i>	Conecta el sistema principal local con un sistema principal remoto, utilizando la interfaz <b>TELNET</b> .

## Mandatos de estado

Aquí se listan descripciones breves de los mandatos de estado de **TCP/IP**.

Item	Descripción
<b>finger</b> o <b>fusuario@sistpral</b>	Muestra información del usuario.
<b>host</b> <i>nombsistpra</i> <i>l</i>	Resuelve un nombre de sistema principal en una dirección de Internet o viceversa.
<b>ping</b> <i>nombsistpra</i> <i>l</i>	Envía una petición de eco a un sistema principal de red.
<b>xwho</b>	Muestra los usuarios que han iniciado una sesión en sistemas principales de la red local.
<b>whois</b> <i>nombre</i>	Identifica un usuario mediante su ID o alias.

## Mandato de comunicaciones remotas

El mandato de comunicaciones remotas de **TCP/IP**, **talk** *Usuario@SistPral*, le permite conversar con otro usuario.

Item	Descripción
<b>talk</b> <i>Usuario@SistPral</i>	Conversa con otro usuario.

## Mandatos de impresión

Aquí se listan descripciones breves de los mandatos de impresión de **TCP/IP**.

Item	Descripción
<b>enq</b> <i>archivo</i>	Pone un archivo en cola.
<b>refresh</b>	Solicita la renovación de un subsistema o grupo de subsistemas.
<b>smit</b>	Efectúa la gestión del sistema.

## Daemons TCP/IP

Un *subsistema* es un daemon, o servidor, controlado por el SRC. Un *subservidor* es un daemon controlado por un subsistema. (Los mandatos de daemon y los nombres de daemon se suelen indicar mediante una **d** al final del nombre).

Las categorías de subsistema y subservidor se excluyen mutuamente. Es decir, los daemons no se listan como subsistema y como subservidor. El único subsistema **TCP/IP** que controla otros daemons es el daemon **inetd**. Todos los subservidores **TCP/IP** también son subservidores **inetd**.

A continuación se proporcionan los daemons **TCP/IP** controlados por el SRC:

### Subsistemas

Item	Descripción
<b>gated</b>	Proporciona funciones de direccionamiento de pasarela y soporta los protocolos <b>RIP (Routing Information Protocol)</b> , <b>RIPng (Routing Information Protocol Next Generation)</b> , <b>EGP (Exterior Gateway Protocol)</b> , <b>BGP (Border Gateway Protocol)</b> y <b>BGP4+</b> , <b>HELLO (Defense Communications Network Local-Network Protocol)</b> , <b>OSPF (Open Shortest Path First)</b> , <b>IS-IS (Intermediate System to Intermediate System)</b> e <b>Internet Control Message Protocol (ICMP e ICMPv6)/Router Discovery Routing</b> . Además, el daemon <b>gated</b> soporta <b>Simple Network Management Protocol (SNMP)</b> . El daemon <b>gated</b> es uno de los dos daemons de direccionamiento disponibles para direccionar a direcciones de red y es el daemon de direccionamiento preferido. Se prefiere el daemon <b>gated</b> al daemon <b>routed</b> porque el daemon <b>gated</b> soporta más protocolos de pasarela.
<b>inetd</b>	Invoca y planifica otros daemons cuando se reciben peticiones de servicios de daemon. Este daemon también puede iniciar otros daemons. El daemon <b>inetd</b> también se conoce como el superdaemon.
<b>iptrace</b>	Proporciona la función de rastreo de paquetes a nivel de interfaz para protocolos de Internet.
<b>named</b>	Proporciona la función de denominación para el protocolo de <b>Servidor de nombres de dominio (DOMAIN)</b> .
<b>routed</b>	Gestionada las tablas de direccionamiento de red y soporta <b>RIP (Routing Information Protocol - Protocolo de información de direccionamiento)</b> . Se prefiere el daemon <b>gated</b> al daemon <b>routed</b> porque el daemon <b>gated</b> soporta más protocolos de pasarela.
<b>xwhod</b>	Envía difusiones a todos los demás sistemas principales cada tres minutos y almacena información sobre los usuarios conectados y el estado de red. Utilice el daemon <b>xwhod</b> con mucho cuidado, porque puede utilizar cantidades significativas de recursos de máquina.
<b>timed</b>	Proporciona la función de servidor horario.

**Nota:** Los daemons **routed** y **gated** se listan como subsistemas TCP/IP. No ejecute el mandato **startsrc -g tcPIP**, que inicia estos dos daemons de direccionamiento, junto con todos los demás subsistemas **TCP/IP**. La ejecución simultánea de ambos daemons en una máquina pueden producir resultados imprevisibles.

Los daemons TCP/IP controlados por el subsistema **inetd** son los siguientes:

### Subservidores **inetd**

Item	Descripción
<b>comsat</b>	Notifica a los usuarios que hay correo de entrada.
<b>fingerd</b>	Proporciona un informe de estado sobre todos los usuarios conectados y el estado de red en el sistema principal remoto especificado. Este daemon utiliza el protocolo <b>Finger</b> .
<b>ftpd</b>	Proporciona la función de transferencia de archivos para un proceso de cliente utilizando el <b>FTP (File Transfer Protocol - Protocolo de transferencia de archivos)</b> .

Item	Descripción
<b>rexecd</b>	Proporciona la función de servidor de sistema principal externo para el mandato <b>rexec</b> .
<b>rlogind</b>	Proporciona la función de recurso de inicio de sesión remoto para el mandato <b>rlogin</b> .
<b>rshd</b>	Proporciona la función de servidor de ejecución de mandatos remota para los mandatos <b>rcp</b> y <b>rsh</b> .
<b>talkd</b>	Proporciona la función de conversación para el mandato <b>talk</b> .
<b>syslogd</b>	Lee y registra los mensajes de sistema. Este daemon está en el grupo de subsistemas de <b>Servicio de acceso remoto</b> (RAS).
<b>telnetd</b>	Proporciona la función de servidor para el protocolo <b>TELNET</b> .
<b>tftpd</b>	Proporciona la función de servidor para <b>Trivial File Transfer Protocol (TFTP)</b> .
<b>uucpd</b>	Maneja las comunicaciones entre los BNU (Basic Network Utilities - Programas de utilidad básicos de red) y <b>TCP/IP</b> .

## Métodos de dispositivo

Los métodos de dispositivo son programas asociados con un dispositivo que realizan operaciones básicas de configuración de dispositivo.

Consulte [List of TCP/IP Programming References](#) en la publicación *Communications Programming Concepts* para obtener información sobre los métodos **TCP/IP**.

## Petición de comentarios

Se soportan las siguientes Peticiones de comentario (Request for Comments - RFC) de **TCP/IP** en el sistema AIX.

Para obtener una lista de las RFC (Petición de comentarios) soportadas por este sistema operativo, consulte [List of TCP/IP Programming References](#) en la publicación *Communications Programming Concepts*.

- RFC 1359 *Conexión a Internet: Qué deben anticipar las instituciones de conexión*
- RFC 1325 *FYI en preguntas y respuestas: Respuestas a preguntas frecuentes del 'nuevo usuario de Internet'*
- RFC 1244 *Manual de seguridad de sitio*
- RFC 1178 *Elección de un nombre para el sistema*
- RFC 1173 *Responsabilidades de los gestores de sistema principal y de red: Resumen de la 'tradición oral' de Internet*

## Programas de utilidad básicos de red (Basic Networking Utilities)

---

Los BNU son un grupo de programas, directorios y archivos que establecen comunicaciones entre sistemas que se encuentran en redes locales y remotas. Puede utilizarse para comunicarse con cualquier sistema UNIX en el que se ejecute una versión del UNIX-to-UNIX Copy Program (UUCP). BNU es uno de los programas de servicios ampliados que se pueden instalar con el sistema operativo base.

BNU contiene un grupo de mandatos relacionados con UUCP, un programa de comunicación UNIX-to-UNIX desarrollado por AT&T y modificado como parte de Berkeley Software Distribution (BSD). BNU facilita mandatos, procesos y una base de datos de soporte para las conexiones con sistemas remotos y locales. Las redes de comunicaciones como, por ejemplo, la red en anillo y Ethernet se utilizan para conectar sistemas de redes locales. La conexión de una red local con un sistema remoto puede realizarse a través de un módem de teléfono o de cable. Esto permite el intercambio de mandatos y archivos entre la red local y el sistema remoto.

Antes de que los usuarios del sistema puedan ejecutar los programas BNU, es necesario instalar y configurar BNU.

BNU está controlado por un conjunto de archivos de configuración que determinan si los sistemas remotos pueden iniciar la sesión en el sistema local y lo que pueden hacer una vez iniciada la sesión. Estos archivos de configuración deben configurarse con función de los requisitos y los recursos del sistema.

Para mantener BNU, es preciso leer y eliminar los archivos de anotaciones cronológicas de forma periódica y comprobar las colas de BNU para garantizar que los trabajos se transfieran correctamente a los sistemas remotos. También es necesario actualizar los archivos de configuración de forma periódica para que reflejen los cambios de su sistema o de los sistemas remotos.

## Cómo funciona BNU

BNU utiliza un conjunto de conexiones de hardware y programas de software para comunicarse entre los sistemas.

Una estructura de directorios y archivos realiza el seguimiento de las actividades de BNU. Esta estructura incluye un conjunto de directorios públicos, un grupo de directorios y archivos de administración, archivos de configuración y archivos de bloqueo. La mayoría de directorios para BNU se crean durante el proceso de instalación. Algunos de los directorios y archivos de administración los crean distintos programas de BNU.

A excepción de los mandatos de inicio de sesión remota, BNU funciona como un sistema por lotes. Cuando un usuario solicita el envío de un trabajo a un sistema remoto, BNU almacena la información necesaria para llevar a cabo el trabajo. Esto se conoce como la colocación en *cola* del trabajo. En el momento en que esté planificado o cuando el usuario así lo indique, BNU contacta con los distintos sistemas remotos, transfiere los trabajos de la cola y acepta los trabajos. Estas transferencias están controladas por los archivos de configuración de su sistema y del sistema remoto.

### Soporte a idiomas nacionales para los mandatos BNU

Todos los mandatos BNU, a excepción de **uucpadm**, están disponibles para el Soporte a idiomas nacionales.

No es necesario que el nombre de los usuarios esté en caracteres ASCII. Sin embargo, todos los nombres de los sistemas deben ir en caracteres ASCII. Si un usuario intenta planificar una transferencia o una ejecución de un mandato remoto que implica nombres de sistemas que no sean ASCII, BNU devolverá un mensaje de error.

## Estructura de archivos y directorios en BNU

BNU utiliza una estructura de directorios y archivos para llevar a cabo un seguimiento de las actividades.

Esta estructura incluye los directorios públicos, los archivos de configuración, los directorios de administración y los archivos de bloqueo.

La mayoría de directorios para BNU se crean durante el proceso de instalación. Algunos de los archivos y los directorios de administración los crean distintos programas de BNU a medida que van ejecutándose.

### Directorios públicos de BNU

Cuando se especifica, el directorio público de BNU (`/var/spool/uucppublic`) almacena los archivos que se han transferido al sistema local desde otros sistemas.

Los archivos esperan en el directorio público hasta que los usuarios los reclaman. El directorio público se crea cuando se instala BNU. En el directorio público, BNU crea un subdirectorio para cada sistema remoto que envía archivos al sistema local.

### Archivos de configuración de BNU

Los archivos de configuración de BNU, también conocidos como la base de datos de soporte de BNU, residen en el directorio `/etc/uucp`. Los archivos deben configurarse de forma específica para su sistema.

Los archivos son propiedad del ID de inicio de sesión de uucp y sólo pueden editarse con autorización root. Los archivos de configuración contienen información acerca de:

- Los sistemas remotos accesibles
- Los dispositivos para contactar con los sistemas remotos
- El momento en que debe contactarse con los sistemas remotos.
- Lo que los sistemas remotos tienen permiso para hacer en su sistema.

Algunos archivos de configuración también especifican límites en las actividades de BNU que evitan que el sistema se sobrecargue.

Entre los archivos de configuración de BNU se incluyen:

<b>Item</b>	<b>Descripción</b>
Devices	Contiene información sobre los dispositivos disponibles, incluidos los dos módems y las conexiones directas.
Dialcodes	Contiene abreviaturas sobre los códigos de marcación que permiten abbreviar los números de teléfono del archivo Systems.
Dialers	Especifica la sintaxis del mandato que realiza la llamada para un tipo de módem concreto ("dialer").
Maxuuscheds	Limita los trabajos simultáneos que pueden planificarse.
Maxuuxqts	Limita las ejecuciones simultáneas de mandatos remotos.
Permissions	Contiene los códigos de permiso de acceso. Este archivo es el archivo principal para determinar la seguridad de BNU.
Poll	Especifica el momento en que el programa BNU debe realizar un sondeo de los sistemas remotos para iniciar las tareas.
Sysfiles	Lista los archivos que sirven como los archivos Systems, Devices y Dialers para la configuración de BNU. Si este archivo no se utiliza, los archivos por omisión son /etc/uucp/Systems, /etc/uucp/Devices y /etc/uucp/Dialers.
Systems	Lista los sistemas remotos accesibles y la información necesaria para contactar con ellos, incluido el dispositivo que debe utilizarse y las combinaciones de nombre de usuario y contraseña necesarias para iniciar la sesión. También especifica el momento en que es posible contactar con los sistemas.

Los archivos de configuración se consultan entre sí cuando se utiliza BNU. Por ejemplo:

- El archivo Devices contiene un campo *Señal* que hace referencia a las entradas del archivo Dialers.
- El archivo Systems contiene una entrada para una *Clase* de dispositivo. En el archivo Devices debe haber definido un dispositivo de cada una de las *Clases* a las que se haga referencia en el archivo Systems.
- El archivo Poll contiene entradas para los sistemas a los que llama su sistema. Cada uno de estos sistemas debe estar definido en el archivo Systems.

Las entradas de los archivos de configuración de BNU dependen de los tipos de conexiones entre el sistema y cada sistema remoto. Por ejemplo, deben realizarse entradas especiales si se utiliza TCP/IP (Transmission Control Protocol/Internet Protocol) o las conexiones directas para contactar con otros sistemas. Si se utilizan módems para contactar con otros sistemas, los módems deben definirse en el archivo Dialers.

Los archivos Systems, Devices y Permissions deben estar configurados en el sistema antes de poder contactar con los sistemas remotos mediante BNU. Otros archivos de configuración permiten utilizar funciones adicionales de BNU como, por ejemplo, el sondeo automático. Muchos de los archivos de configuración deben modificarse periódicamente para reflejar los cambios de su sistema o de los sistemas con los que se contacte. El archivo Sysfiles puede utilizarse para especificar archivos distintos de Systems, Devices y Dialers que cumplan las mismas funciones.

## **Directarios y archivos de administración de BNU**

Los directarios y archivos de administración de BNU se encuentran en subdirectorios del directorio /var/spool/uucp.

Estos directarios y archivos contienen dos tipos de información:

- Datos a la espera de ser transferidos a otros sistemas
- Información de errores y anotaciones cronológicas acerca de las actividades de BNU.

Bajo el directorio /var/spool/uucp, BNU crea los directarios siguientes:

<b>Item</b>	<b>Descripción</b>
.Admin	Contiene cuatro archivos de administración: <ul style="list-style-type: none"><li>• audit</li><li>• Foreign</li><li>• errors</li><li>• xferstats</li></ul> Estos archivos contienen información de errores y anotaciones cronológicas acerca de las actividades de BNU.
.Corrupt	Contiene copias de los archivos que el programa BNU no puede procesar.
.Log y .Old	Contiene archivos de anotaciones cronológicas de transacciones de BNU.
.Status	Almacena la última vez que el daemon <b>uucico</b> ha intentado ponerse en contacto con los sistemas remotos.
.Workspace	Conserva archivos temporales que los programas de transporte de archivos utilizan internamente.
.Xqtdir	Contiene archivos de ejecución con listas de mandatos que los sistemas remotos pueden ejecutar.
<i>NombreSistema</i>	Contiene los archivos que los programas de transporte de archivos utilizan. Estos archivos son los siguientes: <ul style="list-style-type: none"><li>• De mandatos (<b>C.*</b>)</li><li>• De datos (<b>D.*</b>)</li><li>• De ejecución (<b>X.*</b>)</li><li>• Temporales (<b>TM.*</b>)</li></ul> BNU crea un directorio <i>NombreSistema</i> para cada sistema remoto con el que conecta.

Los directarios cuyos nombres empiezan por un punto son *ocultos*. No pueden encontrarse con el mandato **ls** o **li** a menos que se utilice el distintivo **-a**. Cuando se inicia el daemon **uucico**, éste busca si hay archivos de trabajo en el directorio /var/spool/uucp y transfiere los archivos desde cualquier directorio que no esté oculto. El daemon **uucico** sólo ve los directarios *NombreSistema*, no los otros directarios de administración.

Los archivos de los directarios ocultos son propiedad del ID de inicio de sesión uucp. A estos archivos sólo puede accederse con autorización root o con un ID de inicio de sesión que tenga el UID 5.

Para obtener más información sobre cómo mantener los directarios de administración de BNU, consulte el apartado “Mantenimiento de BNU” en la página 530.

## **Archivos de bloqueo de BNU**

Los archivos de bloqueo de BNU se almacenan en el directorio /var/locks. Cuando BNU utiliza un dispositivo para conectar con un sistema remoto, coloca un archivo de bloqueo sobre este dispositivo en el directorio /var/locks.

Cuando otro programa BNU o cualquier otro programa necesita el dispositivo, este programa comprueba si hay algún archivo de bloqueo en el directorio /var/locks. Si existe un archivo de bloqueo, el programa espera hasta que el dispositivo esté disponible o utiliza otro dispositivo para la comunicación.

Además, el daemon **uucico** coloca archivos de bloqueo sobre los sistemas remotos en el directorio /var/locks. Antes de contactar con un sistema remoto, el daemon **uucico** comprueba si existe algún archivo de bloqueo para dicho sistema en el directorio /var/locks. Estos archivos impiden que otras instancias del daemon **uucico** establezcan conexiones duplicadas con el mismo sistema remoto.

**Nota:** Además de BNU, software como, por ejemplo, Asynchronous Terminal Emulation (ATE) y TCP/IP también utiliza el directorio /var/locks.

## Configuración de BNU

Este procedimiento explica cómo configurar los BNU (Basic Network Utilities) para distintos tipos de conexiones, como las conexiones directas, de módem y de Protocolo de control de transmisiones/Protocolo Internet (Transmission Control Protocol/Internet Protocol) (TCP/IP).

### Prerrequisitos

- BNU debe estar instalado en el sistema.
- Debe tener autorización de usuario root para editar los archivos de configuración de BNU.
- Si utiliza conexiones directas para las comunicaciones BNU, se deben configurar las conexiones correctas entre el sistema y los sistemas remotos.
- Si utiliza módems para las comunicaciones BNU, debe instalar y configurar cada módem.
- Si una o más de las conexiones utiliza TCP/IP, TCP/IP debe estar en ejecución entre el sistema y los sistemas remotos adecuados.
- Recopile la información que necesite para configurar BNU (consulte la lista siguiente). Esta información incluye una lista de los sistemas remotos y listas de los dispositivos y módems a utilizar para conectar con los sistemas.

### Recopilación de la información de sistema necesaria

Antes de configurar BNU, recopile la información siguiente:

- Para cada *sistema remoto* que llame el sistema, recopile la información siguiente:
  - Nombre del sistema
  - El nombre de inicio de sesión que utiliza el sistema en el sistema remoto
  - La contraseña para el nombre de inicio de sesión.
  - Solicitudes de inicio de sesión y contraseña en el sistema remoto.
  - El tipo de conexión que utiliza para ponerse en contacto con el sistema remoto (directo, módem, o TCP/IP)

Si la conexión es directa, recopile la información siguiente:

- La velocidad en bits de la conexión
- El puerto del sistema local con el que está conectada la conexión.

Si la conexión es por medio de un módem (conexión telefónica), recopile la información siguiente:

- El número de teléfono del sistema remoto.
- La velocidad del módem que sea compatible con la velocidad del sistema remoto.

**Nota:** Si alguno de los sistemas remotos llama al sistema, asegúrese de que el administrador de BNU de cada uno de los sistemas remotos tenga toda la información anterior acerca del sistema.

- Para cada *módem local* que utilice para las conexiones BNU, recopile la información siguiente:
  - El script de chat del módem (consulte la documentación del módem).

**Nota:** Para algunos módems, el script de chat está disponible en el archivo /etc/uucp/Dialers.

- El puerto local del módem.

### Creación de una lista de dispositivos de sistema

Utilice la información que ha recopilado para realizar una lista de cada dispositivo del sistema que necesita para conectarse a un sistema remoto. A continuación se muestra una lista de ejemplo para el sistema local morgan:

```
direct:  
hera 9600 tty5  
zeus& 2400 tty2  
ariadne 2400 tty1  
hayes modem (tty3): apollo, athena  
TCP/IP: merlin, arthur, percy
```

En el ejemplo anterior, es posible conectarse al sistema hera, y se utiliza una conexión direct a una velocidad de 9600 desde el puerto tty5. Para conectarse al sistema apollo, se utiliza el módem hayes, que está conectado al puerto tty3. Se utiliza TCP/IP para conectarse a sistemas merlin, arthur y percy.

### Configuración de los recursos de comunicación remotos

Para que BNU funcione correctamente en su sitio, debe configurar los recursos de comunicación remotos tal como se indica a continuación:

- Listar los dispositivos que se utilizan para establecer un enlace de comunicaciones directo, telefónico o de módem.
- Listar los módems que se utilizan para ponerse en contacto con los sistemas remotos a través de la red telefónica.
- Listar los sistemas remotos accesibles.
- Listar las abreviaturas representando los prefijos de los números de teléfono que se utilizan para ponerse en contacto con los sistemas remotos especificados (opcional).
- Establecer los permisos de acceso que especifican las formas en las que se pueden comunicar los sistemas locales y remotos.
- Programar la supervisión de los sistemas remotos de la red (opcional).

Para crear estas listas, permisos y planificaciones, lleve a cabo los pasos siguientes:

- Cambie los archivos de configuración de BNU.
- Edite el archivo /var/spool/cron/crontabs/uucp para eliminar los caracteres de comentario (#) del principio de las líneas que planifican las rutinas de mantenimiento automático.

**Nota:** Debe configurar los archivos Sistemas, Dispositivos y Permisos para asegurarse de que BNU se ejecuta correctamente en su sitio. Sin embargo, no es necesario cambiar los archivos de configuración de BNU en ningún orden concreto.

Una vez que lleve a cabo los procedimientos anteriores, puede configurar BNU en el sistema.

### Configuración de BNU en el sistema

Para configurar BNU, lleve a cabo los pasos siguientes:

1. Asegúrese de que BNU esté instalado en el sistema ejecutando el mandato siguiente:

```
lslpp -h bos.net.uucp
```

Si BNU está instalado, bos.net.uucp se muestra en la salida. Si no lo ve, instale BNU desde la cinta de instalación.

2. Establezca los ID y las contraseñas de inicio de sesión adecuados para los sistemas remotos que llamen al sistema y proporcione a la persona responsable de la administración de BNU o del UUCP (UNIX-to-UNIX Copy Program) en cada sistema remoto la contraseña y el inicio de sesión.

Este paso se completará editando los archivos /etc/passwd, /etc/group, /etc/security/login.cfg y /etc/security/passwd.



**Atención:** Si permite que los sistemas remotos inicien la sesión en el sistema local con el ID de inicio de sesión de UUCP, la seguridad del sistema estará en riesgo. Los sistemas remotos que inicien la sesión con el ID de UUCP pueden visualizar y posiblemente modificar los archivos Systems y Permissions locales. Estas acciones del sistema remoto dependen de los permisos que se especifican en la entrada LOGNAME del archivo Permissions. Se recomienda que cree otros ID de inicio de sesión de BNU para los sistemas remotos y que reserve el ID de inicio de sesión de UUCP para el BNU de administración de la persona en el sistema local. Para una mejor seguridad, cada sistema remoto que contacte con el sistema local debe tener un ID de inicio de sesión exclusivo con un número de ID de usuario exclusivo (UID). Estos ID de inicio de sesión deben tener los ID de grupo (GID) de 5. De forma predeterminada, el sistema operativo incluye el ID de inicio de sesión de NUUUCP para transferir los archivos.

- a) Si necesita mantener un control completo del acceso de cada sistema individual, debe crear ID de inicio de sesión independientes y combinar las entradas MACHINE y LOGNAME en el archivo Permissions. Tiene la opción de mantener inicios de sesión independientes, o de tener un solo inicio de sesión para todas las conexiones BNU. A continuación se muestran algunas entradas de ejemplo de /etc/passwd:

```
Umicrtk!:!105:5:micrtk uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico  
Ufloyd1!:!106:5:floyd1 uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico  
Uicus!:!107:5:icus uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico  
Uriscakr!:!108:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
```

- b) Si desea tener un conjunto de permisos y no desea mantener un control independiente de ninguna de las conexiones UUCP, puede tener un solo inicio de sesión para todos los sistemas. Una entrada de ejemplo para tal caso de ejemplo es el siguiente:

```
nuucp!:!6:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
```

**Nota:**

- El UID, que es el tercer campo separado por dos puntos, debe ser exclusivo para evitar cualquier riesgo de seguridad.
- El GID, que es el cuarto campo separado por dos puntos, debe ser 5 para asegurarse de que está en el mismo grupo que UUCP.
- El directorio de inicio, que es el sexto campo separado por dos puntos, se puede cambiar a cualquier directorio válido.
- El shell de inicio de sesión, que es el séptimo campo separado por dos puntos, siempre debe ser /usr/sbin/uucp/uucico.

- c) Asegúrese de que el archivo /etc/group contenga los usuarios nuevos. Un ejemplo de tal entrada se indica a continuación:

```
uucp!:5:uucp,uucpadm,nuucp,Umicrtk,Uicus,Urisctakr
```

- d) Añadir cualquier usuario con el grupo UUCP, que utilizan módems para conectarse con programas distintos del mandato **cu**.
- e) Tras editar estos archivos como root, establezca una contraseña para los usuarios nuevos con el mandato **passwd UserName**.

**Nota:** Si cambia una contraseña del inicio de sesión raíz, la entrada de los distintivos de la stanza para el usuario en el archivo /etc/security/passwd contendrá la línea siguiente:

```
flags = ADMCHG
```

Debe cambiar la línea anterior, tal como se muestra en el ejemplo siguiente:

```
flags =
```

De lo contrario, cuando el proceso remoto **uucico** inicie la sesión en el sistema, el sistema le solicitará que especifique una nueva contraseña. Esta acción no es posible y, por lo tanto, el inicio de sesión fallará.

- f) Para evitar interrupciones en el proceso de inicio de sesión que están causadas por el proceso **uucico**, que se puede iniciar por el indicador predeterminado con todos los Ctrl-J, comente la stanza predeterminada (con asteriscos) y defina una stanza para el tty, tal como se muestra en el ejemplo siguiente:

```
/dev/tty0:  
    herald = "\nrisc001 login:"
```

- g) Utilice un editor de textos ASCII o el mandato **uucpadmin** para editar el archivo Poll1. Añada una entrada para cada sistema que sondea el sistema.

**Nota:** Los sistemas que aparecen en el archivo Poll1 también deben aparecer en el archivo /etc/uucp/Systems.

- h) Utilice un editor de texto ASCII para editar el archivo /var/spool/cron/crontabs/uucp. Elimine los caracteres de comentario (#) de las líneas que ejecutan los mandatos **uudemon.hour** y **uudemon.poll**.

Puede cambiar el número de veces que se ejecutan estos mandatos. Sin embargo, asegúrese de planificar el mandato **uudemon.poll** aproximadamente 5 minutos antes de planificar el mandato **uudemon.hour**.

- i) Asegúrese de que los cambios hayan entrado en vigor ejecutando el mandato siguiente:

```
crontab -l uucp
```

- j) Configure los siguientes archivos de datos BNU: Systems, Permissions, Devices, Dialers y Sysfiles.

Puede utilizar el mandato /usr/sbin/uucp/uucpadmin para configurar inicialmente los archivos y, a continuación, editarlos para que se adapten a sus necesidades. Utilice el archivo Sysfiles para especificar otros archivos además de /etc/uucp/Systems, /etc/uucp/Devices y /etc/uucp/Dialers para la configuración de BNU. Para obtener más información, consulte el apartado Sysfiles.

3. Si decide utilizar las abreviaturas de los códigos de marcación para los números de teléfono en los archivos Systems, configure la entrada Dialcodes para cada abreviatura. Para obtener detalles, consulte el apartado Dialcodes File Format for BNU.

Si utiliza TCP/IP para las conexiones BNU, utilice el mandato **netstat** para ver si el daemon **uucpd** funciona, especificando el mandato siguiente:

```
netstat -a
```

El daemon **inetd** inicia el daemon **uucpd**. Si el daemon **uucpd** no se ejecuta, vuelva a configurar el daemon **inetd** para iniciar el daemon **uucpd**. Para obtener más información, consulte: “Configuración del daemon inetd” en la página 431).

4. Utilice la lista de dispositivos que ha recopilado, antes de empezar este procedimiento, para cambiar el archivo Devices en el sistema. Cree una entrada para cada módem y cada conexión directa. Si utiliza TCP/IP, elimine el comentario de la entrada de TCP/IP en el archivo Devices.

Puede configurar el archivo /etc/uucp/Sysfiles para especificar otros archivos que se deben utilizar para la configuración de dispositivos. Para obtener detalles sobre el archivo Devices, consulte el apartado Devices File Format for BNU.

Además, si utiliza TCP/IP, verifique que el archivo /etc/services incluye la línea siguiente:

```
uucp      540/tcp      uucpd
```

Si no, añada esta línea al archivo.

5. Utilice la información sobre cada sistema remoto que ha recopilado, antes de empezar este procedimiento, para cambiar el archivo Systems en el sistema. Utilice los ejemplos comentados del archivo Systems como guía al especificar la configuración. Si utiliza TCP/IP, asegúrese de que la tabla de nombre de host del archivo /etc/hosts incluya el nombre del sistema remoto con el que desea conectarse. Puede configurar el archivo /etc/uucp/Sysfiles para especificar otros archivos que se deben utilizar para la configuración de sistemas.
6. Utilice la información sobre los dispositivos y módems que ha recopilado, antes de empezar este procedimiento, para asegurarse de que el archivo Dialers del sistema contiene una entrada para cada módem. Si utiliza TCP/IP y conexiones directas, asegúrese de que la entrada TCP/IP y las entradas directas estén presentes en el archivo. Puede configurar el archivo /etc/uucp/Sysfiles para especificar otros archivos que se deben utilizar para la configuración de los dialers.
7. Decida cuánto acceso al sistema desea proporcionar a cada sistema remoto al que llame y para cada sistema remoto que lo llame. Configure las entradas adecuadas para cada sistema y cada nombre de inicio de sesión en el archivo Permissions.
8. Utilice el mandato **uuchek** para verificar que los directorios, los programas y los archivos de soporte estén configurados correctamente:

```
/usr/sbin/uucp/uuchek -v
```

El mandato **uuchek** verifica que los directorios, los programas y los archivos de soporte estén configurados correctamente y que las entradas del archivo Permissions sean coherentes. Si el mandato **uuchek** indica algún error, arréglelo.

9. Opcional: Configure la supervisión automática de las operaciones de BNU y el sondeo automático de los sistemas remotos. Para obtener más información, consulte el apartado “Configuración de la supervisión automática en BNU” en la página 521 y “Configuración del sondeo de sistemas remotos en BNU” en la página 521).

### **Configuración de la supervisión automática en BNU**

BNU utiliza el daemon **cron** para iniciar los daemons de BNU y supervisar la actividad de BNU.

#### **Prerrequisitos**

- Realice los pasos que se indican en el apartado “Configuración de BNU” en la página 517.
- Debe tener autorización de usuario root para editar el archivo /var/spool/cron/crontabs/uucp.

El daemon **cron** lee el archivo /var/spool/cron/crontabs/uucp en busca de instrucciones sobre el momento de iniciar los procedimientos de BNU.

Para configurar la supervisión automática de BNU, lleve a cabo los pasos siguientes:

1. Inicie la sesión como usuario con autorización de usuario root.
2. Utilice un editor de texto ASCII para editar el archivo /var/spool/cron/crontabs/uucp.
3. Descomente las líneas de los procedimientos de mantenimiento de BNU, uudemon.admin y uudemon.cleanup.

Puede cambiar los momentos en que se ejecutan estos procedimientos si el sistema necesita mantenimiento a intervalos con una frecuencia superior o inferior. Sin embargo, es mejor ejecutar el mandato uudemon.admin por lo menos una vez al día y el mandato uudemon.cleanup por lo menos una vez a la semana.

4. Utilice el archivo crontabs/uucp para planificar otros mandatos de mantenimiento de BNU, por ejemplo, los mandatos **uulog**, **uuclean** o **uucleanup**.

Además, puede utilizar el archivo crontabs/uucp para indicar al daemon **cron** que debe iniciar los daemons **uucico**, **uuxqt** o **uusched** en momentos determinados.

### **Configuración del sondeo de sistemas remotos en BNU**

Para que BNU realice un sondeo de los trabajos en los sistemas remotos, los sistemas deben aparecer en el archivo /etc/uucp/Poll.

#### **Prerrequisitos**

- Siga los pasos que se listan en “Configuración de BNU” en la página 517.
- Debe tener autorización root para editar el archivo /var/spool/cron/crontabs/uucp y el archivo /etc/uucp/Poll.

Además de realizar un listado de los sistemas en el archivo /etc/uucp/Poll, ejecute los mandatos **uudemon.hour** y **uudemon.poll** de forma periódica.

Para establecer un sondeo de BNU de sistemas remotos, lleve a cabo los pasos siguientes:

1. Decida en qué sistemas remotos se realizará un sondeo de forma automática. Decide la frecuencia con la que desea realizar el sondeo de cada sistema. Especifique las horas de cada sistema con el archivo Poll, que puede ser tan poco frecuente como una vez al día o tan frecuente como desee.
2. Inicie la sesión como usuario con autorización root.
3. Utilizando un editor de textos ASCII o el mandato **uucpadmin**, edite el archivo Poll. Añada una entrada para cada sistema que el sistema esté configurado para sondear.

**Nota:** Los sistemas que aparecen en el archivo Poll también deben aparecer en el archivo /etc/uucp/Systems.

4. Utilizando un editor de textos ASCII, edite el archivo /var/spool/cron/crontabs/uucp. Elimine los caracteres de comentario (#) de las líneas que ejecutan los mandatos **uudemon.hour** y **uudemon.poll**.

Puede cambiar el momento en que se ejecutarán estos mandatos. Sin embargo, asegúrese de planificar el mandato **uudemon.poll** aproximadamente 5 minutos antes de planificar el mandato **uudemon.hour**.

BNU se ha establecido para sondear automáticamente los sistemas que están listados en el archivo Poll en el momento que ha especificado.

### Archivo /etc/uucp/Systems

Los sistemas remotos se muestran en los archivos /etc/uucp/Systems.

El archivo /etc/uucp/Systems es el archivo Systems por omisión. El administrador del sistema puede especificar archivos adicionales en el archivo **/etc/uucp/Sysfiles**.

Cada entrada de un archivo Systems contiene los elementos siguientes:

- El nombre del sistema remoto
- Las horas en las que los usuarios se pueden conectar al sistema remoto
- El tipo de enlace (línea directa o módem)
- La velocidad de transmisión a través del enlace
- La información que es necesaria para iniciar sesión en el sistema remoto

Cada entrada de un archivo Systems representa un sistema remoto. Para establecer las comunicaciones, el sistema remoto debe listarse en el archivo Systems local. Debe existir un archivo Systems en cada sistema que utilice el recurso BNU. Normalmente, sólo el usuario root puede leer los archivos Systems. Cualquier usuario, sin embargo, puede listar los nombres de los sistemas BNU remotos, utilizando el mandato **uname**.

### Edición de los archivos Devices para una conexión directa

Para editar el archivo Devices para una conexión directa, debe tener autorización root para editar el archivo /etc/uucp/Devices u otro archivo especificado en el archivo /etc/uucp/Sysfiles como un archivo Devices.

Para configurar una conexión directa que especifica un puerto y un sistema remoto, haga una entrada como la siguiente:

1. Escriba el nombre del sistema remoto al que desee conectar el sistema local a través de la línea directa en el campo **Tipo** en la segunda línea de la entrada.
2. Escriba el nombre de dispositivo adecuado para la conexión directa que se utiliza en su sitio en el campo **Línea** en ambas líneas de la entrada.

3. Escriba un guión (-) para un marcador del campo **Line2** en ambas líneas de la entrada.
4. Escriba la velocidad de transmisión adecuada para la conexión directa que se utiliza en su sitio en el campo **Velocidad** en ambas líneas de la entrada.
5. Escriba **direct** (todo en minúsculas) en el campo **Pares dialer-señal** en ambas líneas de la entrada.

Por ejemplo:

```
type device - speed direct
```

Continúe añadiendo entradas al archivo Devices hasta que haya listado cada dispositivo que conecta el sistema local directamente a un sistema remoto.

Para configurar una conexión directa entre dos sistemas que utilizan una conexión en serie asíncrona permanente, haga una entrada de una línea como la siguiente:

1. Especifique el nombre del sistema remoto en el campo **Tipo**.
2. Especifique el nombre del dispositivo tty en el campo **Línea**.
3. Especifique un guión (-) para un marcador en el campo **Line2**.
4. Escriba la velocidad de transmisión adecuada para la conexión directa que se utiliza en su sitio en el campo **Clase**.
5. Especifique **direct** (todo en minúsculas) en el campo **Pares dialer-señal**.

Por ejemplo:

```
type device - speed direct
```

Continúe añadiendo entradas al archivo Devices hasta que haya listado cada uno de los dispositivos directos que conectan el sistema local a un sistema remoto.

### **Edición del archivo de dispositivos para una conexión de marcador automático**

Siga estos pasos al editar el archivo /etc/uucp/Devices.

Debe tener autorización root para editar el archivo /etc/uucp/Devices u otro archivo especificado en el archivo /etc/uucp/Sysfiles como un archivo Dispositivos.

En las entradas de conexiones telefónicas, el campo **Tipo** se especifica como una unidad de llamada automática (ACU). Especifique ACU como la entrada de campo **Tipo** en todas las conexiones remotas establecidas a través de una línea telefónica. Para configurar las entradas del archivo Devices para las conexiones mediante autodialers, cree una entrada de una línea para cada módem:

1. En el campo **Tipo**, especifique ACU.
2. En el campo **Línea**, especifique el nombre de dispositivo que está conectado al módem.
3. En el campo **Línea2**, especifique un guión (-) como marcador de posición, a menos que el marcador automático sea un marcador estándar 801. Si el autodialer es un dialer 801 estándar, escriba 801.
4. En el campo **Velocidad**, escriba la velocidad en baudios adecuada al módem y a la línea, o la clase del módem (por ejemplo, D2400). El valor de la velocidad en baudios puede ser 300, 1200, 2400 o superior, en función del módem.

**Nota:** Si el módem puede utilizarse a más de una velocidad en baudios especificada, cree una entrada distinta en el archivo Dispositivos para cada velocidad. Si el módem puede utilizarse en cualquier velocidad en baudios, escriba la palabra Any en el campo **Velocidad**.

5. Escriba el nombre del módem como la entrada del campo **Dialer** en el campo **Par Dialer-Señal**.

Si piensa incluir números de teléfono completos en el archivo /etc/uucp/Systems o en otro archivo Systems, que se especifica en el archivo /etc/uucp/Sysfiles, deje el campo **Señal** en blanco. Un espacio en blanco indica al programa BNU que utilice la señal \D predeterminada. Si piensa utilizar las abreviaturas del código de marcación especificadas en el archivo /etc/uucp/Dialcodes, especifique la señal \T.

Por ejemplo:

```
type line - speed dialer - token pair
```

Continúe añadiendo entradas al archivo Devices hasta que haya listado cada una de las conexiones entre el sistema local y un sistema remoto que utilice una línea telefónica y un módem.

### **Edición del archivo Devices para TCP/IP**

Siga estos pasos al editar el archivo /etc/uucp/Devices.

Debe tener autorización root para editar el archivo /etc/uucp/Devices, u otro archivo especificado en el archivo /etc/uucp/Sysfiles como un archivo Devices.

Si el sitio utiliza TCP/IP para conectarse a los sistemas, incluya la entrada TCP/IP relevante en el archivo Devices. Para configurar el archivo para su uso con el TCP/IP, especifique la línea siguiente en el archivo Devices:

```
TCP - - - TCP
```

### **Ejemplos: Configuración de BNU para una conexión TCP/IP**

Este grupo de ejemplos configura BNU para una conexión TCP/IP.

Los archivos siguientes están configurados para una conexión TCP/IP entre sistemas zeus y hera, donde zeus es el sistema local y hera es el sistema remoto.

#### ***Archivos BNU para entradas de una conexión TCP/IP en los archivos del sistema local***

Estos archivos BNU son entradas en el sistema local zeus.

- **Archivo Systems:** El archivo Systems del sistema zeus contiene la siguiente entrada para que zeus se pueda poner en contacto con el sistema hera:

```
hera Any TCP,t - - in:--in: uzeus word: cumpleaños
```

Este ejemplo especifica que el sistema zeus puede llamar al sistema hera en cualquier momento, utilizando el protocolo **t** para las comunicaciones con el sistema hera. El sistema zeus inicia la sesión en el sistema hera como uzeus con la contraseña cumpleaños.

**Nota:** El protocolo **t** da soporte a **TCP**. Por lo tanto, siempre deberá utilizar el protocolo **t** para las comunicaciones BNU a través de conexiones TCP/IP. Sin embargo, el protocolo **t** no se puede utilizar cuando se utiliza el campo **Tipo** ACU (unidad de llamada automática) o cuando se utiliza una conexión de módem.

BNU utiliza los campos **Tipo** y **Clase** del archivo Systems para hallar la conexión. Comprueba el archivo Devices en busca de una entrada de tipo TCP.

- **Archivo Devices:** El archivo Devices que utiliza el daemon **uucico** en el sistema zeus contiene la entrada siguiente para las conexiones TCP/IP:

```
TCP - - - TCP
```

Como el tipo de dispositivo es TCP, no existe ninguna entrada **Clase**, **Línea** ni **Línea2**. El **Dialer** también se especifica como TCP. BNU busca en los archivos Dialers una entrada TCP.

- **Archivo Dialers:** El archivo Dialers que utiliza el daemon **uucico** en el sistema zeus contiene una entrada TCP/IP como la siguiente:

```
TCP
```

Esta entrada especifica que no es necesario configurar el dialer.

**Nota:** Nunca es necesario configurar el dialer a través de una conexión TCP/IP.

- **Archivo Permissions:** El archivo Permissions del sistema zeus contiene la entrada siguiente, que otorga al sistema hera acceso al sistema zeus:

```
LOGNAME=uhera SENDFILES=yes REQUEST=yes \
MACHINE=zeus:hera VALIDATE=uhera \
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera COMMANDS=ALL
```

Las entradas combinadas LOGNAME y MACHINE proporcionan los permisos siguientes al sistema hera, cuando el sistema zeus y el sistema hera están conectados:

- El sistema hera puede solicitar y enviar archivos con independencia de quién haya iniciado la llamada.
- El sistema hera puede leer y grabar en el directorio público y en el directorio /home/hera en el sistema zeus.
- El sistema hera puede ejecutar todos los mandatos en el sistema zeus.
- El sistema hera debe iniciar la sesión en el sistema zeus como usuario uhera, y el sistema hera no puede utilizar ningún otro ID de inicio de sesión para las transacciones de BNU.

**Nota:** Como los permisos son los mismos con independencia de qué sistema inicie la llamada, las entradas LOGNAME y MACHINE anteriores se combinan. Si los permisos no son los mismos para el sistema hera y el sistema zeus, las entradas LOGNAME y MACHINE serán las siguientes:

```
LOGNAME=uhera VALIDATE=hera SENDFILES=yes REQUEST=yes \
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera

MACHINE=zeus:hera REQUEST=yes COMMANDS=ALL\
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera
```

#### **Archivos BNU para entradas de una conexión TCP/IP en los archivos del sistema remoto**

Estos archivos se encuentran en el sistema remoto hera.

- **Archivo Systems:** Un archivo Systems en el sistema hera contiene la entrada siguiente para permitir a hera ponerse en contacto con el sistema zeus:

```
zeus Any TCP,t - - ogin:--login: uhera ord: relámpago
```

Este ejemplo especifica que el sistema hera puede llamar al sistema zeus en cualquier momento, utilizando el protocolo t para las comunicaciones con el sistema zeus. El sistema hera inicia la sesión en el sistema zeus como el usuario uhera con la contraseña relámpago. BNU comprueba a continuación si en los archivos Devices existe alguna entrada de tipo TCP.

**Nota:** El protocolo t da soporte a **TCP**. Por lo tanto, siempre deberá utilizar el protocolo t para las comunicaciones BNU a través de conexiones TCP/IP. Sin embargo, el protocolo t no puede utilizarse cuando el campo *Tipo* es ACU o si se está utilizando una conexión por módem.

- **Archivo Devices:** El archivo Devices que se utiliza mediante el daemon **uucico** en el sistema hera contiene la entrada siguiente para las conexiones TCP/IP:

```
TCP - - - TCP
```

Como el tipo de dispositivo es TCP, no existe ninguna entrada *Tipo*, *Línea* o *Línea2*. El *Dialer* también se especifica como TCP. BNU busca en los archivos Dialers una entrada TCP.

- **Archivo Dialers:** El archivo Dialers que utiliza el daemon **uucico** en el sistema hera contiene una entrada TCP/IP como la siguiente:

```
TCP
```

Esta entrada especifica que no es necesario configurar el dialer.

**Nota:** Nunca es necesario configurar el dialer a través de una conexión TCP/IP.

- **Archivo Permissions:** El archivo Permissions en el sistema hera contiene la entrada siguiente, que otorga al sistema zeus acceso al sistema hera:

```
LOGNAME=uzeus SENDFILES=yes REQUEST=yes \
MACHINE=hera:zeus VALIDATE=zeus COMMANDS=rmail:who:uucp
```

Las entradas combinadas LOGNAME y MACHINE proporcionan los permisos siguientes al sistema zeus, cuando el sistema zeus y el sistema hera están conectados:

- El sistema zeus puede solicitar y enviar archivos con independencia de quién haya iniciado la llamada.
- El sistema zeus puede leer y grabar sólo en el directorio público (el valor predeterminado).
- El sistema zeus sólo puede ejecutar los mandatos **rmail**, **who** y **uucp**.
- El sistema zeus debe iniciar la sesión en el sistema hera como usuario uzeus y el sistema zeus no puede utilizar ningún otro ID de inicio de sesión para las transacciones de BNU.

**Nota:** Si los permisos no son los mismos para el sistema hera y el sistema zeus, las entradas LOGNAME y MACHINE serán las siguientes:

```
LOGNAME=uzeus VALIDATE=zeus SENDFILES=yes REQUEST=yes
MACHINE=hera:zeus COMMANDS=rmail:who:uucp REQUEST=yes
```

### Ejemplos: Configuración de BNU para una conexión telefónica

Los archivos de ejemplo se han configurado para conectar los sistemas venus y merlin a través de una línea telefónica utilizando módems.

El sistema venus es el sistema local, y el sistema merlin es el sistema remoto.

En ambos sistemas, el dispositivo **tty1** está conectado a un módem Hayes a 1200 baudios. El ID de inicio de sesión utilizado para el sistema venus para iniciar sesión en el sistema merlin es **uvenus**, y la contraseña asociada es **mirror**. El ID de inicio de sesión para el sistema merlin para iniciar la sesión en el sistema venus es **umerlin**, y la contraseña asociada es **oaktree**. El número de teléfono del módem que está conectado a venus es **9=3251436**; el número del módem merlin es **9=4458784**. Ambos sistemas incluyen números de teléfonos parciales en los archivos **Systems** e incluyen códigos de marcación en los archivos **Dialcodes**.

Los siguientes archivos de ejemplo están configurados para conectar los sistemas venus y merlin:

- **Archivo Systems:** El archivo **Systems** en el sistema venus contiene la entrada siguiente para el sistema merlin, incluido un número de teléfono y un prefijo de marcación:

```
merlin Any ACU 1200 local8784 "" in:--in: uvenus word: espejo
```

El sistema venus puede llamar al sistema merlin en cualquier momento, utilizando un dispositivo ACU a 1200 baudios e iniciando la sesión como **uvenus** con la contraseña **mirror**. El número de teléfono se amplía según el código **local** del archivo **Dialcodes** y el dispositivo que debe utilizarse se determina en base a las entradas **Tipo** y **Clase**. BNU comprueba los archivos **Devices** para un dispositivo de tipo ACU y clase 1200.

- **Archivo Dialcodes:** El archivo **Dialcodes** del sistema venus contiene el prefijo de código de marcación siguiente para su utilización con el número en el archivo **Systems**:

```
local 9=445
```

Dado este código, el número de teléfono del sistema merlin del archivo **Systems** se amplía a **9=4458784**.

- **Archivo Devices:** El archivo **Devices** en el sistema venus contiene la entrada siguiente para la conexión con el sistema merlin:

```
ACU tty1 - 1200 hayes \T
```

El puerto que debe utilizarse es **tty1** y la entrada de **Dialer** del campo **Pares Dialer-Señal** es **hayes**. La entrada **Token**, **\T**, indica que el número de teléfono debe ampliarse utilizando un código del archivo **Dialcodes**. BNU busca en los archivos **Dialers** un tipo de dialer **hayes**.

- **Archivo Dialers:** El archivo Dialers que utiliza el daemon **uucico** en el sistema venus contiene la entrada siguiente para el módem hayes:

```
hayes =,-, "" \dAT\r\c OK \pATDT\T\r\c CONNECT
```

**Nota:** Los caracteres que se esperan para el envío están definidos en el formato del archivo Dialers.

- **Archivo Permissions:** El archivo Permissions en el sistema venus contiene las entradas siguientes, que especifican las maneras en que el sistema merlin puede llevar a cabo las transacciones **uucico** y **uxqt** con el sistema venus:

```
LOGNAME=umerlin REQUEST=yes SENDFILES=yes \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin \
MACHINE=venus:merlin VALIDATE=umerlin REQUEST=yes SENDFILES=yes \
COMMANDS=ALL \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin
```

El sistema merlin inicia la sesión en el sistema venus como umerlin, que es un inicio de sesión exclusivo para el sistema merlin. El sistema merlin puede solicitar y enviar archivos con independencia de quién haya iniciado la llamada. Además, el sistema merlin puede leer y grabar en el directorio /var/spool/uucppublic y en el directorio /home/merlin en el sistema venus. El sistema merlin puede emitir todos los mandatos en el conjunto de mandatos predeterminados en el sistema venus.

#### *Archivos BNU con entradas de conexión telefónica en el sistema local*

Estos archivos contienen entradas de conexión telefónica en el sistema local venus.

- **Archivos Systems:** Un archivo Systems en el sistema venus contiene la siguiente entrada para el sistema merlin, incluido un número de teléfono y un prefijo de marcación:

```
merlin Any ACU 1200 local8784 "" in:--in: uvenus word: espejo
```

El sistema venus puede llamar al sistema merlin en cualquier momento, utilizando un dispositivo ACU a 1200 baudios e iniciando la sesión como el usuario uvenus con la contraseña mirror. El número de teléfono se amplía según el código local del archivo Dialcodes y el dispositivo que debe utilizarse se determina en base a las entradas *Tipo* y *Clase*. BNU comprueba los archivos Devices para un dispositivo de tipo ACU y clase 1200.

- **Archivo Dialcodes:** El archivo Dialcodes del sistema venus contiene el prefijo de código de marcación siguiente para su utilización con el número en el archivo Systems:

```
local 9=445
```

Dado este código, el número de teléfono del sistema merlin del archivo Systems se amplía a 9=4458784.

- **Archivo Devices:** El archivo Devices en el sistema venus contiene la entrada siguiente para la conexión con el sistema merlin:

```
ACU tty1 - 1200 Hayes \T
```

El puerto que debe utilizarse es tty1 y la entrada de *Dialer* del campo **Pares Dialer-Señal** es hayes. La entrada *Token*, \T, indica que el número de teléfono debe ampliarse utilizando un código del archivo Dialcodes. BNU comprueba los archivos Dialers para una entrada de un tipo de dialer hayes.

- **Archivo Dialers:** El archivo Dialers que utiliza el daemon **uucico** en el sistema venus contiene la entrada siguiente para el módem hayes:

```
hayes =,-, "" \dAT\r\c OK \pATDT\T\r\c CONNECT
```

**Nota:** Los caracteres que se esperan para el envío están definidos en el formato del archivo Dialers.

- **Archivo Permissions:** El archivo Permissions en el sistema venus contiene las entradas siguientes, que especifican las maneras en que el sistema merlin puede llevar a cabo las transacciones **uucico** y **uuxqt** con el sistema venus:

```
LOGNAME=umerlin REQUEST=yes SENDFILES=yes \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin \
MACHINE=venus:merlin VALIDATE=umerlin REQUEST=yes SENDFILES=yes \
COMMANDS=ALL \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin
```

El sistema merlin inicia la sesión en el sistema venus como umerlin, que es un inicio de sesión exclusivo para el sistema merlin. El sistema merlin puede solicitar y enviar archivos con independencia de quién haya iniciado la llamada. Además, el sistema merlin puede leer y grabar en el directorio /var/spool/uucppublic y en el directorio /home/merlin en el sistema venus. El sistema merlin puede emitir todos los mandatos en el conjunto de mandatos predeterminados en el sistema venus.

#### **Archivos BNU con entradas de conexión telefónica en el sistema remoto**

Estos archivos contienen entradas de conexión telefónica en el sistema remoto merlin.

- **Archivo Systems:** El archivo Systems del sistema merlin contiene la entrada siguiente para el sistema venus, incluido un número de teléfono y un prefijo de marcación:

```
venus Any ACU 1200 intown4362 "" in:--in: umerlin word: roble
```

El sistema merlin puede llamar al sistema venus en cualquier momento, utilizando un dispositivo ACU a 1200 baudios e iniciando la sesión como el usuario umerlin con la contraseña oaktree. El número de teléfono se amplía según el código intown del archivo Dialcodes y el dispositivo que debe utilizarse se determina en base a las entradas *Tipo* y *Clase*. BNU comprueba los archivos Devices para un dispositivo de tipo ACU y clase 1200.

- **Archivo Dialcodes:** El archivo Dialcodes del sistema merlin contiene el prefijo de código de marcación siguiente para su utilización con el número en el archivo Systems:

```
intown 9=325
```

Por lo tanto, el número de teléfono ampliado para contactar con el sistema venus es 9=3254362.

- **Archivo Devices:** El archivo Devices del sistema merlin contiene la entrada siguiente para la conexión al sistema venus:

```
ACU tty1 - 1200 hayes \T
```

El ACU está conectado al puerto tty1 y el dialer es hayes. El número de teléfono está ampliado con información del archivo Dialcodes. BNU comprueba los archivos Dialers para una entrada del módem hayes.

- **Archivo Dialers:** El archivo Dialers que utiliza el daemon **uucico** en el sistema merlin contiene la entrada siguiente para el módem:

```
hayes =,-, "" \dAT\r\c OK \pATDT\T\r\c CONNECT
```

- **Archivo Permissions:** El archivo Permissions en el sistema merlin contiene las entradas siguientes, que otorgan al sistema venus acceso al sistema merlin:

```
LOGNAME=uvenus SENDFILES=call REQUEST=no \
WRITE=/var/spool/uucppublic:/home/venus \
READ=/var/spool/uucppublic:/home/venus \
MACHINE=merlin:venus VALIDATE=uvenus \
READ=/ WRITE=/ COMMANDS=ALL REQUEST=yes \
NOREAD=/etc/uucp:/usr/etc/secure \
NOWRITE=/etc/uucp:/usr/etc/secure
```

## Ejemplos: Configuración de BNU para una configuración directa

Los archivos de ejemplo siguientes están configurados para una conexión directa entre sistemas zeus y hera, donde zeus es el sistema local y hera es el sistema remoto.

El dispositivo directo en el sistema zeus es tty5. En el sistema hera, el dispositivo directo es tty1. La velocidad de la conexión es 1200 bps. El ID de inicio de sesión para el sistema zeus en el sistema hera es uzeus y la contraseña asociada es trueno. El ID de inicio de sesión para el sistema hera en el sistema zeus es uhera y la contraseña asociada es portento.

### Archivos BNU con conexión directa en los archivos del sistema local

Estos archivos contienen entradas de conexión telefónica en el sistema local zeus.

- **Archivo Systems:** El archivo Systems en el sistema zeus contiene la entrada siguiente para el sistema remoto hera:

```
hera Any hera 1200 - "" \r\d\r\d\r in:--in: uzeus word: trueno
```

Esta entrada especifica que el sistema hera puede iniciar la sesión en el sistema zeus en cualquier momento, utilizando una conexión directa, que se especifica en los archivos Devices. Para hallar la entrada en los archivos Devices, BNU utiliza el tercer y cuarto campo de la entrada Systems. Por lo tanto, BNU busca una entrada en los archivos Devices con un *Tipo* de hera y una *Clase* de 1200. El sistema zeus inicia la sesión en el sistema hera como el usuario uzeus con la contraseña trueno.

- **Archivo Devices:** El archivo Devices del sistema zeus contiene la entrada siguiente para conectarse al sistema remoto hera:

```
hera    tty5   -  1200  direct
```

Esta entrada especifica que el sistema zeus utiliza el dispositivo tty5 a 1200 bps para comunicarse con el sistema hera. Observe que el *Dialer* en ambos campos **Pares de Dialer-Señal** es directo. Al conectarse al sistema hera, BNU comprueba el archivo Dialers en busca de una entrada direct.

- **Archivo Dialers:** El archivo Dialers en el sistema zeus contiene la entrada siguiente para las conexiones directas:

```
directa
```

Esta entrada especifica que no se necesita ningún reconocimiento de conexión directa.

- **Archivo Permissions:** El archivo Permissions en el sistema local zeus contiene la entrada siguiente, que especifica los modos en que el sistema remoto hera puede llevar a cabo las transacciones **uucico** y **uuxqt** con el sistema zeus:

```
LOGNAME=uhera MACHINE=hera VALIDATE=uhera REQUEST=yes \
SENDFILES=yes MACHINE=zeus READ=/ WRITE=/ COMMANDS=ALL
```

Esta entrada especifica que el sistema hera inicia la sesión como uhera. Como se incluye la opción VALIDATE=uhera, el sistema hera no puede iniciar la sesión en el sistema zeus con ningún otro ID de inicio de sesión y ningún otro sistema remoto puede utilizar el ID de uhera. El sistema hera puede leer y grabar en cualquier directorio del sistema zeus y puede enviar y solicitar archivos con independencia de quién haya iniciado la llamada. El sistema hera también puede inicializar mandatos en el sistema zeus.

**Nota:** Puesto que los permisos que se otorgan son los mismos independientemente del sistema que haya iniciado la conexión, se han combinado las entradas LOGNAME y MACHINE. Si los permisos no son los mismos para el sistema hera y el sistema zeus, las entradas LOGNAME y MACHINE serán las siguientes:

```
LOGNAME=uhera REQUEST=yes SENDFILES=yes READ=/ WRITE=/
MACHINE=zeus:hera VALIDATE=uhera READ=/ WRITE=/ REQUEST=yes \
COMMANDS=ALL
```



**Atención:** Otorgar los permisos en el ejemplo anterior es equivalente a proporcionar a cualquier usuario del sistema remoto un ID de inicio de sesión en el sistema local. Unos permisos tan

liberales pueden poner en peligro su seguridad y sólo se le otorgan a sistemas remotos de mucha confianza en el mismo sitio.

### **Archivos BNU con conexión directa en los archivos del sistema remoto**

Estos archivos contienen entradas de conexión telefónica en el sistema remoto hera.

- **Archivo Systems:** El archivo Systems en el sistema hera contiene la entrada siguiente para el sistema zeus:

```
zeus Any zeus 1200 - "" \r\d\r\d\r in:--in: uhera word: portento
```

Esta entrada especifica que el sistema hera puede iniciar la sesión en el sistema zeus en cualquier momento, utilizando una conexión directa, que se especifica en los archivos Devices. Para hallar la entrada en los archivos Devices, BNU utiliza el tercer y cuarto campo de la entrada Systems. Por lo tanto, BNU busca una entrada en los archivos Devices con el campo **Tipo** de valor zeus y un campo **Clase** de valor 1200. El sistema hera inicia la sesión en el sistema zeus como el usuario uhera con la contraseña portento.

- **Archivo Devices:** El archivo Devices del sistema hera contiene la entrada siguiente para las comunicaciones con el sistema zeus:

```
zeus    tty1   -  1200  direct
```

Esta entrada especifica que el sistema hera utiliza el dispositivo tty1 a 1200 bps para comunicarse con el sistema zeus. Puesto que el **Dialer** se ha especificado como direct, BNU comprueba los archivos Dialers en busca de una entrada direct.

- **Archivo Dialers:** El archivo Dialers del sistema hera contiene la entrada siguiente para las conexiones directas:

```
directa
```

Esta entrada especifica que no es necesario configurar el dialer en la conexión directa.

- **Archivo Permissions:** El archivo Permissions del sistema hera contiene las entradas siguientes, que especifican las formas en las que zeus puede llevar a cabo las transacciones **uucico** y **uuxqt** con el sistema hera:

```
LOGNAME=uzeus REQUEST=yes SENDFILES=yes READ=/ WRITE=/
MACHINE=hera:zeus VALIDATE=uzeus REQUEST=yes COMMANDS=ALL READ=\
WRITE=/

```

Estas entradas especifican que el sistema zeus debe iniciar la sesión en el sistema hera como uzeus. Puesto que se incluye el parámetro VALIDATE=uzeus, el sistema zeus no puede iniciar sesión en el sistema hera con ningún otro ID de inicio de sesión, ni puede ningún otro sistema remoto utilizar el ID de uzeus. El sistema zeus puede leer y grabar en cualquier directorio del sistema hera y puede enviar y solicitar archivos con independencia de quién haya iniciado la llamada. El sistema zeus también puede inicializar mandatos en el sistema hera.



**Atención:** Si proporciona todos los permisos en el ejemplo anterior, es equivalente a proporcionar a cualquier usuario del sistema remoto un ID de inicio de sesión en el sistema local. Unos permisos tan liberales pueden poner en peligro su seguridad y se le otorgan sólo a los sistemas remotos del mismo sitio.

## **Mantenimiento de BNU**

BNU requiere un mantenimiento para que funcione correctamente en el sistema.

Para el mantenimiento de BNU:

- Lea y suprima los archivos de anotaciones cronológicas de forma periódica.
- Utilice los mandatos **uuq** y **uustat** para comprobar las colas de BNU y asegurarse de que los trabajos se estén transfiriendo a los sistemas remotos correctamente.

- Planifique mandatos automáticos para sondear los sistemas remotos en busca de trabajos, devolver los archivos no enviados a los usuarios y enviar mensajes sobre el estado de BNU de forma periódica.
- Actualice los archivos de configuración periódicamente para que reflejen las modificaciones de su sistema.

Además, cada cierto tiempo compruebe con los administradores de los sistemas remotos si las modificaciones de sus sistemas puede afectar la configuración. Por ejemplo, si el supervisor del sistema venus cambia la contraseña del sistema, deberá colocar la contraseña nueva en el archivo /etc/uucp/Systems (o en el archivo Systems adecuado que /etc/uucp/Sysfiles especifique) para que su sistema pueda iniciar la sesión en el sistema venus.

### **Archivos de anotaciones cronológicas de BNU**

BNU crea archivos de anotaciones cronológicas y archivos de errores para realizar un seguimiento de sus propias actividades.

Estos archivos deben comprobarse y eliminarse periódicamente para evitar que llenen el espacio de almacenamiento del sistema. BNU proporciona varios mandatos que pueden utilizarse para eliminar los archivos de anotaciones cronológicas:

- uulog
- uuclean
- uucleanup
- uu demon .cleanu .

Ejecute estos mandatos manualmente o utilice entradas del archivo /var/spool/cron/crontabs/uucp para que el daemon **cron** ejecute los mandatos.

### **Archivos de anotaciones cronológicas de los directorios .Log y .Old**

BNU crea archivos de anotaciones cronológicas individuales en el directorio /var/spool/uucp/.Log.

BNU crea estos archivos de anotaciones cronológicas para cada sistema remoto accesible utilizando los mandatos **uucp**, **uucico**, **uux** y **uuxqt**. BNU coloca la información de estado sobre cada transacción en el archivo de anotaciones cronológicas adecuado cada vez que alguien utiliza BNU en el sistema. Cuando se ejecuta más de un proceso BNU, el sistema no puede acceder al archivo de anotaciones cronológicas. En su lugar, coloca la información de estado en otro archivo con el prefijo .LOG.

El mandato **uulog** muestra un resumen de las peticiones **uucp** o **uux**, clasificadas por usuarios o por sistemas. El mandato **uulog** muestra los archivos. Sin embargo, también puede hacer que BNU combine los archivos de anotaciones cronológicas de forma automática en un archivo de anotaciones cronológicas primario. Esto se denomina *compactación* de los archivos de anotaciones cronológicas y puede realizarse con el mandato **uu demon .cleanu**, normalmente ejecutado por el daemon **cron**.

El daemon **cron** ejecuta el mandato **uu demon .cleanu**. El mandato **uu demon .cleanu** combina los archivos de anotaciones cronológicas **uucico** y **uuxqt** del sistema local y los almacena en el directorio /var/spool/uucp/.Old. Al mismo tiempo, el mandato elimina los archivos de anotaciones cronológicas antiguos previamente almacenados en el directorio .Old. Por omisión, el mandato **uu demon .cleanu** guarda los archivos de anotaciones cronológicas que tienen dos días de antigüedad.

Si el espacio de almacenamiento resulta un problema, plantéese reducir el número de días que se guardan los archivos. Para realizar un seguimiento de las transacciones de BNU durante un período de tiempo más amplio, plantéese aumentar el número de días que se guardan los archivos. Para cambiar el tiempo por omisión que los archivos de anotaciones cronológicas se guardan, modifique el procedimiento de shell del mandato **uu demon .cleanu**. Este script se almacena en el directorio /usr/sbin/uucp y puede modificarse con autorización root.

### **Archivos de anotaciones cronológicas de BNU /.Admin**

BNU también recopila información y la almacena en el directorio /var/spool/uucp/.Admin. Este directorio contiene los archivos errors, xferstats, Foreign y audit.

Estos archivos deben comprobarse y eliminarse periódicamente para ahorrar espacio de almacenamiento. BNU crea cada archivo cuando lo necesita.

Cuando otro sistema contacta con su sistema con la modalidad de depuración del daemon **uucico** activada, éste invoca al daemon **uucico** de su sistema con la depuración activada. Los mensajes de depuración que el daemon genere en el sistema local se almacenan en el archivo audit. Este archivo puede hacerse bastante grande. Compruebe y elimine el archivo audit con frecuencia.

El archivo errors registra los errores que el daemon **uucico** encuentra. Comprobando este archivo podrá corregir problemas como, por ejemplo, permisos incorrectos sobre archivos de trabajo de BNU.

El archivo xferstats contiene información sobre el estado de cada transferencia de archivos. Compruebe y elimine este archivo con frecuencia.

El archivo Foreign es importante para la seguridad del sistema. Cada vez que un sistema desconocido intenta iniciar la sesión en el sistema local, BNU llama al procedimiento de shell remote.unknown. Este procedimiento de shell registra el intento en el archivo Foreign. El archivo Foreign contiene el nombre de los sistemas que han intentado llamar al sistema local y han sido rechazados. Si un sistema ha estado intentando llamar con frecuencia, utilice esta información cuando se plantea si debe permitirse el acceso a este sistema.

#### **Archivos de anotaciones cronológicas de todo el sistema que BNU utiliza**

Como muchos procesos BNU requieren autorización root para llevar a cabo sus tareas, BNU crea con frecuencia entradas en el archivo /var/spool/sulog/log.

De forma similar, si se utiliza el daemon **cron** para planificar las tareas BNU, se crearán varias entradas en el archivo /var/spool/cron/log. Cuando utilice BNU, compruebe y limpie estos archivos.

#### **Mandatos de mantenimiento de BNU**

Los Programas de utilidad básicos de red (Basic Networking Utilities o BNU) contienen varios mandatos para supervisar las actividades de BNU y limpiar los directorios y archivos de BNU.

#### **Mandatos de limpieza de BNU**

BNU incluye tres mandatos para limpiar los directorios y eliminar los archivos que no se han enviado.

<b>Item</b>	<b>Descripción</b>
<b>uuclean</b>	Suprime de los directorios de administración de BNU todos los archivos con una antigüedad superior al número de horas especificado. Utilice el mandato <b>uuclean</b> para especificar el directorio que debe limpiarse o el tipo de archivo que debe suprimirse. También puede indicar al mandato que informe a los propietarios de los archivos suprimidos. El mandato <b>uuclean</b> es el equivalente de Berkeley del mandato <b>uucleanup</b> .
<b>uucleanup</b>	Realiza funciones similares al mandato <b>uuclean</b> . Sin embargo, el mandato <b>uucleanup</b> comprueba la antigüedad de los archivos en función de los <i>días</i> en vez de las horas. Utilice el mandato <b>uucleanup</b> para enviar un mensaje de advertencia a los usuarios cuyos archivos no se hayan transferido, comunicándoles que los archivos continúan en la cola. El mandato <b>uucleanup</b> también elimina los archivos relativos a un sistema remoto especificado.
<b>uudemon.cleanu</b>	Un procedimiento de shell que emite los mandatos <b>uulog</b> y <b>uucleanup</b> para comprimir los archivos de anotaciones cronológicas de BNU y eliminar los archivos de trabajo y de anotaciones cronológicas cuya antigüedad supere los tres días. El daemon <b>cron</b> es el que ejecuta el mandato <b>uudemon.cleanu</b> .

#### **Mandatos BNU para la comprobación del estado**

BNU también proporciona mandatos para comprobar el estado de las transferencias y los archivos de anotaciones cronológicas.

Item	Descripción
<b>uuq</b>	Visualiza los trabajos que están actualmente en la cola de trabajos de BNU. Utilice el mandato <b>uuq</b> para visualizar el estado de un trabajo especificado o de todos los trabajos. Si posee autorización root, podrá utilizar el mandato <b>uuq</b> para suprimir un trabajo de la cola.
<b>uustat</b>	Proporciona información similar a la que proporciona el mandato <b>uuq</b> , con un formato distinto. Utilice el mandato <b>uustat</b> para comprobar el estado de los trabajos y suprimir los trabajos de los que sea el propietario. Si posee autorización root, también podrá suprimir los trabajos que pertenezcan a otros usuarios.
<b>uulog</b>	Visualiza un resumen de las peticiones de <b>uucp</b> o <b>uux</b> , clasificadas por usuarios o por sistemas. El mandato <b>uulog</b> visualiza el nombre de los archivos. Consulte el apartado “Archivos de anotaciones cronológicas de BNU” en la página 531.
<b>uupoll</b>	Impone un sondeo de un sistema remoto. Esto resulta útil cuando en la cola está esperando trabajo para este sistema que debe transferirse antes de que se haya planificado una llamada automática del sistema.
<b>uusnap</b>	Visualiza un resumen muy breve del estado de BNU. Para cada sistema remoto, este mandato muestra el número de archivos que deben transferirse. Sin embargo, no muestra cuánto tiempo han estado esperando. El mandato <b>uusnap</b> es el equivalente de Berkeley del mandato <b>uustat</b> .

### Procedimientos del shell BNU

BNU se proporciona con dos procedimientos para el shell que se utilizan para su mantenimiento:

Item	Descripción
<b>uudemon.cleanu</b>	Se trata en el apartado “Mandatos de limpieza de BNU” en la página 532.
<b>uudemon.admin</b>	Emite el mandato <b>uustat</b> . El mandato <b>uustat</b> informa sobre el estado de los trabajos de BNU. Envía el resultado al ID de inicio de sesión de uucp en forma de correo. Es posible modificar el procedimiento del shell <b>uudemon.admin</b> para enviar el correo a otro lugar o utilizar un programa de correo para redireccionar todo el correo del ID de inicio de sesión de uucp al usuario responsable de la administración de BNU.

Estos procedimientos del shell se almacenan en el directorio `/usr/sbin/uucp`. Copie los procedimientos y modifique la copia si desea cambiar lo que hacen. Ejecute los procedimientos desde la línea de mandatos o planifíquelo para que los ejecute el daemon **cron**.

Para ejecutar los mandatos **uudemon.cleanu** y **uudemon.admin** de forma automática, elimine los caracteres de comentario (#) del principio de las líneas correspondientes del archivo `/var/spool/cron/crontabs/uucp`.

### Nombres de vías de acceso de BNU

Los nombres de vía de acceso que se utilizan con los mandatos de los Programas de utilidad básicos de red (BNU) se pueden entrar de distintas formas.

Los nombres de vía de acceso constan del directorio raíz o de una vía de acceso de atajo al destino, que es el nombre de un sistema o de varios sistemas remotos. Cada formato sigue unas directrices específicas.

#### Nombre de vía de acceso completo

Un nombre de vía de acceso completo empieza en el directorio raíz y efectúa un rastreo de todos los directorios que quedan por debajo hasta llegar al archivo y directorio de destino.

Por ejemplo, `/etc/uucp/Devices` hace referencia al archivo `Devices` del directorio `uucp` del directorio raíz `etc`.

Para indicar un directorio raíz, siempre es preciso especificar delante el carácter de barra inclinada (/). Separe siempre los elementos de la vía de acceso mediante el carácter de barra inclinada (/).

## Nombre de vía de acceso relativo

El nombre de vía de acceso relativo sólo contiene los directorios que dependen del directorio actual.

Por ejemplo, si el directorio actual es `/usr/bin` y el directorio de destino es `/usr/bin/reports`, escriba el nombre de vía de acceso relativo `reports` (sin la barra inclinada inicial).

Los nombres de vía de acceso relativos se pueden utilizar con los mandatos **cu**, **uucp** y **uux**, así como con el nombre del archivo fuente en el mandato **uuto**.

**Nota:** Puede que los nombres de vía de acceso relativos no funcionen con todos los mandatos BNU. Si experimenta algún problema al utilizar un nombre de vía de acceso relativo, vuelva a entrar el mandato con el nombre de vía de acceso completo.

## Nombre de vía de acceso ~ [opción]

El nombre de vía de acceso `~ [opción]` representa el directorio inicial del usuario especificado.

El carácter de tilde (~) se puede utilizar como un atajo a determinados directorios.

Por ejemplo, `~juan` hace referencia al directorio inicial del usuario `juan`. La entrada `~uucp` o `~` (tilde sola) hace referencia al directorio público de BNU en el sistema remoto. El nombre de vía de acceso completo del directorio público de BNU es `/var/spool/uucppublic`.

**Nota:** Este uso de la tilde no debe confundirse con el otro uso de la tilde en BNU. El carácter de tilde también se utiliza delante de algunos mandatos para su ejecución en un sistema local cuando el usuario ha iniciado una sesión en un sistema remoto utilizando el mandato **cu**.

## nombre\_sistema!, nombre de vía de acceso

El nombre de vía de acceso `nombre_sistema!` identifica la vía de acceso a un archivo de otro sistema.

Por ejemplo, `distant!/account/march` hace referencia al archivo `march` del directorio `account` del sistema remoto `distant`.

## nombre\_sistema!nombre\_sistema!, nombre de vía de acceso

El nombre de vía de acceso `nombre_sistema!nombre_sistema!` identifica una vía de acceso a través de múltiples sistemas.

Por ejemplo, si sólo se puede llegar al sistema denominado `distant` a través de otro sistema denominado `near`, el nombre de vía de acceso es `near!distant!/account/march`.

Separé los nombres de sistemas mediante un signo de exclamación final (!). En el caso de múltiples nombres de vía de acceso de sistemas, no se aplica la norma de separación de los nombres de sistemas con una barra inclinada (/). No obstante, la norma sí sigue siendo válida para el sistema final, en el que se estipulan los archivos y directorios.

**Nota:** Cuando utilice un shell Bourne, separe los nombres de sistema con un signo de exclamación final (!). Cuando utilice BNU en un shell C o Korn, ponga una barra inclinada invertida (\) delante del signo de exclamación. La barra inclinada invertida es un carácter de escape necesario para poder interpretar literalmente el siguiente carácter y no como un carácter especial.

## Daemons de BNU

El software de BNU incluye cuatro daemons que están almacenados en el directorio `/usr/sbin/uucp`.

Item	Descripción
<b>uucico</b>	Facilita las transferencias de archivos (consulte el apartado “ <a href="#">uucico, daemon</a> ” en la página 535)
<b>uusched</b>	Facilita la planificación de peticiones de trabajo de los archivos en cola en el directorio de spooling local (consulte el apartado “ <a href="#">Daemon uusched</a> ” en la página 535)
<b>uuxqt</b>	Facilita la ejecución de los mandatos remotos (consulte el apartado “ <a href="#">uuxqt, daemon</a> ” en la página 536)

<b>Item</b>	<b>Descripción</b>
<b>uucpd</b>	Facilita la comunicación utilizando TCP/IP (consulte el apartado “ <a href="#">Daemon uucpd</a> ” en la página 536)

El daemon **cron** inicia los daemons **uucico**, **uusched** y **uuxqt** en función de la planificación establecida por el administrador de BNU. Con autorización root, también es posible iniciar estos daemons manualmente. El daemon **uucpd** debe iniciar el daemon de TCP/IP **inetd**.

#### **uucico, daemon**

El daemon **uucico** transporta los archivos necesarios para enviar datos de un sistema a otro.

Los mandatos **uucp** y **uux** inician el daemon **uucico** para transferir archivos de mandatos, datos y ejecución al sistema especificado. El planificador de BNU, el daemon **uusched**, también inicia el daemon **uucico** periódicamente. Cuando lo inicia el daemon **uusched**, el daemon **uucico** intenta contactar con los otros sistemas y ejecutar las instrucciones de los archivos de mandatos.

Para ejecutar las instrucciones de los archivos de mandatos, el daemon **uucico** comprueba primero el archivo `/etc/uucp/Systems` (o uno o más archivos distintos especificados mediante `/etc/uucp/Sysfiles`) para el sistema que debe llamarse. El daemon comprueba entonces la entrada del archivo `Systems` en busca del tiempo válido para llamar. Si el tiempo es válido, el daemon **uucico** comprueba los campos *Tipo* y *Clase* y accede al archivo `/etc/uucp/Devices` (o a uno o más archivos distintos especificados mediante `/etc/uucp/Sysfiles`) en busca de un dispositivo que coincida.

Una vez encontrado un dispositivo, el daemon **uucico** comprueba el directorio `/var/locks` en busca de un archivo de bloqueo para el dispositivo. Si existe uno, el daemon comprueba si hay otro dispositivo del tipo y la velocidad especificados.

Cuando no hay disponible ningún dispositivo, el daemon vuelve a los archivos `Systems` en busca de otra entrada para el sistema remoto. Si existe una, el daemon repite el proceso de búsqueda de un dispositivo. Si no se encuentra otra entrada, el daemon hace una entrada en el archivo `/var/spool/uucp/.Status/SystemName` para este sistema remoto y continúa hasta la siguiente petición. El archivo de mandatos permanece en la cola. El daemon **uucico** intenta volver a realizar la transmisión más tarde. Este intento posterior se denomina *reintento*.

Cuando el daemon **uucico** llega al sistema remoto, utiliza las instrucciones de los archivos `Systems` para iniciar la sesión. Esto hace que se invoque una instancia del daemon **uucico** en el sistema remoto también.

Los dos daemons **uucico**, uno en cada sistema, trabajan juntos para realizar la transferencia. El daemon **uucico** del sistema que realiza la llamada controla el enlace y especifica las peticiones que deben realizarse. El daemon **uucico** del sistema remoto comprueba si los permisos locales permiten que se realice la petición. En caso afirmativo, se inicia la transferencia del archivo.

Una vez el daemon **uucico** del sistema que realiza la llamada ha terminado de transferir todas las peticiones que tiene para el sistema remoto, éste envía una petición de quedar en suspenso. Cuando el daemon remoto **uucico** tiene transacciones para enviar al sistema que llama, éste rechaza la petición de quedar en suspenso y los dos daemons invierten sus funciones.

**Nota:** El archivo `/etc/uucp/Permissions` del sistema local o el archivo `/etc/uucp/Permissions` del sistema remoto pueden prohibir que los daemons inviertan sus funciones. En este caso, el sistema remoto debe esperar hasta que llame al sistema local para transferir los archivos.

Cuando no quede nada por transferir en ninguna de las direcciones, los dos daemons **uucico** quedan en suspenso. En este punto, se llama al daemon **uuxqt** (“[uuxqt, daemon](#)” en la página 536) para ejecutar las peticiones de mandatos remotas.

En el transcurso del proceso de transferencia, los daemons **uucico** de ambos sistemas registran los mensajes en los archivos de errores y de anotaciones cronológicas de BNU.

#### **Daemon uusched**

El daemon **uusched** planifica la transferencia de archivos que están en cola en el directorio de spooling en el sistema local.

El directorio de spooling es `/var/spool/uucppublic`. Cuando se invoca el daemon **uusched**, éste busca los archivos de mandatos en el directorio de spooling y, a continuación, coloca los archivos aleatoriamente e inicia el daemon **uucico**. El daemon **uucico** transfiere los archivos.

#### **uuxqt, daemon**

Cuando un usuario emite el mandato **uux** para ejecutar un determinado mandato en un sistema especificado, el daemon **uuxqt** ejecuta el mandato.

Después de crear los archivos necesarios, el mandato **uux** inicia el daemon **uucico**, que transfiere estos archivos al directorio de spooling público del sistema especificado.

El daemon **uuxqt** busca de forma periódica las peticiones de ejecución de mandatos en el directorio de spooling de cada uno de los sistemas conectados. Cuando localiza una petición de este tipo, el daemon **uuxqt** comprueba la existencia de los archivos y los permisos necesarios. Entonces, si se le permite, el daemon ejecuta el mandato especificado.

#### **Daemon uucpd**

El daemon **uucpd** debe poder ejecutarse en el sistema remoto antes de que BNU pueda establecer comunicación con un sistema remoto mediante **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

El daemon **uucpd** es un subservidor del daemon de TCP/IP **inetd** y es el daemon **inetd** quien lo inicia.

Por omisión, el daemon **uucpd** aparece comentado en el archivo `inetd.conf`. Para utilizarlo, debe eliminar el carácter de comentario y reiniciar **inetd**. Sin embargo, si éste se ha cambiado en su sistema, es posible que necesite reconfigurar el daemon **inetd** para iniciar el daemon **uucpd**.

## **Seguridad en BNU**

Como otros sistemas contactan con su sistema para iniciar la sesión, transferir archivos y escribir mandatos, BNU proporciona una forma para establecer seguridad.

La seguridad en BNU permite restringir lo que los usuarios de sistemas remotos pueden realizar en el sistema local (los usuarios de los sistemas remotos también pueden restringir lo que puede hacerse en sus sistemas). BNU ejecuta varios daemons para llevar a cabo sus actividades y utiliza directorios administrativos para almacenar los archivos que necesita. BNU también mantiene un registro de sus propias actividades.

La seguridad en BNU funciona a varios niveles. Al configurar BNU, es posible determinar:

- Quién en el sistema tiene acceso a los archivos BNU.
- Con qué sistemas remotos puede contactar su sistema.
- Cómo puede iniciar la sesión en su sistema los usuarios de sistemas remotos.
- Qué pueden hacer los usuarios de sistemas remotos en el sistema una vez han iniciado la sesión.

#### **ID de inicio de sesión de uucp**

Cuando BNU está instalado, todos los archivos de configuración y los daemons y muchos de los mandatos y los procedimientos del shell son propiedad del ID de inicio de sesión de uucp.

El ID de inicio de sesión de uucp tiene un ID de usuario (UID) de 5 y un ID de grupo (GID) de 5. El daemon **cron** lee el archivo `/var/spool/cron/crontabs/uucp` para planificar los trabajos automáticos para BNU.

Normalmente no se permite iniciar la sesión como uucp del usuario. Para cambiar los archivos que son propiedad del ID de inicio de sesión de uucp, inicie la sesión con autorización root.



**Atención:** Al permitir que los sistemas remotos inicien la sesión en el sistema local con el ID de inicio de sesión de uucp se pone en serio peligro la seguridad del sistema local. Los sistemas remotos que inicien la sesión con el ID de uucp pueden visualizar, y posiblemente modificar, los archivos `Systems` y `Permissions` locales, en función del resto de los permisos que se hayan especificado en la entrada `LOGNAME`. Se recomienda encarecidamente que cree otros ID de inicio de sesión de BNU para los sistemas remotos y que reserve el ID de inicio de sesión de uucp para la persona responsable de administrar el BNU en el sistema local. Para una mejor seguridad, cada

sistema remoto que contacte con el sistema local debe tener un ID de inicio de sesión exclusivo con un número de UID exclusivo.

El sistema operativo proporciona un ID de inicio de sesión de nuucp por omisión para la transferencia de archivos.

### ID de inicio de sesión de BNU

El shell de arranque para los ID de inicio de sesión de BNU es el daemon **uucico** (/usr/sbin/uucp/uucico).

Cuando los sistemas remotos llaman al sistema, inician de forma automática el daemon **uucico** en el sistema. Los ID de inicio de sesión de BNU tienen el ID de grupo de uucp 5.

Los ID de inicio de sesión que los sistemas remotos utilizan requieren contraseñas. Para evitar que la seguridad solicite un ID de inicio de sesión de BNU nuevo cuando el sistema remoto inicia la sesión, la contraseña debe establecerse tan pronto como se cree la cuenta. Para hacerlo, utilice el mandato **passwd** seguido por el mandato **pwdadm**. Por ejemplo, para establecer una contraseña para el ID de inicio de sesión de nuucp, inicie la sesión como usuario root y entre los mandatos siguientes:

```
passwd nuucp
```

```
pwdadm -f NOCHECK  
nuucp
```

El sistema le solicita una contraseña para el ID de inicio de sesión de nuucp. Tras completar estos pasos, el sistema remoto puede iniciar la sesión sin que se le solicite una contraseña nueva de inmediato (lo que el ID de inicio de sesión de nuucp, que está orientado por lotes, no puede proporcionar).

Una vez creado el ID de inicio de sesión para un sistema remoto, deberá indicar al administrador del BNU del sistema el ID de inicio de sesión y la contraseña para acceder a su sistema.

Un usuario con autorización root puede configurar un ID de inicio de sesión de administración de BNU. Esto resulta útil si desea delegar las tareas de administración de BNU a un usuario sin autorización root. El ID de inicio de sesión de administración de BNU debe tener seguridad de contraseña, el UID 5 y encontrarse en el ID de grupo de uucp 5. El shell de inicio de sesión para el inicio de sesión de administración debería ser el programa /usr/bin/sh (en lugar del daemon **uucico**). Al proporcionar al inicio de sesión de administración de BNU el UID 5, éste obtiene los mismos privilegios que el ID de inicio de sesión de **uucp**. Por ello, por razones de seguridad, no debería permitirse que los sistemas remotos iniciaran la sesión como administradores de BNU.

### Seguridad en los archivos Systems y remote.unknown

En la mayoría de sistemas BNU, sólo los sistemas remotos que se listan en el archivo /etc/uucp/Systems o un sustituto de los mismos (especificado en el archivo Sysfiles) puede iniciar la sesión en el sistema local.

El script /usr/sbin/uucp/remote.unknown se ejecuta siempre que un sistema desconocido intenta llamar al sistema local. Este script no permite que el sistema desconocido inicie la sesión y crea una entrada en el archivo /var/spool/uucp/.Admin/Foreign que registra la hora en que se ha intentado iniciar la sesión.

Con autorización root o como un administrador BNU, es posible modificar el procedimiento del shell remote.unknown para que registre más información sobre el sistema remoto o almacene la información en un archivo distinto. Por ejemplo, puede modificar el procedimiento del shell para enviar el correo al administrador de BNU cada vez que un sistema desconocido intente iniciar la sesión.

Si se eliminan los permisos de ejecución sobre el procedimiento del shell remote.unknown, se permite iniciar la sesión a las máquinas desconocidas. En este caso, debe añadir una entrada MACHINE=OTHER al archivo /etc/uucp/Permissions para establecer los permisos para las máquinas desconocidas.

El sistema sólo puede contactar con los sistemas remotos listados en el archivo Systems. Con ello se evita que los usuarios de su sistema contacten con sistemas desconocidos.

## **Seguridad en el archivo Permissions**

Tenga en cuenta los siguientes aspectos sobre seguridad cuando utilice el archivo Permissions.

El archivo /etc/uucp/Permissions determina:

- El nombre de los usuarios autorizados a un inicio de sesión remoto en el sistema local
- Los mandatos y privilegios aprobados para los sistemas remotos que inician la sesión en el sistema local.

El archivo /etc/uucp/Permissions contiene dos tipos de entradas:

<b>Item</b>	<b>Descripción</b>
<b>LOGNAME</b>	Define los nombres de inicio de sesión y los privilegios asociados con ellos. Las entradas LOGNAME surten efecto cuando un sistema remoto llama al sistema local e intenta iniciar la sesión.
<b>MACHINE</b>	Define los nombres de las máquinas y los privilegios asociados con ellos. Las entradas MACHINE surten efecto cuando el sistema remoto intenta ejecutar mandatos en el sistema local.

Las opciones del archivo Permissions permiten establecer varios niveles de seguridad para cada sistema remoto. Por ejemplo, si muchos sistemas remotos comparten un ID de inicio de sesión en el sistema local, puede utilizar la opción VALIDATE para que cada sistema remoto deba utilizar un ID de inicio de sesión exclusivo. Las opciones SENDFILES, REQUEST y CALLBACK especifican qué sistema tiene control, manteniendo el sistema local en control de las transacciones si es necesario.

Las opciones READ, WRITE, NORREAD y NOWRITE definen el acceso a directorios específicos del sistema local. Estas opciones también control las ubicaciones del sistema en las que los usuarios remotos pueden colocar datos. La opción COMMANDS limita el número de mandatos que los usuarios de sistemas remotos pueden ejecutar en el sistema local. La opción COMMANDS=ALL permite la totalidad de privilegios a los sistemas estrechamente asociados con su sistema.



**Atención:** La opción COMMANDS=ALL puede suponer un serio peligro para la seguridad de su sistema.

## **Comunicación entre sistemas locales y remotos**

Para la comunicación entre un sistema remoto y un sistema local, el sistema remoto debe tener un enlace por cable o módem con el sistema local, tener instalado un sistema operativo basado en UNIX y tener en ejecución BNU u otra versión de UNIX-to-UNIX Copy Program (UUCP).

**Nota:** Se puede utilizar BNU para comunicarse con un sistema que no sea UNIX, pero dichas conexiones puede que precisen hardware o software adicional.

BNU posee dos mandatos que le permiten comunicarse con sistemas remotos. El mandato **cu** conecta sistemas a través de líneas telefónicas o cableadas. El mandato **ct** únicamente conecta sistemas a través de líneas telefónicas, con el uso de un módem.

Utilice el mandato **cu** para establecer la comunicación entre redes cuando conozca el número de teléfono o el nombre del sistema de destino. Para utilizar el mandato **ct**, *debe* disponer del número de teléfono del sistema de destino.

**Nota:** Existe un tercer mandato, **tip**, que funciona de forma muy parecida al mandato **cu**. Sin embargo, el mandato **tip** es un componente de la versión Berkeley Software Distribution (BSD) del programa UUCP. Su instalación con BNU precisa una configuración especial.

### **Comunicación con otro sistema por cable o módem**

Utilice el mandato **cu** desde el sistema local para llevar a cabo las siguientes tareas comunicativas:

- Establecer una conexión con un sistema remoto especificado
- Iniciar una sesión en el sistema remoto
- Realizar tareas en el sistema remoto

- Trabajar al mismo tiempo en ambos sistemas, pasando de uno a otro indistintamente

Si el sistema remoto se está ejecutando con el mismo sistema operativo, puede emitir los mandatos habituales desde el sistema local. Por ejemplo, emita mandatos para cambiar de directorio, ver su contenido, examinar archivos o enviarlos a la cola de impresión de un sistema remoto. Si desea emitir mandatos para su uso en el sistema local o para iniciar intercambios de archivos y mandatos remotos, utilice mandatos locales **cu** especiales, precedidos por el carácter de tilde (~).

### **Comunicación con otro sistema por módem**

Emita el mandato **ct** para comunicarse por módem con otro sistema.

Entre el mandato **ct**, seguido de un número de teléfono, para llamar al módem remoto. Cuando se establezca la conexión, aparecerá el indicador de inicio de sesión remota en la pantalla.

El mandato **ct** puede resultar útil en determinadas situaciones. Para obtener detalles sobre cómo utilizar el mandato de BNU **ct**, consulte:

- “Marcación de un número hasta establecer una conexión” en la página 539
- “Marcación de varios números hasta establecer una conexión” en la página 539

#### **Marcación de un número hasta establecer una conexión**

Este procedimiento describe cómo utilizar el mandato **ct** para continuar marcando un número de módem remoto hasta que se haya establecido una conexión o hasta que haya transcurrido un tiempo especificado.

El sistema al que va a llamar debe estar ejecutando los Programas de utilidad básicos de red (BNU) o alguna versión del UNIX-to-UNIX Copy Program (UUCP).

Escriba lo siguiente en la línea de mandatos del sistema local:

```
ct -w3 5550990
```

Se efectúa la llamada al número de teléfono 555-0990 del módem remoto. El distintivo y el número **-w3** indican al mandato **ct** que debe llamar al módem remoto hasta que se establezca una conexión o hasta que hayan transcurrido tres minutos.

**Nota:** Escriba el número de teléfono del módem remoto en la línea de mandatos de **ct**, antes o después del distintivo.

#### **Marcación de varios números hasta establecer una conexión**

Este procedimiento describe el uso del mandato **ct** para continuar marcando múltiples números de módems remotos hasta establecer una conexión o hasta que se agota un período de tiempo especificado.

El sistema al que va a llamar debe estar ejecutando los Programas de utilidad básicos de red (BNU) o alguna versión del UNIX-to-UNIX Copy Program (UUCP).

Escriba lo siguiente en la línea de mandatos del sistema local:

```
ct -w6 5550990 5550991 5550992 5550993
```

Se efectúa la llamada a los números de teléfono 555-0990, 555-0991, 555-0992 y 555-0993 de los módems remotos. El distintivo y el número **-w6** indican al mandato **ct** que debe llamar al módem remoto a intervalos de un minuto hasta que se establezca una conexión o hasta que hayan transcurrido seis minutos.

**Nota:** Escriba los números de teléfono de los módems remotos en la línea de mandatos de **ct**, antes o después del distintivo.

### **Intercambio de archivos entre sistemas locales y remotos**

La transferencia de archivos entre sistemas es la aplicación más típica de los Programas de utilidad básicos de red (BNU). BNU utiliza cuatro mandatos, **uucp**, **uusend**, **uuto** y **uupick**, para intercambiar archivos entre sistemas locales y remotos.

El mandato **uucp** es el programa de utilidad principal para transferencia de datos BNU. El mandato **uusend** es el mandato de transferencia de Berkeley Software Distribution (BSD) incorporado a BNU. Los mandatos **uuto** y **uupick** son mandatos de envío y recepción especializados que funcionan con el mandato **uucp**.

Los mandatos BNU, **uuencode** y **uudecode**, facilitan la transferencia de archivos. Estos mandatos codifican y decodifican los archivos binarios que se transmiten por medio del recurso de correo BNU.

### **Envío y recepción de archivos**

Entre los mandatos utilizados para enviar y recibir archivos a través de una conexión BNU se incluyen los mandatos **uucp** y **uusend**.

Utilice el mandato **uucp** y las opciones para intercambiar archivos en el sistema local, entre el sistema local y un sistema remoto y entre sistemas remotos. Por ejemplo, las opciones de **uucp** pueden crear directorios para contener los archivos en el sistema destinatario, o para enviar mensajes sobre el éxito o el fracaso de las transferencias de archivos.

Utilice el mandato **uusend** para enviar archivos a un sistema remoto que no está enlazado directamente al sistema remitente, pero al que se puede acceder a través de una cadena de conexiones BNU. A pesar de estar provisto de un menor número de opciones que el mandato **uucp**, **uusend** se incluye entre los programas de utilidad BNU para satisfacer las preferencias de los usuarios del UNIX-to-UNIX Copy Program (UUCP) de BSD.

### **Envío de archivos a un usuario específico**

Para enviar archivos a un usuario en concreto, los sistemas remitente y destinatario deben ejecutar los Programas de utilidad básicos de red (BNU) o alguna versión de UNIX-to-UNIX Copy Program (UUCP).

Utilice el mandato **uuto** para enviar archivos de un sistema a otro. Forma parte del mandato **uucp** y simplifica el proceso de intercambio de archivos tanto para los remitentes como para los destinatarios. El mandato **uuto** envía archivos a un determinado usuario y los deposita directamente en su directorio personal, el cual se encuentra en el directorio público BNU de dicho sistema. También notifica al destinatario que ha llegado un archivo. El destinatario utiliza el mandato **uupick** para manejar el archivo nuevo.

### **Envío de un archivo con el mandato uuto**

Cuando utilice el mandato **uuto** para enviar un archivo, incluya el archivo que se debe enviar, el destino del sistema remoto y el usuario de destino.

Por ejemplo:

```
uuto /home/bin/archivo1 distant!eva
```

Esta operación envía *archivo1* desde el directorio local */home/bin* al usuario *joe* del sistema remoto *distant*.

El mandato **uuto** se ejecuta bajo el mandato **uucp**. El archivo se transfiere al sistema remoto, en */var/spool/uucppublic*. El archivo se deposita en el directorio */var/spool/uucppublic/receive/usuario/Sistema* del sistema remoto. Si el directorio de destino no existe, se crea durante el intercambio del archivo.

El mandato BNU **rmail** notifica la llegada de un archivo al destinatario.

**Nota:** Para enviar un archivo a un usuario de un sistema *local*, entre el mandato **uuto** e incluya el archivo que deba enviarse, el destino del sistema local y el usuario del destino local. Por ejemplo:

```
uuto /home/bin/archivo2 near!nestor
```

Esta operación envía *archivo2* desde el directorio local */home/bin* al usuario *nick* del sistema local *near*.

## **Recepción de archivos**

Para recibir y gestionar archivos, los sistemas remitente y destinatario deben ejecutar los Programas de utilidad básicos de red (BNU) o alguna versión de UNIX-to-UNIX Copy Program (UUCP).

Para recibir y manipular archivos enviados con el mandato **uuto**, utilice el mandato **uupick**. Éste tiene opciones de manejo de archivos que permiten al destinatario localizar los archivos enviados, mover los archivos a un directorio especificado, ejecutar mandatos o suprimir archivos.

### **Recepción de un archivo con el mandato uupick**

Utilice el mandato **uupick** para recibir un archivo.

Por ejemplo:

```
uupick
```

El mandato **uupick** busca en el directorio público los archivos que incluyan el ID del usuario remoto en los nombres de vía de acceso. A continuación, el mandato **uupick** visualiza un mensaje parecido a éste en la pantalla remota:

```
from system base: archivo archivo1?
```

El ? (signo de interrogación) de la segunda línea del aviso solicita al destinatario que utilice cualquiera de las opciones de **uupick** para manejar archivos en el directorio público BNU.

Para obtener una lista de todas las opciones disponibles, escriba un asterisco (\*) en la línea situada bajo el indicador de signo de interrogación (?). Las opciones para salir, guardar y visualizar son las siguientes:

<b>Item</b>	<b>Descripción</b>
<b>p</b>	Visualiza el contenido del archivo.
<b>m [Directorio]</b>	Guarda el archivo en el directorio especificado mediante la variable <i>[Directorio]</i> . Si no se especifica destino alguno con la opción <b>m</b> , el archivo pasará al directorio de trabajo actual.
<b>q</b>	Abandona el proceso de gestión de archivos <b>uupick</b> (sale del mismo).

## **Codificación y decodificación de archivos para transferirlos**

Utilice los mandatos **uuencode** y **uudecode** si desea preparar archivos para su transmisión por módem.

Los mandatos funcionan uno tras otro. El mandato **uuencode** transforma los archivos binarios en archivos ASCII. Posteriormente, estos archivos se pueden enviar a un sistema remoto mediante el recurso de correo.

Con el mandato **uudecode**, el usuario convierte los archivos codificados en ASCII al formato binario.

## **Informes sobre el estado de intercambios de mandatos y archivos**

Es posible visualizar los informes sobre el estado de los intercambios de archivos utilizando los mandatos **uusnap**, **uuq** y **uustat**.

### **Visualización del estado de los sistemas conectados mediante BNU**

El mandato **uusnap** visualiza una tabla de información sobre todos los sistemas conectados mediante BNU.

La tabla muestra una línea para cada sistema, en la que figuran los nombres y números de archivos de mandatos, archivos de datos y ejecuciones de mandatos remotos que se encuentran en las colas de los sistemas. El último elemento de cada línea es un mensaje de estado. Este mensaje indica una conexión BNU satisfactoria o una explicación de la razón por la cual BNU no ha establecido un enlace.

Consulte el mandato **uusnap**.

### **Visualización de la cola de trabajos de BNU**

El mandato **uuq** lista todas las entradas de la cola de trabajos BNU.

El formato de la lista es similar al formato que muestra el mandato **ls**. Cada entrada incluye el número de trabajo, seguido en la misma línea por un resumen en el que consta el nombre del sistema, el número de trabajos del sistema y el número total de bytes a enviar. Los usuarios con autorización root pueden utilizar el mandato **uuq** para identificar trabajos en cola específicos mediante sus números de trabajo.

### Estado de las operaciones BNU

El mandato **uustat** facilita el estado de un determinado intercambio de archivo o mandato en el sistema BNU.

Especificado sin ninguna opción de distintivo, el mandato **uustat** visualiza una sola línea para cada trabajo solicitado por el usuario actual, en la que se incluye:

- Número de ID de trabajo
- Fecha y hora
- Estado (enviado o recibido)
- El nombre del sistema
- ID de usuario de la persona que ha emitido el mandato
- Tamaño y nombre del archivo de trabajo

Dotado de varios distintivos, el mandato **uustat** puede informar de todos los trabajos de la cola, de todos los usuarios, o sólo de los trabajos solicitados por otros sistemas de la red.

El mandato **uustat** proporciona a los usuarios un control limitado de los trabajos en cola para ejecutarlos en un sistema remoto. Es posible examinar el estado de las conexiones BNU con otros sistemas y hacer un seguimiento de los intercambios de archivos y mandatos. Por ejemplo, el usuario puede cancelar las peticiones de copia iniciadas mediante el mandato **uucp**.

Consulte el mandato **uustat**.

## Intercambio de mandatos entre sistemas locales y remotos

Los Programas de utilidad básicos de red (BNU) permiten a los usuarios intercambiar mandatos entre sistemas locales y remotos.

El mandato **uux** ejecuta mandatos en un sistema remoto. El mandato **uupoll** controla la sincronización de la ejecución de los mandatos.

### Peticiones de ejecución de mandatos en un sistema remoto

Utilice el mandato **uux** para solicitar la ejecución de un mandato en un sistema remoto.

El mandato **uux** no ejecuta los mandatos en el sistema remoto. En lugar de ello, prepara los archivos de datos y control necesarios en `/var/spool/uucp`. Para realizar la transferencia, se invoca el daemon **uucico**. Cuando la transferencia se ha completado, el daemon **uucico** del sistema remoto crea un archivo ejecutable en el directorio de spool.

Cuando los dos daemons **uucico** se ponen de acuerdo para quedarse en suspenso, el daemon **uuxt** explora el directorio de spool en busca de peticiones de ejecución pendientes, verifica los permisos y comprueba si se necesita información adicional. A continuación inicia un mandato para que lleve a cabo la acción solicitada.

**Nota:** Puede utilizar el mandato **uux** en cualquier sistema configurado para ejecutar un mandato determinado. Sin embargo, y por motivos de seguridad, las normas de algunos emplazamientos puede que limiten el uso de ciertos mandatos. Por ejemplo, es posible que en algunos emplazamientos sólo se permita la ejecución del mandato **mail**.

Una vez recibidos los archivos en el sistema remoto, el daemon **uuxqt** ejecuta el mandato especificado en dicho sistema. El daemon **uuxqt** explora periódicamente el directorio de spool público del sistema remoto en busca de archivos recibidos en transmisiones de **uux**. El daemon **uuxqt** comprueba que los datos a los que deben acceder los archivos enviados estén en el sistema remoto. También verifica que el sistema remitente disponga de permiso para acceder a los datos. A continuación, el daemon **uuxqt** ejecuta el mandato o notifica al sistema remitente que éste no se ha ejecutado.

## Supervisión de una conexión remota de BNU

Utilice el procedimiento siguiente para supervisar una conexión remota de BNU.

- El programa BNU debe estar instalado en el sistema.
- Debe haber configurado un enlace (por cable, por módem o TCP/IP) entre su sistema y el sistema remoto.
- Los archivos de configuración de BNU, incluidos el archivo `Systems`, el archivo `Permissions`, el archivo `Devices` y el archivo `Dialers` (y el archivo `Sysfiles`, si es aplicable), deben estar configurados para las comunicaciones entre su sistema y el sistema remoto.

**Nota:** Debe tener autorización de usuario root para modificar los archivos de configuración de BNU.

El mandato **Uutry** puede ayudar a supervisar el proceso del daemon **uucico** si los usuarios de su sitio informan de problemas de transferencia de archivos.

1. Emite el mandato **uustat** para determinar el estado de todos los trabajos de transferencia de la cola actual, como a continuación:

```
uustat -q
```

El sistema muestra un informe sobre el estado, similar al siguiente:

```
venus 3C (2) 05/09-11:02 NO PUEDE ACCEDER AL DISPOSITIVO  
hera 1C 05/09-11:12 SATISFACTORIO  
merlin 2C 5/09-10:54 NO HAY DISPOSITIVOS DISPONIBLES
```

Este informe indica que tres archivos de mandatos (C.\*) destinados al sistema remoto venus han estado en la cola durante dos días. Las razones de este retraso podrían ser diversas. Por ejemplo, es posible que el sistema venus haya estado desconectado para el mantenimiento o que el módem haya estado apagado.

2. Antes de realizar actividades de resolución de problemas de mayor envergadura, emita el mandato **Uutry** de la forma siguiente, para determinar si el sistema local puede contactar con el sistema venus ahora:

```
/usr/sbin/uucp/Uutry -r venus
```

Este mandato inicia el daemon **uucico** con una cantidad de depuración moderada y la instrucción de alterar temporalmente el tiempo de reintento por omisión. El mandato **Uutry** dirige la salida de depuración a un archivo temporal, `/tmp/venus`.

3. Si el sistema local logra establecer una conexión con el sistema venus, la salida de depuración contendrá bastante información. Sin embargo, la línea final de este script, que se muestra a continuación, es la más importante:

```
Conversation Complete: Status SUCCEEDED
```

Si la conexión es satisfactoria, puede suponer que se trataba de problemas temporales de transferencia de archivos que ahora se han solucionado. Emite el mandato **uustat** de nuevo para asegurarse de que los archivos del directorio de spooling se hayan transferido satisfactoriamente al sistema remoto. En caso contrario, siga los pasos del apartado “[Supervisión de una transferencia de archivos BNU](#)” en la página 544 para comprobar si ha habido problemas de transferencia de archivos entre el sistema y el sistema remoto.

4. Si el sistema local no puede contactar con el sistema remoto, la salida de depuración que el mandato **Uutry** genera contendrá el tipo de información siguiente (la forma exacta de la salida puede variar):

```
mchFind called (venus)  
conn (venus)  
getto ret -1  
Call Failed: CAN'T ACCESS DEVICE  
exit code 101  
Conversation Complete: Status FAILED
```

En primer lugar, compruebe las conexiones físicas entre el sistema local y el remoto. Asegúrese de que el sistema remoto esté encendido y de que todos los cables están conectados correctamente, que los puertos estén habilitados o inhabilitados (tal como sea necesario) en ambos sistemas y que los módems estén en funcionamiento (si es aplicable).

Si las conexiones físicas son correctas y seguras, verifique todos los archivos de configuración relevantes tanto en el sistema local como en el sistema remoto, incluidos los siguientes:

- Asegúrese de que las entradas de los archivos Devices, Systems y Permissions (y el archivo Sysfiles, si es aplicable) del directorio **/etc/uucp** sean correctas en los dos sistemas.
- Si utiliza un módem, asegúrese de que el archivo /etc/uucp/Dialers (o un archivo alternativo que haya especificado en **/etc/uucp/Sysfiles**) contenga la entrada correcta. Si utiliza abreviaturas de códigos de marcación, asegúrese de que las abreviaturas estén definidas en el archivo /etc/uucp/Dialcodes.
- Si utiliza una conexión TCP/IP, asegúrese de que el daemon **uucpd** pueda ejecutarse en el sistema remoto y de que los archivos de configuración contengan las entradas de TCP correctas.

## 5. Después de haber comprobado las conexiones físicas y los archivos de configuración, vuelva a emitir el mandato **Uutry**.

Si la salida de depuración sigue indicando que la conexión ha fallado, es posible que necesite ponerse en contacto con un miembro del equipo de soporte de su sistema. Guarde la salida de depuración que el mandato **Uutry** haya generado. Esto podría resultar útil para diagnosticar el problema.

### Transferencia de un archivo a un sistema remoto para imprimirla

Utilice el mandato **uux** si desea transferir un archivo a un sistema remoto para imprimirla.

Para transferir un archivo a un sistema remoto para su impresión, deben satisfacerse los requisitos previos siguientes:

- Se debe establecer una conexión de los Programas de utilidad básicos de red (BNU) con el sistema remoto
- Debe tener permiso para ejecutar operaciones en el sistema remoto

Escriba lo siguiente en la línea de mandatos del sistema local:

```
uux remote!:/usr/bin/lpr local!nombatch
```

Se imprimirá el archivo local *nombatch* en el sistema remoto.

### Supervisión de una transferencia de archivos BNU

Utilice este procedimiento para supervisar una transferencia de archivo a un sistema remoto.

- El programa BNU debe estar instalado en su sistema y estar configurado para el mismo.
- Establezca una conexión con un sistema remoto siguiendo los pasos que se indican en el apartado “[Supervisión de una conexión remota de BNU](#)” en la página 543.

La supervisión de una transferencia de archivos resulta útil cuando las transferencias de archivos al sistema remoto fallan por alguna razón que se desconoce. La información de depuración que genera el daemon **uucico** (al que llama el mandato **Uutry**) puede ayudarlo a averiguar qué es lo que no funciona correctamente.

El mandato **Uutry** permite supervisar las transferencias de archivos, de la forma siguiente:

## 1. Prepare un archivo para la transferencia utilizando el mandato **uucp** con el distintivo **-r** escribiendo lo siguiente:

```
uucp -r test1 venus!~/test2
```

El distintivo **-r** indica al programa UUCP que debe crear y poner en cola todos los archivos de transferencia necesarios pero que *no* debe iniciar el daemon **uucico**.

## 2. Emite el mandato **Uutry** con el distintivo **-r** para iniciar el daemon **uucico** con la depuración activada, escribiendo lo siguiente:

```
/usr/sbin/uucp/Uutry -r venus
```

Esto indica al daemon **uucico** que debe contactar con el sistema remoto venus y alterar temporalmente el tiempo de reintento por omisión. El daemon contacta con el sistema venus, inicia la sesión y transfiere el archivo, mientras que el mandato **Uutry** genera salida de depuración que permite supervisar el proceso **uucico**. Pulse la secuencia de teclas de interrupción para detener la salida de depuración y volver al indicador de mandatos.

El mandato **Uutry** también almacena la salida de depuración en el archivo `/tmp/NombreSistema`. Si sale de la salida de depuración antes de que la conexión haya finalizado, puede desplazarse por el archivo de salida para ver el resultado de la conexión.

### Trasmisiones de trabajos en spool

Utilice el mandato **uupoll** para iniciar la transmisión de trabajos almacenados en el directorio de spooling público del sistema local.

El mandato **uupoll** crea un trabajo nulo en el directorio público para el sistema remoto e inicia el daemon **uucico**. Esto hace que el daemon **uucico** se ponga inmediatamente en contacto con el sistema remoto y transfiera los trabajos que están en la cola.

### Identificación de sistemas compatibles

Utilice el mandato **uname** para visualizar una lista de todos los sistemas a los que puede acceder el sistema local.

Por ejemplo, si escribe:

```
uname
```

en la línea de mandatos, el sistema muestra una lista como ésta:

```
arturo  
isabel  
neptuno  
zeus
```

Esta información se utiliza para determinar el nombre de un sistema accesible antes de copiar un archivo en él. El mandato **uname** también se utiliza para establecer la identidad del sistema local. El mandato **uname** obtiene la información leyendo el archivo `/etc/uucp/systems`.

### Comunicación con los sistemas UNIX conectados utilizando el mandato tip

Utilice el mandato **tip** para contactar con un sistema conectado que utilice el sistema operativo UNIX.

El mandato **tip** se instala con los Programas de utilidad básicos de red (Basic Networking Utilities - BNU) y puede utilizar las mismas conexiones asíncronas que utilice BNU.

El mandato **tip** utiliza variables y señales de escape, así como distintivos, para controlar sus operaciones. Los distintivos pueden utilizarse en la línea de mandatos. Las señales de escape pueden utilizarse a través de una conexión con un sistema remoto para iniciar y detener las transferencias de archivos, cambiar la dirección de una transferencia de archivos y salir de un subshell.

### Variables del mandato tip

Las variables del mandato **tip** definen valores como, por ejemplo, el carácter de fin de línea, la señal de interrupción y la modalidad de la transferencia de archivos.

Los valores de las variables pueden inicializarse durante la ejecución utilizando un archivo `.tiprc`. Los valores de las variables también pueden modificarse durante la ejecución utilizando la señal de escape `~s`. Algunas variables como, por ejemplo, el carácter de fin de línea, pueden establecerse para un sistema individual en la entrada del sistema del archivo `remote`.

El mandato **tip** lee tres archivos, el archivo `phones`, el archivo `remote` y el archivo `.tiprc`, para determinar los valores iniciales para sus variables. El archivo `.tiprc` siempre debe estar en el directorio inicial del usuario. Los nombres y las ubicaciones de los archivos `remote` y `phones` pueden variar. Los nombres del archivo `remote` y del archivo `phones` pueden determinarlos las variables de entorno:

<b>Item</b>	<b>Descripción</b>
PHONES	Especifica el nombre del archivo telefónico del usuario. El archivo puede tener cualquier nombre de archivo válido y debe configurarse en el formato del archivo /usr/lib/phones-file. El archivo por omisión es etc/phones. Si se especifica un archivo con la variable PHONES, éste se utiliza en lugar del archivo /etc/phones (no además del mismo).
REMOTE	Especifica el nombre del archivo de definiciones del sistema remoto del usuario. El archivo puede tener cualquier nombre de archivo válido y debe configurarse en el formato del archivo /usr/lib/remote-file. El archivo por omisión es /etc/remote. Si se especifica un archivo con la variable REMOTE, éste se utiliza en lugar del archivo /etc/remote (no además del mismo).

Para utilizar una variable de entorno, establezcala antes de iniciar el mandato **tip**. Como alternativa, los nombres de los archivos phones y remote pueden determinarse utilizando, respectivamente, la variable phones y la variable remote del mandato **tip**, en el archivo .tiprc.

**Nota:** El mandato **tip** sólo lee el *último* archivo remote o phones especificado. Así pues, si se especifica un archivo remote o phones con una variable, el nuevo archivo se utiliza en lugar de (no además de) los archivos anteriores que se hayan especificado.

El mandato **tip** utiliza los valores de las variables en el orden siguiente:

1. El mandato comprueba los valores de las variables de entorno PHONES y REMOTE para los archivos que deben utilizarse como archivos phones y remote.
2. El mandato lee el archivo .tiprc y establece todas las variables de la forma correspondiente. Si la variable phones o remote está establecida en el archivo .tiprc, este valor altera temporalmente el valor de la variable de entorno.
3. Cuando se inicia una conexión con un sistema remoto, el mandato lee la entrada del archivo remote para dicho sistema. Los valores de la entrada del archivo remote alteran temporalmente los valores del archivo .tiprc.
4. Si el distintivo - BaudRate se utiliza con el mandato **tip**, la velocidad especificada altera temporalmente todos los valores previos de la velocidad en baudios.
5. Un valor efectuado con la señal de escape ~s altera temporalmente todos los valores anteriores de una variable.

**Nota:** Cualquier usuario de **tip** puede crear un archivo .tiprc y utilizarlo para especificar los valores iniciales de las variables de **tip**. El archivo .tiprc debe colocarse en el directorio \$HOME del usuario.

#### **Archivos de configuración del mandato tip**

Antes de que el mandato **tip** pueda conectarse a un sistema remoto, deben establecerse los archivos /etc/remote y /etc/phones.

<b>Item</b>	<b>Descripción</b>
/etc/remote	Define atributos de los sistemas remotos como, por ejemplo, el puerto y el tipo de dispositivo que debe utilizarse para conectar con el sistema, así como las señales que deben utilizarse para indicar el inicio y el final de las transmisiones.
/etc/phones	Lista los números de teléfono para contactar con sistemas remotos a través de una línea de módem.

En el paquete bos.net.uucp se proporcionan los archivos de ejemplo remote y phones. El archivo de ejemplo remote se denomina /usr/lib/remote-file. El archivo de ejemplo phones se denomina /usr/lib/phones-file. Copie /usr/lib/remote-file en /etc/remote y modifique /etc/remote. Para establecer uno de estos archivos, copie un archivo de ejemplo en el nombre correcto y modifíquelo para que satisfaga las necesidades de su sitio.

Un usuario **tip** también puede crear archivos remote y phones personalizados. Un archivo remote individual debe seguir el formato del archivo /usr/lib/remote-file y especificarse con la variable remote o la variable de entorno REMOTE. Un archivo phones individual debe seguir el formato del

archivo /usr/lib/phones-file y especificarse con la variable phones o la variable de entorno PHONES. Si un archivo phones o remote individual se especifica con una de las variables, este archivo se leerá en lugar del archivo /etc/phones o /etc/remote (no además del mismo).

Los usuarios de **tip** pueden utilizar combinaciones de archivos phones y remote individuales. Por ejemplo, un usuario podría utilizar el archivo remote por omisión, /etc/remote, pero utilizar un archivo phones individual denominado con la variable phones.

### Cancelación de trabajos remotos

Utilice el mandato **uustat** para cancelar un proceso BNU emitido para un sistema remoto.

Para cancelar un trabajo remoto, deben satisfacerse los requisitos previos siguientes:

- Se debe establecer una conexión de los Programas de utilidad básicos de red (BNU) con el sistema remoto de destino
- Se debe haber emitido un trabajo remoto desde el sistema local

1. Determine el número de ID de trabajo del proceso, en cual figura en la lista de la cola remota. Escriba lo siguiente en la línea de mandatos del sistema local:

```
uustat -a
```

La opción **-a** visualiza todos los trabajos de la cola del sistema remoto y las peticiones de trabajos de cualquier otro usuario BNU del sistema.

BNU responde con un mensaje parecido a éste:

```
heraC3113 11/06-17:47 S hera you 289 D.venus471af8d  
merlinC3119 11/06-17:49 S merlin jane 338 D.venus471bc0a
```

2. A continuación, escriba:

```
uustat -k heraC3113
```

La opción **-k** cancela la petición de trabajo heraC3113.

## Resolución de problemas en BNU

Los mensajes de error de BNU pueden vincularse a una fase en concreto del flujo de la conversación. Utilice el "Diagrama de flujo de la conversación de BNU" y las descripciones de los errores siguientes para el diagnóstico de problemas con BNU.

Es posible que BNU no envíe algunos de los mensajes siguientes, pero se incluyen en caso de que se utilice otra versión de UUCP.

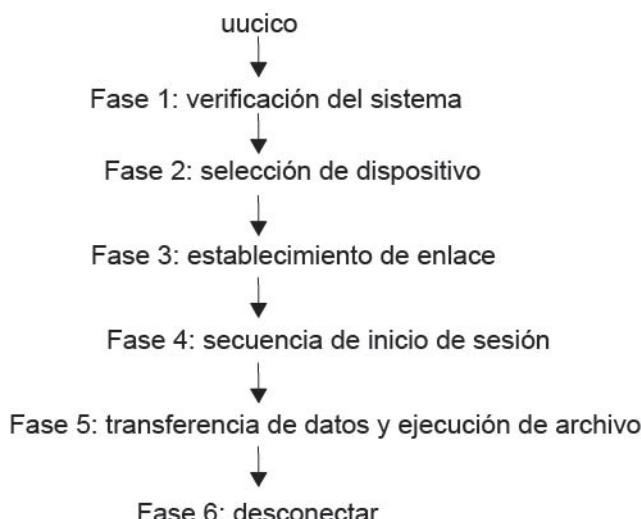


Figura 26. Diagrama de flujo de la conversación de BNU

Esta ilustración muestra el flujo y las diferentes fases de la conversión de BNU. Desde uucico en la parte superior, los datos se pasan a la Fase 1-Verificación del sistema, luego a la Fase 2-Selección de dispositivo y a la Fase 3-Establecimiento de enlace, luego a la Fase 4-Secuencia de inicio de sesión, a continuación a la Fase 5-Transferencia de datos y Ejecución de archivos y finalmente a la Fase 6-Desconexión.

### Mensajes de estado de BNU FASE 1

Existen cinco mensajes de estado en BNU FASE 1. Se describen en la tabla siguiente.

Item	Descripción
Error de declaración	La unidad del sistema local tiene problemas. Compruebe las causas posibles en el informe de errores emitiendo el mandato <code>erprt -a   pg</code> .
El sistema no está en Systems	Si ha proporcionado un nombre de sistema remoto que no se encuentra en los archivos Systems se creará este mensaje de estado y BNU finalizará. Utilice el mandato <b>uname</b> para volver a comprobar el nombre del sistema.
Hora de llamada equivocada	El archivo Systems tiene restricciones sobre las horas en que permite llamadas de salida. BNU intentará probando hasta que sea la hora correcta. Compruebe el archivo Systems.
Devolución de llamada requerida	La red tiene un uso restringido, por motivos de seguridad o económicos y en este momento se deniega el acceso.
No se puede llamar. No ha llamado	Estos errores significan que BNU recientemente ha intentado llamar al sistema remoto y no lo ha conseguido. No volverá a intentarlo de forma inmediata. También pueden deberse a que un archivo de estado del sistema antiguo esté retenido y ello impida que el daemon <b>uucico</b> vuelva a intentarlo.

### Mensajes de estado de BNU FASE 2

Existen cuatro mensajes de estado en BNU FASE 2. Se describen en la tabla siguiente.

Item	Descripción
Ha fallado el script del dialer	El script del archivo Dialers no ha finalizado satisfactoriamente.
No hay ningún dispositivo disponible. No se puede acceder al dispositivo	El módem o la línea telefónica de salida del sistema están ocupados. Compruebe si hay algún error en la entrada del dispositivo del archivo Systems. Además, compruebe los archivos Devices y Dialers para estar seguro de que los dispositivos lógicos tengan asociados dispositivos físicos. Es posible que el archivo /etc/uucp/Sysfiles especifique un archivo Systems, Devices o Dialers alternativo que no esté configurado correctamente. ¿Algún otro programa está utilizando el dispositivo? Compruebe si existe algún bloqueo sobre el puerto en el directorio /var/locks. Si existe un archivo de bloqueos (por ejemplo, LCK..TTY0), compruebe si el proceso identificado mediante el número del archivo de bloqueos todavía está activo. En caso contrario, puede eliminarlo (por ejemplo, rm /var/locks/LCK..TTY0). Compruebe también los permisos sobre el puerto.

Item	Descripción
Ha fallado la marcación Ha fallado (la llamada al sistema)	Estos errores aparecen cuando el sistema marca a otro satisfactoriamente pero el otro sistema no contesta. También puede indicar un problema en los archivos Devices. Escriba el mandato <b>uucico -r1 -x6 -s nombreSistema</b> . Es posible que BNU esté esperando alguna serie que no recibe. Efectúe la conexión manualmente para averiguar qué debe incorporarse en la entrada de los archivos Systems para satisfacer la petición. Tenga en cuenta la "temporización"; quizás sean necesarios algunos retardos en la serie de marcación del módem. Esto también podría significar que el puerto está ocupado, que ha marcado un número incorrecto o que BNU ha perdido la propiedad sobre el puerto.
OK Marcación automática	Se trata de mensajes meramente informativos y no indican ningún error.

#### Mensajes de estado de BNU FASE 3

Existen cinco mensajes de estado en BNU FASE 3. Se describen en la tabla siguiente.

Item	Descripción
Reconocimiento fallido (bloqueo)	El dispositivo se está utilizando; el proceso no ha podido crear el archivo LCK. En ocasiones, el administrador debe eliminar los archivos LCK manualmente. Después de unos cuantos reintentos, consulte al administrador del sistema. Vea si otro proceso tiene el control del puerto (por ejemplo, otra instancia del daemon <b>uucico</b> ).
Ha fallado el inicio de sesión	El inicio de sesión ha fallado debido a una conexión defectuosa o posiblemente a una máquina lenta.
Tiempo de espera excedido	El sistema remoto no ha respondido dentro del período de tiempo establecido. Esto también podría indicar un problema con el script de chat.
Satisfactoria (Llamada al sistema)	La llamada ha finalizado.
BNU (continuación)	Se trata de mensajes meramente informativos y no indican ningún error.

#### Mensajes de estado de BNU FASE 4

Existen seis mensajes de estado en BNU FASE 4. Se describen en la tabla siguiente.

Item	Descripción
El arranque ha fallado Remoto rechazado después del inicio de sesión	Después de iniciar la sesión, el daemon <b>uucico</b> se inicia en el sistema remoto. Si ocurre algún problema al iniciar una conversación entre los dos sistemas, se crean estos mensajes. También es posible que haya iniciado la sesión en la cuenta de BNU incorrecta o que el reconocimiento inicial haya fallado.
Nombre de máquina incorrecto	Se ha llamado a una máquina de forma incorrecta o el nombre de la máquina se ha cambiado.
Combinación de inicio de sesión/máquina errónea	El inicio de sesión con el sistema remoto ha fallado. El problema puede deberse a un número de teléfono incorrecto, a un inicio de sesión o una contraseña incorrectos o a un error en el script de chat.
Remoto tiene un archivo de bloqueo para mí	Ambos sistemas estaban intentado llamarse el uno al otro de forma simultánea. La petición local fallará temporalmente.

Item	Descripción
OK Hablando	Se trata de mensajes meramente informativos y no indican ningún error.
INICIO DE SESIÓN: CONTRASEÑA:	<p>Si la solicitud de inicio de sesión o de contraseña aparece todo en mayúsculas, es posible que el módem esté en modalidad de eco (E1 en los compatibles con Hayes). Esto hace que el módem devuelva el eco o envíe un RING al sistema cuando se reciba una llamada de entrada. El mandato <b>getty</b> recibe la serie y correspondientemente cambia el inicio de sesión: o la contraseña: a todo mayúsculas. Cambie la modalidad de eco del módem a desactivado (utilice ATE0 para los compatibles con Hayes).</p> <p><b>Nota:</b> Tenga en cuenta que una vez realizada esta modificación, deberá utilizar ATE1 en el script de chat de los archivos Dialers o el módem no devolverá el OK esperado.</p> <p>Si en el puerto remoto se ha establecido delay o getty -r y el script de chat espera entrada clave, los puertos en los que se haya establecido delay esperarán uno o más retornos de carro antes de proseguir con el inicio de sesión. Intente empezar el script de chat en el sistema de marcación con lo siguiente:</p> <pre>" " \r\d\r\d\r\d\r in:--in: ...</pre> <p>La interpretación de este script de chat sería la siguiente: no se espera nada, enviar retorno, retardo, retorno, retardo, retorno, retardo, retorno.</p>

#### Mensajes de estado de BNU FASE 5

Existen cinco mensajes de estado en BNU FASE 5. Se describen en la tabla siguiente.

Item	Descripción
Alarma	El daemon <b>uucico</b> tiene problemas con la conexión. La conexión no es satisfactoria o "xon/xoff" se ha establecido en sí en el módem.
Acceso remoto a vía/ archivo denegado copia (fallido)	Este mensaje indica un problema de permiso; compruebe los permisos del archivo y de la vía de acceso.
Lectura errónea	El sistema remoto se ha quedado sin espacio, probablemente en el área de spool o el daemon <b>uucico</b> no ha podido leer o grabar en el dispositivo.
Ha fallado la conversación	Se ha perdido la detección de la portadora del módem. Posiblemente el módem estaba apagado, el cable estaba suelto o desconectado o el sistema remoto estaba apagado o colgado. Una desconexión del teléfono también podría provocar este error.
Solicitado Copia (satisfactoria)	Se trata de mensajes meramente informativos y no indican ningún error.

#### Mensajes de estado de BNU FASE 6

Existen dos mensajes de estado en BNU FASE 6. Se describen en la tabla siguiente.

Item	Descripción
OK (Conversación finalizada)	El sistema remoto puede denegar la petición de colgar e invertir las funciones (lo que significa que el sistema remoto tiene trabajo que el sistema local debe realizar). Una vez los dos daemons <b>uucico</b> acuerdan que no existe más trabajo, cuelgan.
Conversación satisfactoria	Se trata de un mensaje meramente informativo y no indica ningún error.

### Depuración de anomalías de inicio de sesión de BNU utilizando el daemon **uucico**

Utilice el daemon **uucico** para depurar las anomalías de inicio de sesión de BNU.

- BNU debe estar instalado en el sistema.
- Debe haber configurado un enlace (por cable, por módem o TCP/IP) entre su sistema y el sistema remoto.
- Los archivos de configuración de BNU, incluidos el archivo Sysfiles (si es aplicable), el archivo Systems, el archivo Permissions, el archivo Devices y el archivo Dialers deben estar configurados para la comunicación entre su sistema y el sistema remoto.

**Nota:** Debe tener autorización de usuario root para modificar los archivos de configuración de BNU.

- Debe tener autorización de usuario root para invocar el daemon **uucico** en modalidad de depuración.

1. Para generar información de depuración sobre una conexión de un sistema local a uno remoto que no funcione, inicie el daemon **uucico** con el distintivo **-x**, de la forma siguiente:

```
/usr/sbin/uucp/uucico -r 1 -s venus -x 9
```

donde **-r 1** especifica la modalidad maestra, o de quien realiza la llamada; **-s venus** el nombre del sistema remoto con el que intenta conectarse y **-x 9** el nivel de depuración que genera la información de depuración más detallada.

2. Si la entrada expect-send sequence de un archivo Systems con el formato /etc/uucp/Systems es la siguiente:

```
venus Any venus 1200 - "" \n in:--in: uucp1 word:  
mirror
```

el daemon **uucico** conecta el sistema local al sistema remoto venus. La salida de depuración será similar a la siguiente:

```
expect: ""  
got it  
sendthem (^J^M)  
expect (in:)^  
M^JLogin:got it  
sendthem (uucp1^M)  
expect (word:)^  
M^JPassword:got it  
sendthem (mirror^M)  
imsg >^M^J^PShere^@Login Successful: System=venus
```

donde:

Item	Descripción
expect: ""	Especifica que el sistema local no esperará ninguna información del sistema remoto.
got it	Reconoce que el mensaje se ha recibido.
sendthem (^J^M)	Especifica que el sistema local enviará al sistema remoto un retorno de carro y una línea nueva.

<b>Item</b>	<b>Descripción</b>
expect (in:)	Especifica que el sistema local espera recibir la solicitud de inicio de sesión del sistema remoto, que finaliza con la serie de caracteres in:.
^M^Jlogin:got it	Confirma que el sistema local ha recibido la solicitud de inicio de sesión remota.
sendthem (uucp1^M)	Especifica que el sistema local enviará el ID de inicio de sesión uucp1 al sistema remoto.
expect (word:)	Especifica que el sistema local espera recibir la solicitud de contraseña del sistema remoto, que finaliza con la serie de caracteres word:.
^M^JPassword:got it	Confirma que el sistema local ha recibido la solicitud de contraseña remota.
sendthem (mirror^M)	Especifica que el sistema local enviará la contraseña para el ID de inicio de sesión uucp1 al sistema remoto.
imsg >^M^J^PShere^@Login Successful: System=venus	Confirma que el sistema local ha iniciado la sesión satisfactoriamente en el sistema remoto venus.

**Nota:**

1. La salida de depuración de envío esperado (expect-send) que el mandato **uucico** genera puede proceder de la información del archivo /etc/uucp/Dialers o de la información del archivo /etc/uucp/Systems. La información acerca de la comunicación con el módem procede del archivo Dialers, mientras que la información acerca de la comunicación con el sistema remoto procede del archivo Systems. (Fíjese en que /etc/uucp/Systems y /etc/uucp/Dialers son los archivos de configuración de BNU por omisión. Es posible especificar otros archivos en /etc/uucp/Sysfiles que satisfagan las mismas funciones.)
2. Para configurar una conexión con un sistema remoto, debe estar familiarizado con la secuencia de inicio de sesión de dicho sistema.

## SNMP para gestión de red

El recurso de Gestión de red proporciona la gestión completa de redes de sistemas mediante el uso del **Protocolo simple de gestión de red (SNMP)**, permitiendo que los sistemas principales de red intercambien información de gestión.

**SNMP** es un protocolo de gestión entre redes diseñado para utilizarse con internets basadas en **TCP/IP**.

Cuando está instalado el sistema operativo AIX, la versión no cifrada de **SNMPv3** se instala de forma predeterminada y se inicia en el arranque del sistema. Si tiene sus propias comunidades, rupturas y entradas SMUX configuradas en el archivo /etc/snmpd.conf, necesitará migrarlas manualmente al archivo /etc/snmpd3.conf. Para obtener información sobre cómo migrar las comunidades, consulte el apartado “[Migración desde SNMPv1 hasta SNMPv3](#)” en la página 562.

Es posible que también desee consultar la información en el apartado [SNMP Overview for Programmers](#) de la publicación *Communications Programming Concepts*.

La gestión de red **SNMP** se basa en el modelo familiar de cliente/servidor que se utiliza ampliamente en aplicaciones de red basadas en **TCP/IP**. Cada sistema principal que se debe gestionar ejecuta un proceso denominado *agente*. El agente es un proceso de servidor que mantiene la base de datos MIB (Management Information Base) para el sistema principal. Los sistemas principales que están implicados en la toma de decisiones de gestión de red pueden ejecutar un proceso denominado *gestor*. Un *gestor* es una aplicación cliente que genera peticiones de información MIB y procesa las respuestas. Además, un *gestor* puede enviar peticiones a servidores de agente para modificar la información de MIB.

**SNMP** de AIX proporciona soporte para las RFC siguientes:

Item	Descripción
<b>RFC 1155</b>	Estructura e identificación de información de gestión para internets basadas en <b>TCP/IP</b>
<b>RFC 1157</b>	Un <b>Protocolo simple de gestión de red (SNMP)</b>
<b>RFC 1213</b>	Management Information Base para gestión de red de internets basadas en <b>TCP/IP</b> : MIB-II
<b>RFC 1227</b>	Protocolo SMUX (Single multiplexer - Multiplexor individual) y MIB (Management Information Base) de <b>Simple Network Management Protocol (SNMP)</b>
<b>RFC 1229</b>	Extensiones a la interfaz genérica Management Information Base (MIB)
<b>RFC 1231</b>	Management Information Base (MIB) de Red en anillo IEEE 802.5
<b>RFC 1398</b>	Definiciones de objetos gestionados para los tipos de interfaz similares a Ethernet
<b>RFC 1512</b>	Management Information Base FDDI
<b>RFC 1514</b>	MIB de recursos de sistema principal
<b>RFC 1592</b>	<b>Simple Network Management Protocol</b> -Distributed Program Interface Versión 2
<b>RFC 1905</b>	Operaciones de protocolo para la Versión 2 de Simple Network Management Protocol (SNMPv2)
<b>RFC 1907</b>	Management Information Base para la Versión 2 de Simple Network Management Protocol (SNMPv2)
<b>RFC 2572</b>	Proceso y despacho de mensajes para <b>Simple Network Management Protocol (SNMP)</b>
<b>RFC 2573</b>	Aplicaciones <b>SNMP</b>
<b>RFC 2574</b>	USM (Modelo de seguridad basado en usuario) para la versión 3 de <b>Simple Network Management Protocol (SNMPv3)</b>
<b>RFC 2575</b>	VACM (Modelo de control de acceso basado en vista) para <b>Simple Network Management Protocol (SNMP)</b>

### **SNMPv3**

En versiones anteriores del sistema operativo AIX, **SNMPv1** era la única versión disponible de **SNMP** para AIX. **SNMPv3**, que se proporciona en el sistema operativo AIX, proporciona una infraestructura potente y flexible para la seguridad de mensajes y el control de acceso.

La información de este apartado se aplica sólo a **SNMPv3**.

La seguridad de mensajes implica que se proporcione lo siguiente:

- Comprobación de integridad de datos para asegurar que los datos no se ha modificado en tránsito.
- Verificación de origen de datos para asegurar que la petición o la respuesta procede del origen que indica que procede.
- Comprobación de puntualidad de mensajes y, opcionalmente, confidencialidad de datos para protegerlos de las intrusiones.

La arquitectura de **SNMPv3** introduce el USM (User-based Security Model - Modelo de seguridad basado en usuario) para la seguridad de mensajes y el VACM (View-based Access Control Model - Modelo de control de acceso basado en vista) para el control de acceso. La arquitectura soporta el uso simultáneo de diferentes modelos de seguridad, control de acceso y proceso de mensajes. Por ejemplo, si lo desea puede utilizar la seguridad basada en comunidad simultáneamente con USM.

USM utiliza el concepto de un usuario para el que los parámetros de seguridad (niveles de seguridad, protocolos de autentificación y privacidad y claves) se configuran en el agente y el gestor. Los mensajes enviados utilizando USM se protegen mejor que los mensajes enviados con la seguridad basada en comunidad, donde las contraseñas se envían fuera de peligro y se visualizan en los rastreos. Con USM, los

mensajes intercambiados entre el gestor y el agente tienen comprobación de integridad de datos y autenticación de origen de datos. Los retardos de mensaje y las reproducciones de mensaje (más allá de lo que sucede normalmente debido a un protocolo de transporte sin conexión) se evitan utilizando indicadores de la hora e ID de petición. La confidencialidad, o el cifrado, de datos también está disponible, donde se permite, como un producto que se puede instalar por separado. La versión cifrada de **SNMP** se puede encontrar en AIX Expansion Pack.

La utilización de VACM implica la definición de colecciones de datos (llamadas vistas), grupos de usuarios de los datos y sentencias de acceso que definen qué vistas puede utilizar un grupo de usuarios determinado para leer, grabar o recibir en una ruptura.

**SNMPv3** también introduce la posibilidad de configurar dinámicamente el agente **SNMP** utilizando los mandatos SET **SNMP** en los objetos MIB que representan la configuración del agente. Este soporte de configuración dinámica permite añadir, suprimir y modificar las entradas de configuración de forma local o remota.

Las políticas de acceso y los parámetros de seguridad de **SNMPv3** se especifican en el archivo `/etc/snmpdv3.conf` del agente **SNMP** y el archivo `/etc/clsnmp.conf` del gestor **SNMP**. Para ver un caso que muestra la configuración de estos archivos, consulte el apartado “[Creación de usuarios en SNMPv3](#)” en la página 565. También puede consultar los formatos de archivo `/etc/snmpdv3.conf` y `/etc/clsnmp.conf` en la publicación *Referencia de archivos*.

### Arquitectura de **SNMPv3**

Existen cuatro partes principales en la arquitectura de **SNMPv3**.

En la siguiente figura se ilustra la interacción entre estos sistemas para proporcionar los datos necesarios solicitados:

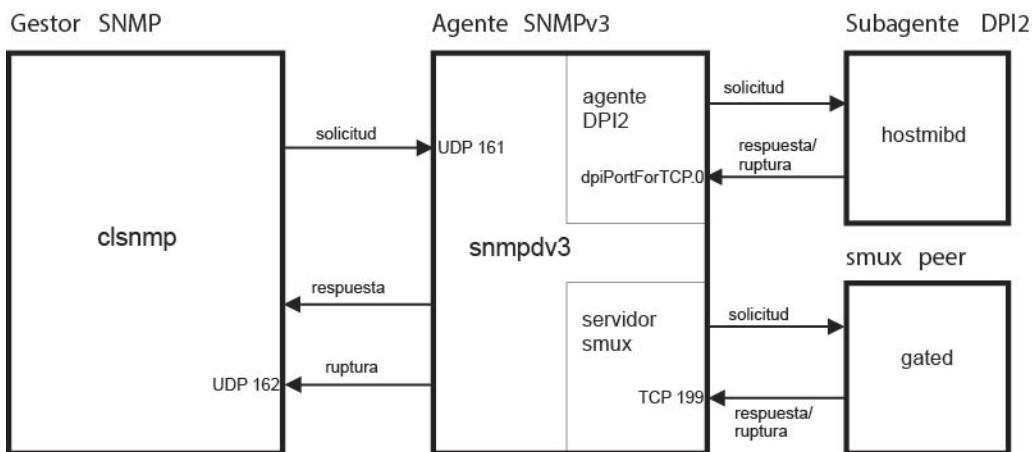


Figura 27. Partes principales de la arquitectura de **SNMPv3**

Esta ilustración muestra un ejemplo de la arquitectura de **SNMPv3**. Se muestran el subagente DPI2, el igual smux, el gestor **SNMP** y el agente **SNMP**. Además, se muestra cómo se comunican entre ellos.

### Agente **SNMP**

El agente **SNMP** recibe peticiones del gestor **SNMP** y crea respuestas para éste.

Además, el agente **SNMP** se comunica con todos los subagentes DPI2 y los iguales SMUX del sistema. El agente **SNMP** gestiona algunas variables MIB y todos los subagentes DPI2 y los iguales SMUX registran las variables MIB en el agente **SNMP**.

Cuando `clsnmp` (el gestor **SNMP**) emite una petición, ésta se envía a UDP 161 en el agente **SNMP**. Si la petición es una petición **SNMPv1** o **SNMPv2c**, el agente **SNMP** verificará el nombre de comunidad y procesará la petición. Si la petición es una petición **SNMPv3**, el agente **SNMP** intentará autenticar el usuario que solicita los datos y se asegurará de que el usuario tenga los permisos de acceso necesarios para satisfacer la petición utilizando las claves de autenticación y, si se está ejecutando la versión cifrada, las claves de privacidad. Si el agente **SNMP** no puede autenticar el usuario o si el usuario no tiene los permisos de acceso correctos para satisfacer la petición, el agente **SNMP** no atenderá la

petición. Para obtener información sobre cómo crear usuarios en **SNMPv3**, consulte el apartado “Creación de usuarios en SNMPv3” en la página 565.

Si el usuario se autentifica y tiene los permisos de acceso correctos, el agente **SNMP** satisfará la petición. El agente **SNMP** localizará las variables MIB que se estén solicitando. Si el propio agente **SNMP** está gestionando las variables MIB solicitadas, procesará la petición y devolverá la respuesta al gestor **SNMP**. Si un subagente DPI2 o un igual SMUX está gestionando las variables MIB solicitadas, el agente **SNMP** reenviará la petición al subagente DPI2 o al igual SMUX en el que se gestionan las variables MIB, le permitirá procesar la petición y, a continuación, responderá al gestor **SNMP**.

### **Subagentes de DPI2**

Un subagente de DPI2, por ejemplo **hostmibd**, se comunica con el agente DPI2 que, en **SNMPv3**, forma parte del agente **SNMP**.

El subagente DPI2 envía respuestas y rupturas al agente DPI2 a través de `dpiPortForTCP.0`. Dado que no es un puerto conocido, el subagente DPI2 debe emitir en primer lugar una solicitud para el número de puerto para `dpiPortForTCP.0`. Esta solicitud se emite en UDP 161 en el agente **SNMP**, después del cual el agente **SNMP** responde al subagente DPI2 con el número de puerto para `dpiPortForTCP.0`. Una vez que se reciba el número de puerto, el subagente DPI2 establece una conexión con el agente DPI2 utilizando el número de puerto proporcionado. Entonces el subagente DPI2 registra los subárboles MIB en el agente DPI2.

**Nota:** Para permitir que el agente **SNMP** escuche en un puerto distinto de UDP 161, debe establecer el entorno **SNMP\_PORT**. Existen dos modos de establecer esta variable:

- **Método 1:** Detenga el subagente DPI2 y escriba los mandatos siguientes:

- `SNMP_PORT=<número_puerto> /usr/sbin/aixmibd -d 128`
- `SNMP_PORT=<número_puerto> /usr/sbin/hostmibd -d 128`
- `SNMP_PORT=<número_puerto> /usr/sbin/snmpmibd -d 128`

donde *número\_puerto* es el número del puerto que desea utilizar.

Cuando los mandatos hayan terminado de ejecutarse, inicie el subagente DPI2.

- **Método 2:** Incluya la variable **SNMP\_PORT** en el archivo `/etc/environment` y asígnele el nuevo valor de puerto. Permita que los daemons **aixmibd**, **hostmibd**, **snmpmibd** y **snmpd** se ejecuten desde `/etc/rc.tcpip` tal cual. En este método, no tiene que ejecutar los mandatos **aixmibd**, **hostmibd** y **snmpmibd** desde la línea de mandatos.

Después de establecer la conexión y de que se hayan registrado los subárboles MIB, el subagente DPI2 estará preparado para responder a las peticiones recibidas del agente DPI2. Cuando se recibe una petición, el subagente DPI2 procesa la petición y responde con la información necesaria.

El subagente DPI2 también está preparado para enviar rupturas, si es necesario. Cuando se envíe una ruptura, el agente **SNMP** comprobará el archivo `/etc/snmpdv3.conf` para determinar la dirección o las direcciones IP a las que se debe reenviar la ruptura y enviará la ruptura a dichas direcciones.

### **Iguales SMUX**

Un igual SMUX (SNMP Multiplexing - Multiplexado SNMP), por ejemplo **gated**, cuando se inicie, establecerá la conexión en **TCP 199** e inicializará la asociación SMUX.

Después de la inicialización, el igual SMUX registrará los subárboles MIB que va a gestionar.

Después del registro, el igual SMUX está preparado para aceptar cualquier petición de entrada del servidor SMUX y devolver respuestas. Cuando el igual SMUX recibe una petición, procesará la petición y devolverá una respuesta al servidor SMUX.

El igual SMUX también puede enviar una ruptura en el servidor SMUX. Si se envía una ruptura, el agente **SNMP** comprobará el archivo `/etc/snmpdv3.conf` para determinar la dirección o las direcciones IP a las que se debe reenviar la ruptura y enviará la ruptura a dichas direcciones.

### **Gestor SNMP**

El gestor **SNMP** ejecuta **clsnmp**, que es compatible con **SNMPv1**, **SNMPv2c** y **SNMPv3**.

Utilice el mandato **clsnmp** para emitir una petición, por ejemplo una petición get, get-next, get-bulk o set. La petición se envía a UDP 161 en el agente **SNMP**, después de lo cual espera la respuesta del agente **SNMP**.

**Nota:** Para permitir que el gestor **SNMP** utilice un puerto distinto de UDP 161, necesita declarar el número de puerto que desea utilizar y la dirección IP en el campo **targetAgent** del archivo /etc/clsnmp.conf. Para obtener información sobre el archivo /etc/clsnmp.conf, consulte el apartado clsnmp.conf File en la publicación *Referencia de archivos*.

También puede escuchar las rupturas **SNMP** en UDP 162. El gestor **SNMP** recibirá rupturas si así se especifica la dirección IP en el archivo /etc/snmpdv3.conf del agente **SNMP**.

#### **Variables MIB**

En las ubicaciones siguientes se puede encontrar información sobre las variables MIB.

Para obtener información sobre las variables MIB, consulte [Management Information Base, Terminology Related to Management Information Base Variables, Working with Management Information Base Variables](#) y [Management Information Base Database](#) en la publicación *Communications Programming Concepts*.

Si desea configurar su propio subagente DPI2 o igual smux, consulte los directorios /usr/samples/snmpd/smux y /usr/samples/snmpd/dpi2.

#### **Claves de autentificación de SNMPv3**

Normalmente la autentificación es necesaria para las peticiones de **SNMPv3** que se deben procesar (a menos que el nivel de seguridad solicitado sea noAuth).

Cuando se autentifica una petición, el agente **SNMP** verifica que la clave de autentificación enviada en una petición **SNMPv3** se pueda utilizar para crear un resumen de mensaje que coincida con el resumen de mensaje creado desde la clave de autentificación definida por el usuario.

Cuando se emite una petición desde el gestor **SNMP**, el mandato **clsnmp** utiliza la clave de autentificación encontrada en una entrada en el archivo /etc/clsnmp.conf del gestor **SNMP**. Necesita correlacionarse con la clave de autentificación especificada en una entrada USM\_USER para dicho usuario en el archivo /etc/snmpdv3.conf del agente **SNMP**. Las claves de autentificación se generan utilizando el mandato **pwtkey**.

La clave de autentificación se genera desde dos unidades de información:

- La contraseña especificada
- La identificación del agente **SNMP** en el que se utilizará la clave. Si el agente es un agente de IBM y el ID de motor (engineID) se ha generado utilizando la fórmula de ID de motor específica de proveedor, es posible que el agente se identifique por la dirección IP o el nombre de sistema principal. De lo contrario, el ID de motor se debe proporcionar como identificación de agente.

Una clave que incorpora la identificación del agente en el que se utilizará se denomina clave localizada. Sólo se puede utilizar en dicho agente. Una clave que no incorpora el ID de motor del agente en el que se utilizará se denomina no localizada.

Se espera que las claves almacenadas en el archivo de configuración del mandato **clsnmp**, /etc/clsnmp.conf, sean claves no localizadas. Las claves almacenadas en el archivo de configuración del agente **SNMP**, /etc/snmpdv3.conf, pueden ser localizadas o no localizadas, aunque se considera más seguro utilizar claves localizadas.

Como alternativa al almacenamiento de claves de autentificación en el archivo de configuración de cliente, el mandato **clsnmp** permite almacenar contraseñas de usuario. Si el mandato **clsnmp** se configura con una contraseña, el código genera una clave de autentificación (y una clave de privacidad si se solicita y si se instala la versión cifrada) para el usuario. Estas claves deben producir los mismos valores de autentificación que las claves configuradas para USM\_USER en el archivo /etc/snmpdv3.conf del agente o configuradas dinámicamente con los mandatos SET de **SNMP**. Sin embargo, la utilización de contraseñas en el archivo de configuración de cliente se considera menos seguro que la utilización de claves en el archivo de configuración.

### **Claves de privacidad de SNMPv3**

El cifrado está disponible como un producto independiente en AIX Expansion Pack donde las leyes de exportación lo permiten. Las claves utilizadas para el cifrado se generan utilizando los mismos algoritmos que los utilizados para la autentificación.

Sin embargo, las longitudes de clave pueden diferir. Por ejemplo, una clave de autentificación HMAC-SHA tiene una longitud de 20 bytes, pero una clave de cifrado localizada utilizada con HMAC-SHA sólo tiene una longitud de 16 bytes.

La versión cifrada se activa automáticamente después de la instalación. Para volver a comutar a la versión no cifrada, utilice el mandato **snmpv3\_ssw**.

### **Claves de generación SNMPv3**

AIX utiliza el mandato **pwtokkey** para generar claves de autentificación y, cuando sea aplicable, claves de privacidad.

El mandato **pwtokkey** permite la conversión de contraseñas en claves de autentificación y privacidad localizadas y no localizadas. El procedimiento **pwtokkey** toma una contraseña y un identificador como agente y genera claves de autentificación y privacidad. Dado que el procedimiento utilizado por el mandato **pwtokkey** es el mismo algoritmo utilizado por el mandato **clsnmp**, la persona que configura el agente **SNMP** puede generar las claves de autentificación (y privacidad) apropiadas para ponerlas en el archivo */etc/clsnmp.conf* del gestor **SNMP** para un usuario, proporcionándose una contraseña determinada y la dirección IP en la que se ejecuta el destino.

Después de haber generado las claves de autentificación (y las claves de privacidad si está ejecutando la versión cifrada), necesitará entrar esas claves en el archivo */etc/snmpdv3.conf* del agente **SNMP** y en el archivo */etc/clsnmp.conf* del gestor **SNMP**.

En **SNMPv3**, existen nuevos posibles configuraciones de usuario. Más abajo se proporciona cada configuración posible, junto con un ejemplo de cada una. Estas claves determinadas se han generado utilizando **defaultpassword** para la contraseña y 9.3.149.49 como dirección IP. Se ha utilizado el siguiente mandato:

```
pwtokkey -u all -p all defaultpassword 9.3.149.49
```

Se han generado las siguientes claves de autentificación y privacidad:

```
Display of 16 byte HMAC-MD5 authKey:  
18a2c7b78f3df552367383eef9db2e9f  
  
Display of 16 byte HMAC-MD5 localized authKey:  
a59fa9783c04bcbe00359fb1e181a4b4  
  
Display of 16 byte HMAC-MD5 privKey:  
18a2c7b78f3df552367383eef9db2e9f  
  
Display of 16 byte HMAC-MD5 localized privKey:  
a59fa9783c04bcbe00359fb1e181a4b4  
  
Display of 20 byte HMAC-SHA authKey:  
754ebf6ab740556be9f0930b2a2256ca40e76ef9  
  
Display of 20 byte HMAC-SHA localized authKey:  
cd988a098b4b627a0e8adc24b8f8cd02550463e3  
  
Display of 20 byte HMAC-SHA privKey:  
754ebf6ab740556be9f0930b2a2256ca40e76ef9  
  
Display of 16 byte HMAC-SHA localized privKey:  
cd988a098b4b627a0e8adc24b8f8cd02
```

Estas entradas aparecerán en el archivo */etc/snmpdv3.conf*. Son posibles las nueve configuraciones siguientes:

- Claves de autentificación y privacidad localizadas utilizando el protocolo HMAC-MD5:

```
USM_USER user1 - HMAC-MD5 a59fa9783c04bcbe00359fb1e181a4b4 DES  
a59fa9783c04bcbe00359fb1e181a4b4 L - -
```

- Claves de autentificación y privacidad no localizadas utilizando el protocolo HMAC-MD5:

```
USM_USER user2 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f DES
18a2c7b78f3df552367383eef9db2e9f N - -
```

- Clave de autentificación localizada utilizando el protocolo HMAC-MD5:

```
USM_USER user3 - HMAC-MD5 a59fa9783c04bcbe00359fb1e181a4b4 - - L -
```

- Clave de autentificación no localizada utilizando el protocolo HMAC-MD5:

```
USM_USER user4 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - - N -
```

- Claves de autentificación y privacidad localizadas utilizando el protocolo HMAC-SHA:

```
USM_USER user5 - HMAC-SHA cd988a098b4b627a0e8adc24b8f8cd02550463e3 DES
cd988a098b4b627a0e8adc24b8f8cd02 L -
```

- Claves de autentificación y privacidad no localizadas utilizando el protocolo HMAC-SHA:

```
USM_USER user6 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 DES
754ebf6ab740556be9f0930b2a2256ca40e76ef9 N -
```

- Clave de autentificación localizada utilizando el protocolo HMAC-SHA:

```
USM_USER user7 - HMAC-SHA cd988a098b4b627a0e8adc24b8f8cd02550463e3 - - L -
```

- Clave de autentificación no localizada utilizando el protocolo HMAC-SHA:

```
USM_USER user8 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - - N -
```

- No se utilizan clave de autentificación ni privacidad (**SNMPv1**)

```
USM_USER user9 - none - none - - -
```

La configuración de usuarios en **SNMPv3** necesita la configuración del archivo `/etc/snmpdv3.conf` y del archivo `/etc/clsnmp.conf`. Para ver un caso de generación de claves de usuario y de edición de los archivos de configuración necesarios, consulte “[Creación de usuarios en SNMPv3](#)” en la página 565. También puede consultar el archivo de configuración `snmpdv3.conf` de ejemplo y el archivo de configuración `clsnmp.conf` ubicado en el directorio `/usr/samples/snmpdv3`.

### **Claves de actualización SNMPv3**

**SNMPv3** ofrece la posibilidad de actualizar dinámicamente claves de usuario basadas en nuevas contraseñas.

Esto se realiza utilizando el mandato `pwchange` para generar nuevas claves de usuario basadas en una contraseña actualizada, utilizando el mandato `clsnmp` para actualizar dinámicamente la clave de usuario en el archivo `/etc/snmpdv3.conf` y editando el archivo `/etc/clsnmp.conf` con las nuevas claves. Durante este proceso, la nueva contraseña no se comunica nunca entre máquinas.

Para obtener instrucciones paso a paso sobre cómo actualizar claves de usuario, consulte “[Actualización dinámica de las claves de autentificación y de privacidad en SNMPv3](#)” en la página 558.

### **Actualización dinámica de las claves de autentificación y de privacidad en SNMPv3**

En este ejemplo se muestra cómo actualizar dinámicamente las claves de autentificación para un usuario en **SNMPv3**.

En este caso, el usuario u4 actualizará las claves de autentificación para el usuario u8. Los dos usuarios u4 y u8 ya habían creado claves de autentificación basadas en la contraseña `contraseñaomisión` y en la dirección IP `9.3.149.49` y todo funciona correctamente.

Durante este caso, se crearán nuevas claves para el usuario u8 y el archivo `/etc/snmpdv3.conf` se actualizará dinámicamente. A continuación, la clave de autentificación para el usuario u8 en el archivo `/etc/clsnmp.conf` del lado del gestor se editarán manualmente para reflejar las nuevas claves.

Cree una copia de seguridad del archivo /etc/snmpd.conf en el agente **SNMP** y el gestor /etc/clsnmp.conf y una copia de seguridad del gestor **SNMP** antes de empezar este procedimiento.

A continuación, se encuentra el archivo /etc/snmpd.conf que se actualizará dinámicamente:

```
USM_USER u4 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - - N -
USM_USER u8 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - - N -

VACM_GROUP group1 SNMPv1 public -
VACM_GROUP group2 USM u4 -
VACM_GROUP group2 USM u8 -

VACM_VIEW defaultView      internet          - included -
VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1 defaultView - defaultView -
VACM_ACCESS  group2 - - noAuthNoPriv USM defaultView defaultView defaultView -
VACM_ACCESS  group2 - - AuthNoPriv USM defaultView defaultView defaultView -
VACM_ACCESS  group2 - - AuthPriv USM defaultView defaultView defaultView -

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 127.0.0.1      traptag trapparms1 - - -
TARGET_ADDRESS Target2 UDP 9.3.149.49       traptag trapparms2 - - -
TARGET_ADDRESS Target3 UDP 9.3.149.49       traptag trapparms3 - - -
TARGET_ADDRESS Target4 UDP 9.3.149.49       traptag trapparms4 - - -

TARGET_PARAMETERS trapparms1 SNMPv1  SNMPv1  public  noAuthNoPriv -
TARGET_PARAMETERS trapparms3 SNMPv2c  SNMPv2c  publicv2c  noAuthNoPriv -
TARGET_PARAMETERS trapparms4 SNMPv3  USM      u4     AuthNoPriv -
```

Este es el archivo /etc/clsnmp.conf que se actualizará para el usuario u8:

```
testu4 9.3.149.49 snmpv3 u4 - - AuthNoPriv HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - -
testu8 9.3.149.49 snmpv3 u8 - - AuthNoPriv HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - -
```

### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

### Actualizar la contraseña y las claves de autentificación

Los nombres de comunidad en el archivo /etc/snmpd.conf forman parte de las entradas VACM\_GROUP en el archivo /etc/snmpd.conf. Cada comunidad debe colocarse en un grupo. A continuación, deberá otorgar a los grupos los permisos de visualización y acceso necesarios.

1. En el lado del gestor **SNMP**, ejecute el mandato **pwchange**. En ese caso, hemos ejecutado el siguiente mandato:

```
pwchange -u auth -p HMAC-SHA contraseñaomisión contraseñaanueva 9.3.149.49
```

Este mandato generará una nueva clave de autentificación.

- -u auth especifica que sólo se creará una clave de autentificación. Si también va a actualizar claves privadas, utilice -u all.
- -p HMAC-SHA especifica el protocolo que se utilizará para crear la clave de autentificación. Si también va a actualizar las claves de privacidad, utilice -p all.
- *contraseñaomisión* es la contraseña que se emplea para crear la última clave de autentificación (por ejemplo, si se hubiera utilizado bluepen para crear la última clave de autentificación, se utilizaría también bluepen aquí)
- *contraseñaanueva* es la nueva contraseña que se utilizará para generar la clave de autentificación. Guárdela como futura referencia
- 9.3.149.49 es la dirección IP donde se ejecuta el agente **SNMP**.

Este mandato ha generado la siguiente salida:

```
Dump of 40 byte HMAC-SHA authKey keyChange value:  
8173701d7c00913af002a3379d4b150a  
f9566f56a4dbde21dd778bb166a86249  
4aa3a477e3b96e7d
```

En el siguiente paso se utilizará esta clave de autentificación.

**Nota:** Guarde las nuevas contraseñas en un lugar seguro. En el futuro las tendrá que utilizar de nuevo cuando realice cambios.

2. En el gestor **SNMP**, el usuario u4 cambiará la clave de autentificación del usuario u8 by escribiendo el siguiente mandato:

```
clsnmp -h testu4 set usmUserAuthKeyChange.12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56  
\'8173701d7c00913af002a3379d4b150af9566f56a4dbde21dd778bb166a862494aa3a477e3b96e7d\'h
```

- Se utiliza `testu4` porque está correlacionado con el usuario `u4` en el archivo `/etc/clsnmp.conf`.
- El ID de instancia de `usmUserAuthKeyChange` incluye, en valores decimales, el ID de motor del agente SNMP donde se realiza la actualización y el nombre de usuario cuya clave de autentificación se está actualizando. El ID de motor lo puede encontrar en el archivo `/etc/snmpd.boots` (el archivo `/etc/snmpd.boots` contiene dos series de números). El ID de motor es la primera serie. Omita la segunda serie de números).

El ID de motor deberá convertirse de valores hexadecimales a valores decimales para poderse utilizar aquí. Cada dos números en el ID de motor hexadecimal se convierten a un valor decimal. Por ejemplo, el ID de motor `000000020000000009039531` se leería como `00 00 00 02 00 00 00 09 03 95 31`. Cada uno de esos números debe convertirse a valores decimales, lo que genera `0.0.0.2.0.0.0.9.3.149.49` (Para ver una tabla de conversión, consulte [Tabla de conversión de valores ASCII, decimales, octales y binarios](#)). El primer número de la serie es el número de bytes de la serie decimal. En este caso, es `12`, lo que genera `12.0.0.0.2.0.0.0.0.9.3.149.49`.

El número siguiente es el número de bytes del nombre de usuario, seguido por los valores decimal del propio nombre de usuario. En este caso, el nombre de usuario es `u8`. Cuando se convierte a valores decimales, `u8` se convierte en `117.56`. Dado que el nombre de usuario tiene 2 bytes de longitud, el valor que representa el nombre de usuario se convierte en `2.117.56`. Añada esto al final del ID de motor decimal (Para ver una tabla de conversión, consulte [Tabla de conversión de valores ASCII, decimales, hexadecimales, octales y binarios](#)).

En este caso, el resultado es `12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56`.

- El siguiente valor en el mandato es la nueva clave de autentificación generada con el mandato **pwchange** en el paso anterior.

**Nota:** Si el usuario también ha configurado claves de privacidad, este procedimiento debe repetirse para actualizarlas. Cuando actualice las claves de privacidad, utilice el valor `usmUserPrivKeyChange` en lugar del valor `usmUserAuthKeyChange`.

La utilización de `usmUserOwnAuthKeyChange` en lugar de `usmUserAuthKeyChange` permitirá que un usuario cambie su propia clave de autentificación. Por ejemplo, el usuario `u4` podría cambiar su propia clave de autentificación mediante `usmUserOwnAuthKeyChange`.

La salida del mandato es la siguiente:

```
1.3.6.1.6.3.15.1.2.2.1.6.12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56 = '8173701d7c00913af002a3379  
d4b150af9566f56a4dbde21dd778bb166a862494aa3a477e3b96e7d'h
```

Una vez completado este mandato, el archivo `/etc/snmpdv3.conf` se actualizará automáticamente cada cinco minutos en el lado del agente **SNMP**. También puede detener e iniciar el daemon **SNMP** para actualizar el archivo. La siguiente entrada para el usuario `u8` se actualizará dinámicamente en el archivo `/etc/snmpdv3.conf`:

```
USM_USER u8 0b0000020000000009039531 HMAC-SHA 4be657b3ae92beee322ee5eaef665b338caf2d9  
None - L nonVolatile
```

3. En el lado del gestor **SNMP**, ejecute el mandato **pwtokey** para generar la nueva clave de autentificación basada en la nueva contraseña y colocarla en el archivo `/etc/clsnmp.conf`. En ese caso, hemos ejecutado el siguiente mandato:

```
pwtokey -u auth -p HMAC-SHA contraseñanueva9.3.149.49
```

- `-u auth` especifica que sólo se creará una clave de autentificación. Si también va a actualizar claves privadas, utilice `-u all`.
- `-p HMAC-SHA` especifica el protocolo que se utilizará para crear la clave de autentificación. Si también va a actualizar claves de privacidad, utilice `-p all`.
- La contraseña empleada (en este caso, `contraseñanueva`) debe ser la misma que la contraseña empleada cuando se generan nuevas claves de autentificación con el mandato **pwchange**.
- La dirección IP empleada (en este caso, `9.3.149.49`) debe ser la dirección IP donde se ejecuta el agente.

El resultado proporciona las claves de autentificación localizadas y no localizadas:

```
Display of 20 byte HMAC-SHA authKey:  
79ce23370c820332a7f2c7840c3439d12826c10d  
  
Display of 20 byte HMAC-SHA localized authKey:  
b07086b278163a4b873aace53a1a9ca250913f91
```

4. Abra el archivo `/etc/clsnmp.conf` con el editor de texto favorito y coloque la clave de autentificación no localizada en la línea del usuario cuyas claves se están actualizando. En ese caso, la entrada es la siguiente:

```
testu8 9.3.149.49 snmpv3 u8 - - AuthNoPriv HMAC-SHA 79ce23370c820332a7f2c7840c3439d12826c10d  
- -
```

Guarde el archivo y ciérrelo.

5. Probar la configuración actualizada ejecutando el siguiente mandato:

```
clsnmp -v -h testu8 walk mib
```

donde `mib` es una variable MIB a la que el usuario tiene acceso de lectura u8. En este caso, el usuario u8 tiene acceso a `internet`.

### Peticiones de SNMPv3

El mandato **clsnmp** se utiliza para enviar peticiones **SNMP** a agentes **SNMP** de sistemas principales locales o remotos.

Las peticiones pueden ser peticiones **SNMPv1**, **SNMPv2c** o **SNMPv3**. Para procesar las peticiones, se debe configurar el archivo `/etc/clsnmp.conf`.

El mandato **clsnmp** puede emitir peticiones get, getnext, getbulk, set, walk y findname. Cada una de estas peticiones se describe brevemente a continuación:

#### get

permite al usuario recopilar datos de una variable MIB

#### getnext

proporciona la siguiente variable MIB del subárbol MIB

#### getbulk

proporciona todas las variables MIB de varios subárboles

#### set

permite al usuario establecer una variable MIB

#### walk

proporciona todas las variables MIB de un subárbol

#### findname

correlaciona el OID con el nombre de variable

## trap

permite a **clsnmp** escuchar rupturas en el puerto 162

## Migración desde SNMPv1 hasta SNMPv3

En este caso, se muestra una migración típica desde **SNMPv1** hasta **SNMPv3**.

En el sistema operativo AIX, el agente **SNMP** de valor predeterminado que se ejecuta en tiempo de arranque del sistema es la versión no cifrada de **SNMPv3**. **SNMPv3** utiliza el archivo /etc/snmpdv3.conf como archivo de configuración. Cualquier parámetro que se haya configurado en el archivo /etc/snmpd.conf, que utiliza **SNMPv1** en versiones anteriores del sistema operativo AIX, se deberá migrar manualmente al archivo /etc/snmpdv3.conf.

En este caso, las comunidades y rupturas configuradas en el archivo /etc/snmpd.conf se migrarán hasta el archivo /etc/snmpdv3.conf. Al final del caso, **SNMPv3** facilitará las mismas funciones que las que **SNMPv1** ofrece. Si no ha configurado ninguna comunidad o ruptura propias de **SNMPv1**, no es necesario que complete este procedimiento.

Este archivo no contiene ninguna información sobre las características disponibles en **SNMPv3**. Para obtener información sobre cómo crear usuarios mediante las características de **SNMPv3** que no están disponibles en **SNMPv1**, consulte el apartado “[Creación de usuarios en SNMPv3](#)” en la página 565.

El archivo que figura a continuación es el archivo /etc/snmpd.conf de ejemplo que se va a migrar. Las comunidades siguientes están configuradas: daniel, vasu y david. Estas comunidades deben migrarse manualmente.

```
logging      file=/usr/tmp/snmpd.log          enabled
logging      size=0                           level=0

community   daniel    0.0.0.0    0.0.0.0    readWrite  1.17.35
community   vasu     9.3.149.49  255.255.255.255 readOnly  10.3.5
community   david    9.53.150.67 255.255.255.255 readWrite  1.17.35

view 1.17.35  udp  icmp  snmp 1.3.6.1.2.1.25
view 10.3.5   system interfaces tcp icmp

trap        daniel    9.3.149.49    1.17.35  fe
trap        vasu     9.3.149.49    10.3.5   fe
trap        david    9.53.150.67   1.17.35  fe

smux        1.3.6.1.4.1.2.3.1.2.3.1.1      sampled_password # sampled
```

Para completar los pasos en este caso, consulte el archivo /etc/snmpd.conf. Tenga preparada una copia de dicho archivo cuando inicie este procedimiento.

## Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

## Paso 1. Migrar la información sobre la comunidad

Los nombres de comunidad en el archivo /etc/snmpd.conf forman parte de las entradas VACM\_GROUP en el archivo /etc/snmpdv3.conf. Cada comunidad debe colocarse en un grupo. A continuación, deberá otorgar a los grupos los permisos de visualización y acceso necesarios.

1. Con la autorización root, abra el archivo /etc/snmpdv3.conf con el editor de texto favorito. Localice las entradas VACM\_GROUP en el archivo.
2. Cree una entrada VACM\_GROUP para cada comunidad que desee migrar. Si varias comunidades van a compartir los mismos permisos de visualización y acceso, sólo deberá crear un grupo para ellas. Los nombres de comunidad en el archivo /etc/snmpd.conf se convierten en los valores securityName de las entradas VACM\_GROUP. En este caso, se han añadido las siguientes entradas para vasu, daniel y david:

```
#-----
# Entradas de VACM_GROUP
# Define un grupo de seguridad (compuesto por usuarios o comunidades)
```

```

#   para el modelo de control de acceso basado en vista (VACM).
# El formato es:
#   groupName securityModel securityName storageType
VACM_GROUP group2 SNMPv1  vasu -
VACM_GROUP group3 SNMPv1  daniel -
VACM_GROUP group3 SNMPv1  david -
#-----

```

- *groupName* puede ser cualquier valor que desee, excepto *group1*.
- *securityModel* sigue siendo *SNMPv1* porque estamos migrando las comunidades *SNMPv1*.
- En este caso, *daniel* y *david* comparten los mismos permisos de visualización y acceso en el archivo */etc/snmpd.conf*. Por consiguiente, ambos son miembros de *group3* en el archivo */etc/snmpdv3.conf*. La comunidad *vasu* se coloca en un grupo distinto porque los permisos de visualización y acceso son diferentes de los de *david* y *daniel*.

Ahora las comunidades están colocadas en grupos.

## Paso 2. Migrar la información de visualización

La información de visualización en el archivo */etc/snmpd.conf* pasará a convertirse en las entradas *COMMUNITY*, *VACM\_VIEW* y *VACM\_ACCESS* en el archivo */etc/snmpdv3.conf*. Estas entradas determinarán los permisos de visualización y acceso para cada grupo.

1. Cree entradas *COMMUNITY* para *daniel*, *vasu*, y *david*, conservando las mismas direcciones IP para *netAddr* y *netMask* tal como se especificaron en el archivo */etc/snmpd.conf*.

```

#-----
# COMMUNITY
# Define una comunidad para la seguridad basada en la comunidad.
# El formato es:
#   communityName securityName securityLevel netAddr netMask storageType
COMMUNITY public    public      noAuthNoPriv 0.0.0.0    0.0.0.0    -
COMMUNITY daniel    daniel     noAuthNoPriv 0.0.0.0    0.0.0.0    -
COMMUNITY vasu     vasu      noAuthNoPriv 9.3.149.49  255.255.255.255 -
COMMUNITY david    david     noAuthNoPriv 9.53.150.67  255.255.255.255 -
#-----

```

2. Cree una entrada *VACM\_VIEW* para cada objeto o variable MIB a los que cada grupo tenga acceso. De acuerdo con el archivo */etc/snmpd.conf*, *daniel* y *david* tienen acceso a *udp*, *icmp*, *snmp* y *1.3.6.1.2.1.25* (subárbol de sistema principal definido en RFC 1514), y *vasu* tiene acceso a *system*, *interfaces*, *tcp* y *icmp*. Estas entradas de la vista se migran hasta el archivo */etc/snmpdv3.conf* tal como se indica a continuación:

```

#-----
# Entradas de VACM_VIEW
# Define un conjunto específico de datos MIB, denominados vista, para el
# Modelo de control de acceso basado en vista (VACM).
# El formato es:
#   viewName viewSubtree viewMask viewType storageType

VACM_VIEW group2View      system          - included -
VACM_VIEW group2View      interfaces      - included -
VACM_VIEW group2View      tcp             - included -
VACM_VIEW group2View      icmp            - included -

VACM_VIEW group3View      udp             - included -
VACM_VIEW group3View      icmp            - included -
VACM_VIEW group3View      snmp            - included -
VACM_VIEW group3View      1.3.6.1.2.1.25 - included -
#-----

```

3. Defina los permisos de acceso para las variables MIB definidas en las entradas *VACM\_VIEW* añadiendo las entradas *VACM\_ACCESS*. En el archivo */etc/snmpd.conf*, tanto *daniel* como *david* tienen permiso *readWrite* para las variables MIB, mientras que *vasu* tiene *readOnly*.

Defina estos permisos añadiendo las entradas *VACM\_ACCESS*. En este caso, hemos creado para *group2* (*vasu*) la entrada *group2View* para el permiso *readView*, pero hemos asignado *-* para el permiso *writeView* porque *vasu* tenía permiso *readOnly* en el archivo */etc/snmpd.conf*. Hemos creado para *group3* (*daniel* y *david*) la entrada *group3View* tanto para los permisos *readView*

como `writeView` porque estos grupos tenían acceso `readWrite` en el archivo `/etc/snmpd.conf`. Vea el siguiente ejemplo.

```
#-----
# Entradas de VACM_ACCESS
#   Identifica el acceso permitido a diferentes grupos de seguridad
#   para el Modelo de control de acceso basado en vista (VACM).
# El formato es:
# groupName contextPrefix contextMatch securityLevel securityModel readView writeView notifyView
storageType
VACM_ACCESS group1 - - noAuthNoPriv SNMPv1 defaultView - defaultView -
VACM_ACCESS group2 - - noAuthNoPriv SNMPv1 group2View - group2View -
VACM_ACCESS group3 - - noAuthNoPriv SNMPv1 group3View group3View group3View -
#-----
--
```

### Paso 3. Migrar la información de ruptura

Las entradas de ruptura en el archivo `/etc/snmpd.conf` pasarán a convertirse en las entradas `NODEFY TARGET_ADDRESS` y `TARGET_PARAMETERS` en el archivo `/etc/snmpdv3.conf`. Sin embargo, sólo deberán migrarse `TARGET_ADDRESS` y `TARGET_PARAMETERS`.

1. Las direcciones IP que figuran en la lista de entradas de ruptura en el archivo `/etc/snmpd.conf` pasarán a formar parte de las entradas `TARGET_ADDRESS` en el archivo `/etc/snmpdv3.conf`. Esta línea especifica el sistema principal al que se enviará la ruptura. Puede definir las entradas `targetParams`. En este caso, utilizamos `trapparms1`, `trapparms2`, `trapparms3` y `trapparms4`, que se definirán en las entradas `TARGET_PARAMETERS`.

```
#-----
# TARGET_ADDRESS
#   Define la dirección y parámetros de una aplicación de gestión
#   que se utilizarán para el envío de notificaciones.
# El formato es:
#   targetAddrName tDomain tAddress tagList targetParams timeout retryCount storageType
TARGET_ADDRESS Target1 UDP 127.0.0.1      traptag trapparms1 - - -
TARGET_ADDRESS Target2 UDP 9.3.149.49     traptag trapparms2 - - -
TARGET_ADDRESS Target3 UDP 9.3.149.49     traptag trapparms3 - - -
TARGET_ADDRESS Target4 UDP 9.53.150.67    traptag trapparms4 - - -
#-----
```

2. Los nombres de comunidad especificados en las entradas de ruptura en el archivo `/etc/snmpd.conf` pasarán a formar parte de las entradas `TARGET_PARAMETERS` en el archivo `/etc/snmpdv3.conf`. Los nombres de comunidad deben estar relacionados con una entrada `TARGET_ADDRESS` específica utilizando los valores `targetParams`. Por ejemplo, la comunidad `daniel` está correlacionada con `trapparms2`, que, bajo la entrada `TARGET_ADDRESS` se correlaciona con la dirección IP `9.3.149.49`. La comunidad `daniel` y la dirección IP `9.3.149.49` eran originalmente una entrada `trap` en el archivo `/etc/snmpd.conf`. Vea el siguiente ejemplo:

```
#-----
# TARGET_PARAMETERS
#   Define los parámetros de proceso y seguridad del mensaje
#   que se utilizarán para el envío de notificaciones a un destino de gestión específico.
# El formato es:
#   paramsName mpModel securityModel securityName securityLevel storageType
TARGET_PARAMETERS trapparms1 SNMPv1  SNMPv1  public  noAuthNoPriv -
TARGET_PARAMETERS trapparms2 SNMPv1  SNMPv1  daniel  noAuthNoPriv -
TARGET_PARAMETERS trapparms3 SNMPv1  SNMPv1  vasu   noAuthNoPriv -
TARGET_PARAMETERS trapparms4 SNMPv1  SNMPv1  david  noAuthNoPriv -
#-----
```

3. La información `trapmask` en el archivo `/etc/snmpd.conf` no migra hasta el archivo `/etc/snmpdv3.conf`.

#### Paso 4. Migrar la información de smux

Si tiene información de smux para migrar, puede copiar esas líneas directamente en el nuevo archivo. En este caso, la entrada de smux sampled se configuró en el archivo /etc/snmpd.conf. Esa línea debe copiarse en el archivo /etc/snmpdv3.conf.

```
#-----  
#      smux <client Identifier> <password> <address> <netmask>  
smux      1.3.6.1.4.1.2.3.1.2.3.1.1      sampled_password # sampled  
#-----
```

#### Paso 5. Detener e iniciar el daemon snmpd

Cuando se haya completado la migración del archivo /etc/snmpd.conf al archivo /etc/snmpdv3.conf, detenga e inicie el daemon **snmpd**. Deberá detener e iniciar el daemon **snmpd** cada vez que realice cambios en el archivo /etc/snmpdv3.conf.

1. Escriba el siguiente mandato para detener el daemon:

```
stopsrc -s snmpd
```

2. Escriba el siguiente mandato para reiniciar el daemon:

```
startsrc -s snmpd
```

**Nota:** Renovar simplemente el agente **SNMPv3** no funcionará tal como lo hizo en **SNMPv1**. Si realiza cambios en el archivo /etc/snmpdv3.conf, deberá detener e iniciar el daemon tal como se ha indicado arriba. La función de configuración dinámica soportada en **SNMPv3** no le permitirá renovar.

#### Creación de usuarios en SNMPv3

En este caso se muestra cómo crear un usuario en SNMPv3 editando manualmente los archivos /etc/snmpdv3.conf y /etc/clsnmp.conf.

En este caso, se creará el usuario u1. Al usuario u1 se le otorgarán claves de autorización, pero no se le otorgarán claves de privacidad (que sólo están disponibles si tiene instalado el conjunto de archivos snmp.crypto). El protocolo HMAC-MD5 se utilizará para crear las claves de autorización de u1. Cuando u1 esté configurado, se transferirá a un grupo y después dicho grupo tendrá definidos los permisos de visualización y acceso. Finalmente, se crearán las entradas de ruptura para u1.

Cada valor individual empleado en los archivos /etc/snmpdv3.conf y /etc/clsnmp.conf no debe sobrepasar 32 bytes.

#### Cuestiones que deben tenerse en cuenta

- La información de este procedimiento se ha probado utilizando versiones específicas de AIX. Los resultados que obtenga pueden variar significativamente dependiendo de la versión y el nivel de AIX.

#### Paso 1. Crear el usuario

1. Decida qué protocolos de seguridad desea utilizar: HMAC-MD5 o bien HMAC-SHA. En este caso, se utilizará HMAC-MD5.
2. Genere las claves de autentificación mediante el mandato pwtokey. La salida puede ser diferente en función del protocolo de autentificación que utilice y si utiliza claves de privacidad. Estas claves se utilizarán en los archivos /etc/snmpdv3.conf y /etc/clsnmp.conf. A continuación, se muestra el mandato empleado para el usuario u1:

```
pwtokey -p HMAC-MD5 -u auth anypassword 9.3.230.119
```

La dirección IP especificada es la dirección IP donde se ejecuta el agente. La contraseña puede ser cualquier contraseña, pero cerciórese de guardarla en un lugar seguro para poderla utilizar más adelante. La salida podría ser similar a la siguiente:

```
Display of 16 byte HMAC-MD5 authKey:  
63960c12520dc8829d27f7fbaf5a0470
```

```
Display of 16 byte HMAC-MD5 localized authKey:  
b3b6c6306d67e9c6f8e7e664a47ef9a0
```

3. Con la autorización como root, abra el archivo `/etc/snmpdv3.conf` con el editor de texto favorito.
4. Cree un usuario añadiendo una entrada `USM_USER` siguiendo el formato suministrado en el archivo. El valor `authKey` será la clave de autentificación localizada que se generó mediante el mandato `pwtkey`. La entrada para el usuario u1 es la siguiente:

```
#-----  
# Entradas de USM_USER  
# Define un usuario para el modelo de seguridad basado en usuario (USM).  
# El formato es:  
#   userName engineID authProto authKey privProto privKey keyType storageType  
#  
USM_USER u1 - HMAC-MD5 b3b6c6306d67e9c6f8e7e664a47ef9a0 - - L -  
#-----
```

- `userName` es el nombre del usuario. En este caso, es u1.
  - `authProto` debe ser el protocolo que utilizó cuando creó las claves. En este caso, es HMAC-MD5.
  - `authKey` es la clave de autentificación localizada que se creó mediante el mandato `pwtkey`.
  - `privProto` y `privKey` no se especifican porque no utilizan las claves de privacidad en este caso.
  - `keyType` es L porque utilizamos la clave de autentificación localizada.
5. Guarde y cierre el archivo `/etc/snmpdv3.conf`.
  6. Abra el archivo `/etc/clsnmp.conf` en el gestor SNMP con el editor de texto favorito.
  7. Añada el nuevo usuario de acuerdo con el formato suministrado en el archivo. La entrada para u1 es la siguiente:

```
#-----  
#-----  
# Formato de entradas:  
# winSnmpName targetAgent admin secName password context secLevel authProto authKey  
privProto privKey  
#  
user1 9.3.230.119 SNMPv3 u1 - - AuthNoPriv HMAC-MD5  
63960c12520dc8829d27f7fbaf5a0470 - -  
#-----  
-----
```

- `winSnmpName` puede ser cualquier valor. Este valor se utilizará cuando se creen solicitudes SNMP mediante el mandato `clsnmp`.
  - `targetAgent` es la dirección IP donde se ejecuta el agente, que también se ha utilizado en la creación de las claves de autentificación.
  - `admin` se establece en SNMPv3 porque enviaremos solicitudes SNMPv3.
  - `secName` es el nombre del usuario que se está creando. En este caso, es u1.
  - `seclevel` se establece en AuthNoPriv porque está configurado para utilizar la autentificación pero no la privacidad (como consecuencia, no hay valores para `privProto` y `privKey`).
  - `authproto` se establece en el protocolo de autentificación que se utilizó en la creación de las claves de autentificación.
  - `authKey` es la clave no localizada generada por el mandato `pwtkey`.
8. Guarde y cierre el archivo `/etc/clsnmp.conf`.

## Paso 2. Configurar el grupo

Ahora el usuario debe colocarse en un grupo. Si ya dispone de un grupo que está configurado con todos los permisos de visualización y acceso que desea conceder a este usuario, puede transferir este usuario a dicho grupo. Si desea conceder a este usuario unos permisos de visualización y acceso que ningún otro grupo tenga o si no tiene ningún grupo configurado, cree un grupo y añádale este usuario.

Para añadir el usuario a un nuevo grupo, cree una nueva entrada VACM\_GROUP en el archivo /etc/snmpdv3.conf. La entrada del grupo para u1 es la siguiente:

```
#-----
# Entradas de VACM_GROUP
# Define un grupo de seguridad (compuesto por usuarios o comunidades)
# para el modelo de control de acceso basado en vista (VACM).
# El formato es:
# groupName securityModel securityName storageType
VACM_GROUP group1 USM u1 -
#-----
```

- *groupName* puede ser un nombre cualquiera. Se convierte en el nombre del grupo. En este caso, es **group1**.
- *securityModel* se establece en USM, que aprovecha las características de seguridad de SNMPv3.
- *securityName* es el nombre del usuario. En este caso, es **u1**.

### Paso 3. Configurar los permisos de visualización y acceso

Deben establecerse permisos de visualización y acceso para el nuevo grupo que se acaba de crear. Estos permisos se establecen añadiendo las entradas VACM\_VIEW y VACM\_ACCESS al archivo /etc/snmpdv3.conf.

1. Decida qué permisos de visualización y acceso desea que el tenga el nuevo grupo.
2. Añada las entradas VACM\_VIEW al archivo /etc/snmpdv3.conf para definir a qué objetos MIB puede acceder el grupo. En este caso, **group1** tendrá acceso a los subárboles de MIB **interfaces**, **tcp**, **icmp**, y **system**. Sin embargo, restringiremos el acceso de **group1** a la variable de MIB **sysObjectID** dentro del subárbol MIB del sistema.

```
#-----
# Entradas de VACM_VIEW
# Define un conjunto específico de datos MIB, denominados vista, para el
# Modelo de control de acceso basado en vista (VACM).
# El formato es:
# viewName viewSubtree viewMask viewType storageType
VACM_VIEW group1View      interfaces      - included -
VACM_VIEW group1View      tcp            - included -
VACM_VIEW group1View      icmp           - included -
VACM_VIEW group1View      system          - included -
VACM_VIEW group1View      sysObjectID    - excluded -
#-----
```

- *viewName* es el nombre de la vista. En este caso, es **group1View**.
- *viewSubtree* es el subárbol MIB al que desea otorgar acceso.
- *viewType* determina si los subárboles MIB definidos se incluyen en la vista. En este caso, se incluyen todos los subárboles, pero la variable de MIB **sysObjectID**, que forma parte del subárbol **system** queda excluida.

3. Añada una entrada VACM\_ACCESS al archivo /etc/snmpdv3.conf para definir los permisos que el grupo tiene sobre los objetos MIB especificados arriba. Para **group1**, sólo se proporciona acceso de lectura.

```
#-
# Entradas de VACM_ACCESS
# Identifica el acceso permitido a diferentes grupos de seguridad
# para el Modelo de control de acceso basado en vista (VACM).
# El formato es:
# groupName contextPrefix contextMatch securityLevel securityModel readView writeView notifyView
storageType
VACM_ACCESS group1 - - AuthNoPriv USM group1View - group1View -
#-
#-----
```

- *groupName* es el nombre del grupo. En este caso, es **group1**.

- *securityLevel* es el nivel de seguridad que se está empleando. En este caso, se utilizan claves de autentificación pero no claves de privacidad. Por consiguiente, el valor se establece en AuthNoPriv.
- *securityModel* es el modelo de seguridad que está utilizando (SNMPv1, SNMPv2c o USM). En este caso, se establece en USM para que se puedan utilizar las características de seguridad SNMPv3.
- *readView* determina a qué entradas de VACM\_VIEW el grupo tiene acceso de lectura. En este caso, se suministra group1View, que suministra acceso de lectura group1 a las entradas group1View VACM\_VIEW.
- *writeView* determina a qué entradas de VACM\_VIEW el grupo tiene acceso de grabación. En este caso, no se suministra ningún acceso de grabación a group1.
- *notifyView* especifica el nombre de la vista que se va a aplicar cuando se establece una ruptura bajo el control de la entrada en la tabla de acceso.

**Nota:** En algunos casos, puede que las entradas de VACM\_ACCESS para un grupo sean necesarias. Si los usuarios del grupo tienen diferentes valores de autentificación y privacidad (noAuthNoPriv, AuthNoPriv o AuthPriv) serán necesarias varias entradas VACM\_ACCESS con el parámetro securityLevel establecido tal como corresponde.

#### Paso 4. Configurar entradas de ruptura para el usuario

Las entradas de ruptura en SNMPv3 se crean añadiendo las entradas NOTIFY, TARGET\_ADDRESS y TARGET\_PARAMETERS al archivo /etc/snmpdv3.conf. La entrada TARGET\_ADDRESS especificará dónde desea enviar las rupturas y la entrada TARGET\_PARAMETERS correlacionará la información TARGET\_ADDRESS con group1.

La entrada NOTIFY se ha configurado de forma predeterminada. A continuación, se muestra la entrada NOTIFY por omisión:

```
NOTIFY notify1 traptag trap -
```

En este caso, utilizaremos el valor especificado en la entrada por omisión, *traptag*.

1. Añada una entrada TARGET\_ADDRESS para especificar a qué lugar desea enviar las rupturas.

```
#-----
# TARGET ADDRESS
# Define la dirección y parámetros de una aplicación de gestión
# que se utilizarán para el envío de notificaciones.
# El formato es:
# targetAddrName tDomain tAddress tagList targetParams timeout retryCount storageType
#-----
TARGET_ADDRESS Target1 UDP 9.3.207.107      traptag trapparms1 - - -
```

- *targetAddrName* puede ser un nombre cualquiera. En este caso, hemos utilizado Target1.
- *tAddress* es la dirección IP donde deben enviarse las rupturas del grupo.
- *tagList* es el nombre configurado en la entrada NOTIFY. En este caso, es *traptag*.
- *targetParams* puede ser cualquier valor. Utilizamos *trapparms1*, que se utilizará en la entrada TARGET\_PARAMETERS.

2. Añada una entrada TARGET\_PARAMETERS.

```
#-----
# TARGET_PARAMETERS
# Define los parámetros de proceso y seguridad del mensaje
# que se utilizarán para el envío de notificaciones a un destino de gestión específico.
# El formato es:
# paramsName mpModel securityModel securityName securityLevel storageType
#-----
TARGET_PARAMETERS trapparms1 SNMPv3 USM      u1          AuthNoPriv -
```

- *paramsName* es el mismo que el valor *targetParams* de la entrada TARGET\_ADDRESS, que, en este caso, es *trapparms1*.
- *mpModel* es la versión de SNMP que se está utilizando.

- *securityModel* es el modelo de seguridad que se está utilizando (SNMPv1, SNMPv3 o USM). En este caso, se establece en USM para que se puedan utilizar las características de seguridad SNMPv3.
- *securityName* es el nombre de usuario especificado en la entrada USM\_USER, que en este caso, es u1.
- *securityLevel* se establece en AuthNoPriv porque utilizamos claves de autentificación pero no claves de privacidad.

## Paso 5. Detener e iniciar el daemon snmpd

Después de realizar los cambios en el archivo /etc/snmpdv3.conf, detenga e inicie el daemon **snmpd**.

1. Escriba el siguiente mandato para detener el daemon **snmpd**.

```
stopsrc -s snmpd
```

2. Escriba el siguiente mandato para iniciar el daemon **snmpd**.

```
startsrc -s snmpd
```

Ahora los nuevos valores entrarán en vigor.

**Nota:** Renovar simplemente el agente SNMPv3 mediante refresh -s snmpd no funcionará tal como lo hizo en SNMPv1. Si realiza cambios en el archivo /etc/snmpdv3.conf, deberá detener e iniciar el daemon tal como se ha indicado arriba. La función de configuración dinámica soportada en SNMPv3 no le permitirá ejecutar la renovación.

## Paso 6. Probar la configuración

Para verificar si la configuración es correcta, puede ejecutar el siguiente mandato en el gestor SNMP.

```
clsnmp -h user1 walk mib
```

donde *mib* es un subárbol MIB al que el usuario tiene acceso. En este caso, podría ser interfaces, tcp, icmp o system. Si la configuración es correcta, verá la información en el subárbol especificado.

Si no ha obtenido la salida correcta, revise los pasos de este documento y verificar si ha especificado correctamente toda la información.

## Resolución de problemas de SNMPv3

Se pueden encontrar estos problemas al utilizar **SNMPv3**.

- Mientras migra, necesita migrar las entradas de comunidad y SMUX definidas en el archivo /etc/snmpd.conf al archivo /etc/snmpdv3.conf. Para obtener información sobre cómo migrar esta información, consulte el apartado “[Migración desde SNMPv1 hasta SNMPv3](#)” en la página 562.
- Las peticiones no generan respuestas.

La causa más probable de este problema es un error de configuración en el archivo /etc/snmpdv3.conf y/o el archivo /etc/clsnmp.conf. Revise detenidamente estos archivos para asegurarse de que se ha entrado toda la información correctamente. Para obtener información sobre cómo editar estos archivos al crear usuario nuevos, consulte el apartado “[Creación de usuarios en SNMPv3](#)” en la página 565.

- Se ha configurado un usuario nuevo utilizando las claves de autentificación y privacidad, pero se devuelve un mensaje de error cuando se utiliza este usuario.

La causa más probable es que no esté ejecutando la versión cifrada de **SNMPv3**. Siga estos pasos para determinar qué versión está ejecutando:

1. Ejecute ps -e | grep snmpd.

- Si no recibe ninguna salida, probablemente necesita iniciar el daemon **snmpd**. Ejecute startsrc -s snmpd.

- Si la salida incluía snmpdv1, está ejecutando **SNMPv1**. Podrá realizar peticiones de **SNMPv1** cuando ejecute esta versión.
  - Si la salida incluía snmpdv3ne, está ejecutando la versión no cifrada de **SNMPv3**. Tras instalar el sistema operativo AIX, esta versión se ejecutará de forma predeterminada. Esta versión no le permite utilizar claves de privacidad.
  - Si la salida incluía snmpdv3e, está ejecutando la versión cifrada de **SNMPv3**, que es un producto que se puede instalar de forma independiente. La versión cifrada de **SNMPv3** está disponible en el AIX Expansion Pack donde se permite. La versión cifrada de **SNMPv3** permite utilizar las claves de privacidad.
2. Determine si la versión que está ejecutando es la versión que quería. Si no lo es, utilice el mandato **snmpv3\_ssw** para cambiar la versión del modo siguiente:
- **snmpv3\_ssw -1** conmutará a **SNMPv1**
  - **snmpv3\_ssw -n** conmutará a **SNMPv3** no cifrado
  - **snmpv3\_ssw -e** conmutará a **SNMPv3** cifrado si está instalado
- Después de realizar cambios en el archivo `/etc/snmpdv3.conf` y de renovar el daemon, los cambios no entran en vigor.

Después de realizar cambios en el archivo `/etc/snmpdv3.conf`, el daemon **SNMP** se debe detener e iniciar. La renovación del daemon no funciona. Utilice el procedimiento siguiente:

1. Detenga el daemon **SNMP** ejecutando `stopsrc -s snmpd`.
2. Inicie el daemon **SNMP** ejecutando `startsrc -s snmpd`.
- Se inicia el subagente DPI2, pero desde él no se puede consultar ninguna variable MIB.

La causa más probable es que la comunidad `public` no esté configurada en el archivo `/etc/snmpdv3.conf`. De forma predeterminada, el subagente DPI2 enviado con AIX utiliza el nombre de comunidad `public` para conectarse al agente **SNMP**. La comunidad `public` se configura en el archivo `/etc/snmpdv3.conf` de forma predeterminada. Si ha eliminado la comunidad `public` del archivo `/etc/snmpd.conf`, añada las líneas siguientes al archivo:

```
VACM_GROUP group1 SNMPv1 public -
VACM_VIEW defaultView 1.3.6.1.4.1.2.2.1.1.1.0 - included -
VACM_ACCESS group1 - - noAuthNoPriv SNMPv1 defaultView - defaultView -
COMMUNITY public      public      noAuthNoPriv 0.0.0.0      0.0.0.0      -
```

`1.3.6.1.4.1.2.2.1.1.1.0` es el OID para `dpiPortForTCP.0`.

- Las variables MIB gestionadas por el igual SMUX que se podían consultar antes de la migración ya no se pueden consultar.

Asegúrese de que la entrada SMUX esté presente en el archivo `/etc/snmpdv3.conf` y el archivo `/etc/snmpd.peers`. Si configura iguales SMUX nuevos, asegúrese de que éstos también se entren en estos dos archivos.

- Se había implementado un conjunto personal de variables MIB, pero las variables no se pueden incluir o excluir en la vista de otros usuarios.

En la entrada VACM\_VIEW del archivo `/etc/snmpdv3.conf`, debe especificar el OID de la variable MIB en lugar del nombre de variable MIB.

- No se reciben rupturas de recepción.

Asegúrese de que ha configurado las entradas de ruptura correctamente en el archivo `/etc/snmpdv3.conf`. Además, si la ruptura es una ruptura **SNMPv3**, también se debe configurar el archivo `/etc/clsnmp.conf`. Para obtener instrucciones sobre cómo configurar rupturas, consulte el apartado [“Creación de usuarios en SNMPv3” en la página 565](#).

Además, asegúrese de que la máquina especificada para recibir rupturas (en el archivo `/etc/snmpdv3.conf`) esté escuchándolas. Puede iniciar este proceso ejecutando `clsnmp trap` en la línea de mandatos de la máquina de recepción.

- ¿Por qué no se ejecuta el servidor DPI2 en el entorno **SNMPv3**?

En la arquitectura **SNMPv3**, el propio agente **SNMPv3** ejecuta el servidor DPI2. Consulte el apartado “Arquitectura de SNMPv3” en la página 554 para obtener más información.

## SNMPv1

Esta información es específica de **SNMPv1**. Cuando se utiliza **SNMPv1**, el agente **snmpd** utiliza un esquema de autenticación simple para determinar qué estaciones de gestor de **SNMP (Protocolo simple de gestión de red)** pueden acceder a las variables de Management Information Base (MIB) variables.

Este esquema de autenticación incluye la especificación de políticas de acceso **SNMP** para **SNMPv1**. Una política de acceso **SNMP** es una relación administrativa que incluye una asociación entre una comunidad **SNMP**, una modalidad de acceso y una vista MIB.

Una *comunidad SNMP* es un grupo de uno o más sistemas principales y un nombre de comunidad. Un nombre de comunidad es una serie de octetos que un gestor **SNMP** debe incorporar en un paquete de petición **SNMP** para la autenticación.

La *modalidad de acceso* especifica el acceso al que están autorizados los sistemas principales de la comunidad en lo que concierne a la recuperación o la modificación de las variables MIB de un agente **SNMP** específico. La modalidad de acceso debe ser una de las siguientes: *ninguna, sólo lectura, lectura y grabación o sólo grabación*.

Una *vista MIB* define uno o más subárboles MIB a los que puede acceder una comunidad **SNMP** específica. La vista MIB puede ser el árbol MIB entero o un subconjunto limitado del árbol MIB entero.

Cuando el agente **SNMP** recibe una petición, el agente verifica el nombre de comunidad con la dirección IP de sistema principal solicitante para determinar si el sistema principal solicitante es un miembro de la comunidad **SNMP** identificada por el nombre de comunidad. Si el sistema principal solicitante es miembro de la comunidad **SNMP**, el agente **SNMP** determina si se permite al sistema principal solicitante el acceso especificado para las variables MIB especificadas como se define en la política de acceso asociada con esa comunidad. Si se satisfacen todos los criterios, el agente **SNMP** intenta satisfacer la petición. De lo contrario, el agente **SNMP** genera una ruptura *authenticationFailure* o devuelve el mensaje de error apropiado al sistema principal solicitante.

Las políticas de acceso **SNMPv1** para el agente **snmpd** son configurables por el usuario y se especifican en el archivo `/etc/snmpd.conf`. Para configurar las políticas de acceso **SNMP** para el agente **snmpd**, consulte el archivo `/etc/snmpd.conf` en *Files Reference*.

## Configuración de daemon SNMP

El daemon **Simple Network Management Protocol (SNMP)** es un proceso de servidor de segundo plano que se puede ejecutar en cualquier sistema principal de estación de trabajo **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

El daemon, que actúa como agente **SNMP**, recibe, autentifica y procesa peticiones **SNMP** de las aplicaciones de gestor. Consulte los apartados *Simple Network Management Protocol*, *How a Manager Functions* y *How an Agent Functions* en la publicación *Communications Programming Concepts* para obtener información más detallada sobre las funciones de agente y gestor.

**Nota:** Los términos **daemon SNMP**, **agente SNMP** y **agente** se utilizan de forma intercambiable.

El daemon **snmpd** necesita que la interfaz **TCP/IP** de bucle de retorno esté activa para la configuración mínima. Entre el siguiente mandato antes de iniciar **TCP/IP**:

```
ifconfig lo0 loopback up
```

El daemon **SNMP** intentará enlazar sockets a determinados puertos conocidos de **User Datagram Protocol (UDP)** y **Transmission Control Protocol (TCP)**, que se deben definir en el archivo `/etc/services` del modo siguiente:

snmp	161/udp
snmp-trap	162/udp
smux	199/tcp

Al servicio snmp se le debe asignar el puerto 161, como lo requiere RFC 1157. El archivo /etc/services asigna los puertos 161, 162 y 199 a estos servicios. Si se está sirviendo el archivo /etc/services desde otra máquina, estos puertos asignados deben dejarse disponibles en el archivo /etc/services servido del servidor para que el daemon **SNMP** se pueda ejecutar.

El daemon **SNMP** lee el archivo de configuración en la versión de **SNMP** en ejecución durante el arranque y cuando se emite un mandato **refresh** (si el daemon **snmpd** se invoca bajo el control del Controlador de recursos del sistema) o la señal **kill -1**.

#### **Archivo /etc/snmpd.conf**

El archivo de configuración /etc/snmpd.conf especifica nombres de comunidad y privilegios de acceso y vistas asociados, sistemas principales para la notificación de ruptura, atributos de registro cronológico, configuraciones de parámetros específicos de **snmpd** y configuraciones de multiplexor individual (SMUX) para el daemon **SNMP** para **SNMPv1**.

Consulte el archivo [/etc/snmpd.conf](#) en *Files Reference* para obtener más información.

#### **Proceso de daemon SNMP**

El daemon **Simple Network Management Protocol (SNMP)** procesa las peticiones **SNMP** de las aplicaciones de gestor.

Lea los apartados [Simple Network Management Protocol \(SNMP\)](#), [How a Manager Functions](#) y [How an Agent Functions](#) en la publicación *Communications Programming Concepts* para obtener información más detallada sobre las funciones de agente y gestor.

#### **Proceso y autenticación de mensajes SNMP**

Todas las peticiones, rupturas y respuestas se transmiten en forma de mensajes codificados con ASN.1.

Un mensaje, tal como se define en RFC 1157, tiene la estructura siguiente:

#### *Versión Comunidad PDU*

donde **Versión** es la versión de SNMP (actualmente la versión 1), **Comunidad** es el nombre de comunidad y **PDU** es la unidad de datos de protocolo que contiene los datos de petición, respuesta o ruptura de **SNMP**. Una PDU también se codifica de acuerdo con las normas de ASN.1.

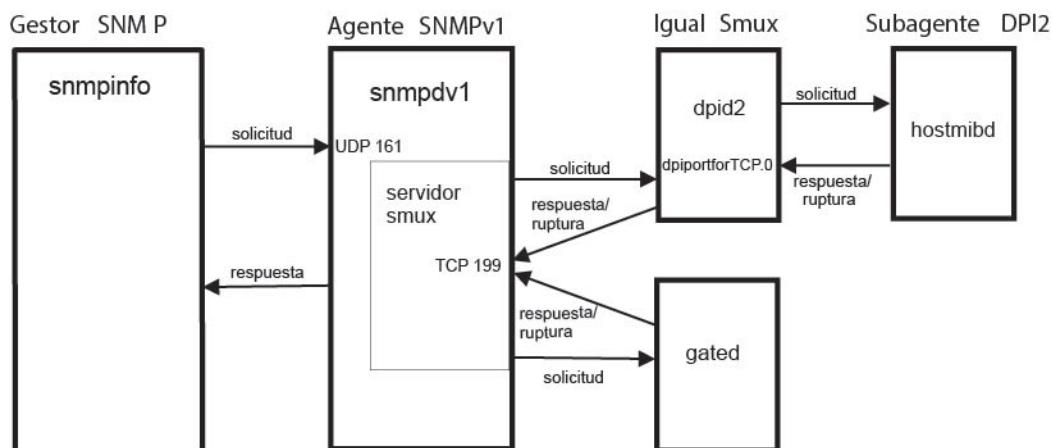


Figura 28. Partes principales de la arquitectura de SNMPv1

Esta ilustración muestra un ejemplo de la arquitectura de **SNMPv1**. Se muestran el subagente DPI2, el igual smux, el gestor **SNMP** y el agente **SNMP**. Además, se muestra cómo se comunican entre ellos.

El daemon **SNMP** recibe y transmite todos los mensajes de protocolo **SNMP** mediante el **UDP (User Datagram Protocol) de TCP/IP (Transmission Control Protocol/Internet Protocol)**. Las peticiones se aceptan en el puerto conocido públicamente 161. Las rupturas se transmiten a los sistemas principales listados en las entradas de ruptura en el archivo /etc/snmpd.conf que escuchan en el puerto conocido públicamente 162.

Cuando se recibe una petición, se comprueban la dirección IP de origen y el nombre de comunidad en una lista que contiene las direcciones IP, los nombres de comunidad, los permisos y las vistas tal como se especifican en las entradas de comunidad y vista del archivo `/etc/snmpd.conf`. El agente `snmpd` lee este archivo en el arranque y en un mandato `refresh` o una señal `kill -1`. Si no se encuentra ninguna entrada coincidente, se ignora la petición. Si se encuentra una entrada coincidente, se permite el acceso de acuerdo con los permisos especificados en las entradas de comunidad y vista para dicha asociación de dirección IP, comunidad y nombre de vista en el archivo `/etc/snmpd.conf`. El mensaje y la PDU se deben codificar de acuerdo con las normas ASN.1.

Este esquema de autenticación no está destinado a proporcionar seguridad completa. Si se utiliza el daemon **SNMP** sólo para las peticiones get y get-next, es posible que la seguridad no sea ningún problema. Si se permiten peticiones set, se puede restringir el privilegio set.

Consulte el archivo `/etc/snmpd.conf` en *Files Reference* para obtener más información. Consulte el apartado *Management Information Base (MIB)* en la publicación *Communications Programming Concepts* para obtener más información.

#### **Proceso de petición SNMP**

Existen tres tipos de PDU de petición que el daemon **SNMP** puede recibir.

Los tipos de petición se definen en RFC 1157 y todas las PDU tienen el formato siguiente:

Tabla 84. Formato de PDU de petición			
request-ID	error-status	error-index	variable-bindings
GET	0	0	<i>ListaEnlacesVar</i>
GET-NEXT	0	0	<i>ListaEnlacesVar</i>
SET	0	0	<i>ListaEnlacesVar</i>

El campo request-ID (ID de petición) identifica la naturaleza de la petición; el campo error-status (estado de error) y el campo error-index (índice de error) no se utilizan y se deben establecer en 0 (cero); y el campo variable-bindings (enlaces de variable) contiene una lista de longitud variable de ID de instancia de formato numérico cuyos valores se están solicitando. Si el valor del campo request-ID es SET, el campo variable-bindings es una lista de pares de ID de instancia y valores.

Lea el apartado *Utilización de la base de datos de Management Information Base (MIB)* en la publicación *Communications Programming Concepts* para obtener una descripción de los tres tipos de petición.

#### **Proceso de respuesta SNMP**

Los PDU de respuesta tienen casi el mismo formato que los PDU de petición.

Tabla 85. Formato de PDU de respuesta			
request-ID	error-status	error-index	variable-bindings
GET-RESPONSE	<i>EstadoError</i>	<i>ÍndiceError</i>	<i>ListaEnlacesVar</i>

Si la petición se ha procesado satisfactoriamente, el valor del campo error-status y error-index es 0 (cero) y el campo de variable-bindings contiene una lista completa de pares de ID de instancia y valores.

Si cualquier ID de instancia del campo variable-bindings del PDU de petición no se ha procesado satisfactoriamente, el agente SNMP deja de procesarse, graba el índice del ID de instancia anómalo en el campo error-index, registra un código de error en el campo error-status y copia la lista de resultados parcialmente completada en el campo variable-bindings.

La RFC 1157 define los siguientes valores para el campo error-status:

Tabla 86. Valores para el campo error-status

Valor	Valor	Explicación
<i>noError</i>	0	Proceso completado satisfactoriamente (error-index es 0).
<i>tooBig</i>	1	El tamaño de PDU de respuesta excederá un límite definido de implementación (error-index es 0).
<i>noSuchName</i>	2	Un ID de instancia no existe en la vista MIB pertinente para los tipos de petición GET y SET o no tiene sucesores en el árbol MIB en la vista MIB pertinente para las peticiones GET-NEXT (error-index distinto de cero).
<i>badValue</i>	3	Sólo para peticiones SET, un valor especificado es sintácticamente incompatible con el atributo de tipo del ID de instancia correspondiente (error-index distinto de cero).
<i>readOnly</i>	4	No definido.
<i>genErr</i>	5	Se ha producido un error definido por implementación (error-index distinto de cero); por ejemplo, un intento de asignación de un valor que excede los límites de implementación.

#### Proceso de ruptura SNMP

Los PDU de ruptura los define la RFC 1157 para que tengan el formato mostrado en esta tabla.

Tabla 87. Formato de PDU de ruptura

enterprise	agent-address	generic-trap	specific-trap	time-stamp	variable-bindings
<i>ID de objeto</i>	<i>Entero</i>	<i>Entero</i>	<i>Entero</i>	<i>Impulsos de reloj</i>	<i>ListaEnlacesVar</i>

Los campos se utilizan del modo siguiente:

Item	Descripción
<i>enterprise</i>	Identificador de objeto asignado al proveedor que implementa el agente. Es el valor de la variable <b>sysObjectID</b> y es exclusivo para cada implementación de un agente <b>SNMP</b> . El valor asignado a esta implementación del agente es <b>1.3.6.1.4.1.2.3.1.2.1.1.3</b> o <b>risc6000snmpd.3</b> .
<i>agent-address</i>	Dirección IP del objeto que genera la ruptura.

<b>Item</b>	<b>Descripción</b>
<i>generic-trap</i>	Entero, como se indica a continuación:
<b>0</b>	<i>arranqueFrío</i>
<b>1</b>	<i>arranqueCaliente</i>
<b>2</b>	<i>enlaceInactivo</i>
<b>3</b>	<i>enlaceActivo</i>
<b>4</b>	<i>anomalíaAutentificación</i>
<b>5</b>	<i>pérdidaVecinoEgp</i>
<b>6</b>	<i>específicoEmpresa</i>
<i>specific-trap</i>	No utilizado, reservado para desarrollo futuro.
<i>time-stamp</i>	Tiempo transcurrido, en centésimas de segundo, desde la última reinicialización del agente hasta el suceso que genera la ruptura.
<i>variable-bindings</i>	Información adicional, dependiente del tipo <i>generic-trap</i> .

Los siguientes valores de generic-trap indican que se han detectado determinados sucesos del sistema:

<b>Item</b>	<b>Descripción</b>
<i>arranqueFrío</i>	El agente se está reinicializando. Los datos de configuración y/o valores de variable MIB pueden haber cambiado. Reinicie los periodos de medición.
<i>arranqueCaliente</i>	El agente se está reinicializando pero los datos de configuración o los valores de variable MIB no han cambiado. En esta implementación del agente <b>SNMP</b> , se genera una ruptura <i>arranqueCaliente</i> cuando se vuelve a leer el archivo /etc/snmpd.conf. La información de configuración del archivo /etc/snmpd.conf es para configuración de agente que no tenga efectos secundarios en las bases de datos de gestor SNMP. Los periodos de medición no se deben reiniciar.
<i>enlaceInactivo</i>	El agente ha detectado que se ha inhabilitado una interfaz de comunicaciones conocida.
<i>enlaceActivo</i>	El agente ha detectado que se ha habilitado una interfaz de comunicaciones conocida.
<i>anomalíaAutentificación</i>	Se ha recibido un mensaje que no se ha podido autenticar.
<i>pérdidaVecinoEgp</i>	Se ha perdido un vecino de <b>Exterior Gateway Protocol (EGP)</b> . Este valor sólo se genera cuando el agente se ejecuta en un sistema principal que ejecuta el daemon <b>gated</b> utilizando <b>EGP</b> .
<i>específicoEmpresa</i>	No se implementa; reservado para uso futuro.

Las rupturas *enlaceInactivo* y *enlaceActivo* contienen un solo par de ID/valor de instancia en la lista de vinculaciones de variables (variable-bindings). El ID de instancia identifica el **ifIndex** del adaptador que se ha inhabilitado o habilitado y el valor es el valor **ifIndex**. La ruptura para *pérdidaVecinoEgp* también

contiene una vinculación que consta del ID de instancia y del valor de *egpNeighAddr* para el vecino perdido.

#### **Soporte de daemon SNMP para la familia EGP de variables MIB**

Si el sistema principal de agente ejecuta el daemon **gated** con el **EGP (Exterior Gateway Protocol - Protocolo de pasarela exterior)** habilitado, hay varias variables MIB (Management Information Base - Base de información de gestión) en el grupo **EGP** soportado por el daemon **gated** a las que el agente **snmpd** puede acceder.

Las siguientes variables MIB de **EGP** tienen una sola instancia exclusiva:

Item	Descripción
<b>egpInMsgs</b>	Número de mensajes <b>EGP</b> recibidos sin error.
<b>egpInErrors</b>	Número de mensajes <b>EGP</b> erróneos recibidos.
<b>egpOutMsgs</b>	Número total de mensajes <b>EGP</b> transmitidos por el daemon <b>gated</b> que se ejecuta en el sistema principal del agente.
<b>egpOutErrors</b>	Número de mensajes <b>EGP</b> que el daemon <b>gated</b> de sistema principal de agente no ha podido enviar debido a las limitaciones de recursos.
<b>egpAs</b>	Número de sistema autónomo del daemon <b>gated</b> de sistema principal de agente.

Las siguientes variables MIB de **EGP** tienen una instancia para cada igual o vecino de **EGP** obtenido por el daemon **gated** de sistema principal de agente:

Item	Descripción
<b>egpNeighState</b>	Estado de este igual de <b>EGP</b> : <b>1</b> desocupado <b>2</b> adquisición <b>3</b> down <b>4</b> up <b>5</b> cese.
<b>egpNeighAddr</b>	Dirección IP de este igual de <b>EGP</b> .
<b>egpNeighAs</b>	Número de sistema autónomo de este igual de <b>EGP</b> . Cero (0) indica que el número de sistema autónomo de este igual aún no se conoce.
<b>egpInNeighMsgs</b>	Número de mensajes de <b>EGP</b> recibidos sin error desde este igual de <b>EGP</b> .
<b>egpNeighInErrs</b>	Número de mensajes de <b>EGP</b> erróneos recibidos de este igual de <b>EGP</b> .
<b>egpNeighOutMsgs</b>	Número de mensajes de <b>EGP</b> generados localmente enviados a este igual de <b>EGP</b> .
<b>egpNeighOutErrs</b>	Número de mensajes de <b>EGP</b> generados localmente no enviados a este igual de <b>EGP</b> debido a limitaciones de recursos.
<b>egpNeighInErrMsgs</b>	Número de mensajes de error definidos por <b>EGP</b> recibidos de este igual de <b>EGP</b>

Item	Descripción
<b>egpNeighOutErrMsgs</b>	Número de mensajes de error definidos por <b>EGP</b> enviados a este igual de <b>EGP</b> .
<b>egpNeighStateUp</b>	Número de transiciones de estado de <b>EGP</b> al estado UP con este igual de <b>EGP</b> .
<b>egpNeighStateDowns</b>	Número de transiciones de estado de <b>EGP</b> del estado UP a cualquier otro estado con este igual de <b>EGP</b> .
<b>egpNeighIntervalHello</b>	Intervalo entre retransmisiones de mandato Hello de <b>EGP</b> en centésimas de segundo.
<b>egpNeighIntervalPoll</b>	Intervalo entre retransmisiones de mandato poll de <b>EGP</b> en centésimas de segundo.
<b>egpNeighMode</b>	Modalidad de sondeo de este igual de <b>EGP</b> . Esta modalidad puede ser activa (1) o pasiva (2).
<b>egpNeighEventTrigger</b>	La variable de control activa sucesos de inicio y detención iniciados por el operador en este igual de <b>EGP</b> . Esta variable MIB se puede establecer para iniciarse (1) o detenerse(2).

Si el daemon **gated** no está en ejecución o si el daemon **gated** está en ejecución pero no está configurado para comunicarse con el agente **snmpd** o si el daemon **gated** no está configurado para **EGP**, las solicitudes de obtención y establecimiento de los valores de estas variables devolverán el código de respuesta de error *noSuchName*.

El archivo de configuración de daemon **gated**, /etc/gated.conf, debe contener la sentencia siguiente:

```
snmp      yes;
```

El daemon **gated** está configurado internamente para ser un igual de protocolo SMUX (single multiplexer - multiplexor individual) de SNMP (Simple Network Management Protocol - Protocolo simple de gestión de red) o un agente proxy del daemon **snmpd**. Cuando el daemon **gated** arranca, registra el árbol de variable *ipRouteTable* de MIB en el agente **snmpd**. Si el daemon **gated** se configura para **EGP**, el daemon **gated** también registra el árbol de variable **EGP** de MIB. Cuando este registro se ha completado, un gestor SNMP puede realizar de forma satisfactoria solicitudes al agente **snmpd** para las variables *ipRouteTable* y **EGP** de MIB soportadas por este daemon **gated** de sistema principal de agente. Cuando el daemon **gated** está en ejecución, toda la información de direccionamiento de MIB se obtiene utilizando el daemon **gated**. En este caso, no se permiten solicitudes de establecimiento a *ipRouteTable*.

Las comunicaciones SMUX entre el daemon **gated** y el daemon **snmpd** tienen lugar a través del puerto 199 conocido de TCP (Transmission Control Protocol). Si el daemon **gated** termina, **snmpd** elimina inmediatamente los registros de los árboles que el daemon **gated** ha registrado anteriormente. Si se inicia el daemon **gated** antes que el daemon **snmpd**, el daemon **gated** comprueba periódicamente el daemon **snmpd** hasta que se puede establecer la asociación SMUX.

Para configurar el agente **snmpd** de forma que reconozca y permita la asociación SMUX con el cliente de daemon **gated**, el usuario debe añadir una entrada SMUX en el archivo /etc/snmpd.conf. El identificador y la contraseña de objeto de cliente especificados en esta entrada SMUX para el daemon **gated** deben coincidir con los especificados en el archivo /etc/snmpd.peers.

El agente **snmpd** soporta solicitudes de establecimiento para las siguientes variables MIB I y MIB II de lectura y grabación:

#### **sysContact**

Identificación de texto de la persona de contacto para este sistema principal de agente. Esta información incluye el nombre de esta persona y el modo de ponerse en contacto con esta persona: por ejemplo, "José Pérez, 555-5555, ext 5." El valor está limitado a 256 caracteres. En el caso de una solicitud de establecimiento, si la serie correspondiente a esta variable MIB tiene más de 256 caracteres, el agente **snmpd** devolverá el error *badValue* y la operación de establecimiento no se

realizará. El valor inicial de *sysContact* se define en */etc.snmp.conf*. Si no se define nada, el valor es una serie nula.

Instancia	Valor	Acción
0	"string"	La variable MIB se establece en "string".

#### **sysName**

Nombre para este sistema principal de agente. Normalmente es el nombre de dominio totalmente calificado del nodo. El valor está limitado a 256 caracteres. En el caso de una solicitud de establecimiento, si la serie correspondiente a esta variable MIB tiene más de 256 caracteres, el agente **snmpd** devuelve el error *badValue* y la operación de establecimiento no se realiza.

Instancia	Valor	Acción
0	"string"	La variable MIB se establece en "string".

#### **sysLocation**

Serie de texto que indica la ubicación física de la máquina en la que reside este agente **snmpd**: por ejemplo "Sitio de Austin, edificio 802, sala 3C-23." El valor está limitado a 256 caracteres. En el caso de una solicitud de establecimiento, si la serie correspondiente a esta variable MIB tiene más de 256 caracteres, el agente **snmpd** devuelve el error *badValue* y la operación de establecimiento no se realiza. El valor inicial de *sysLocation* se define en */etc/snmp.conf*. Si no se define nada, el valor es una serie nula.

Instancia	Valor	Acción
0	"string"	La variable MIB se establece en "string".

#### **ifAdminStatus**

Estado deseado de un adaptador de interfaz en el sistema principal del agente. Los estados soportados son activo (up) e inactivo (down). El estado se puede establecer en probar pero una acción de este tipo no tiene ningún efecto en el estado operativo de la interfaz.

Instancia	Valor	Acción
f	1	El adaptador de interfaz con <b>ifIndex f</b> está habilitado.

**Nota:** Es posible que el valor de *ifAdminStatus* se pueda establecer en activo o inactivo, aunque el cambio operativo real de la interfaz haya fallado. En tal caso, es posible que una solicitud de obtención de *ifAdminStatus* refleje *up* mientras que una solicitud *ifOperStatus* para dicha interfaz refleja *down*. Si se produce una situación de este tipo, el administrador de red emitirá otra solicitud de establecimiento para establecer *ifAdminStatus* en activo (up) a fin de intentar otra vez el cambio operativo.

#### **atPhysAddress**

Parte de dirección de hardware de un enlace de tabla de direcciones en el sistema principal de agente (una entrada de la tabla de Protocolo de resolución de direcciones). Es la misma variable MIB que *ipNetToMediaPhysAddress*.

Instancia	Valor	Acción
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Para la interfaz con <b>ifIndex f</b> , cualquier enlace de tabla ARP existente para la dirección IP n.n.n.n se sustituye por el enlace (n.n.n.n, hh:hh:hh:hh:hh:hh). Si no existía ningún enlace, se añade el nuevo enlace. hh:hh:hh:hh:hh:hh es una dirección de hardware de doce dígitos hexadecimales.

#### atN0etAddress

Dirección IP correspondiente al hardware o a la dirección física especificada en *atPhysAddress*. Es la misma variable MIB que *ipNetToMediaNetAddress*.

Instancia	Valor	Acción
f.1.n.n.n.n	m.m.m.m	Para la interfaz con <b>ifIndex f</b> , se sustituye una entrada de tabla ARP existente para la dirección IP n.n.n.n por la dirección IP m.m.m.m.

#### ipForwarding

Indica si este sistema principal de agente está reenviando datagramas.

Tabla 88. ipforwarding		
Instancia	Valor	Acción
0	1	Si el sistema principal de agente tiene más de una interfaz activa, el kernel <b>TCP/IP</b> se configura para reenviar paquetes. Si el sistema principal de agente sólo tiene una interfaz activa, la solicitud de establecimiento falla.
0	2	El kernel <b>TCP/IP</b> en el sistema principal de agente se configura para no reenviar paquetes.

#### ipDefaultTTL

Valor de tiempo de vida (TTL) predeterminado insertado en las cabeceras IP de los datagramas originados por el sistema principal de agente.

Instancia	Valor	Acción
0	n	El valor de tiempo de vida predeterminado utilizado por el soporte de protocolo IP se establece en el entero n.

#### ipRouteDest

Dirección IP de destino de una ruta de la tabla de rutas.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n.n.n.n	m.m.m.m	La ruta de destino para la ruta n.n.n.n se establece en la dirección IP m.m.m.m.

#### **ipRouteNextHop**

Pasarela mediante la cual se puede alcanzar una dirección IP de destino desde el sistema principal de agente (una entrada en la tabla de rutas).

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n.n.n.n	m.m.m.m	La entrada de tabla de rutas para alcanzar la red n.n.n.n utilizando la pasarela m.m.m.m se añade a la tabla de rutas. La parte de sistema principal de la dirección IP n.n.n.n debe ser 0 para indicar una dirección de red.

#### **ipRouteType**

Estado de una entrada de tabla de rutas en el sistema principal de agente (se utiliza para suprimir entradas).

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
h.h.h.h	1	Se suprime cualquier ruta a la dirección IP de sistema principal h.h.h.h.
n.n.n.n	2	Se suprime cualquier ruta a la dirección IP de sistema principal n.n.n.n.

#### **ipNetToMediaPhysAddress**

Parte de dirección de hardware de un enlace de tabla de direcciones en el sistema principal de agente (una entrada en la tabla ARP). Es la misma variable MIB que *atPhysAddress*.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Para la interfaz con <b>ifIndex f</b> , cualquier enlace de tabla ARP existente para la dirección IP n.n.n.n se sustituye por el enlace (n.n.n.n, hh:hh:hh:hh:hh:hh). Si no existía ningún enlace, se añade el nuevo enlace. hh:hh:hh:hh:hh:hh es una dirección de hardware de 12 dígitos hexadecimales.

#### **ipNetToMediaNetAddress**

Dirección IP correspondiente al hardware o a la dirección física especificada en *ipNetToMediaPhysAddress*. Es la misma variable MIB que *atNetAddress*.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
f.1.n.n.n.n	m.m.m.m	Para la interfaz con <b>ifIndex f</b> , se sustituye una entrada de tabla ARP existente para la dirección IP n.n.n.n por la dirección IP m.m.m.m.

**ipNetToMediaType**

Tipo de correlación de la dirección IP con la dirección física.

Instancia	Valor	Acción
f.1.n.n.n.n	1	Para la interfaz con <b>ifIndex f</b> , correspondiente a un enlace ARP existente de la dirección IP a la dirección física, el tipo de correlación se establece en 1, o otra.
f.1.n.n.n.n	2	Para la interfaz con <b>ifIndex f</b> , correspondiente a un enlace ARP existente de la dirección IP a la dirección física, el tipo de correlación se establece en 2, o no válida. Como efecto secundario, la entrada correspondiente en <b>ipNetMediaTable</b> se invalida; es decir, la interfaz se desasocia de esta entrada <b>ipNetToMediaTable</b> .
f.1.n.n.n.n	3	Para la interfaz con <b>ifIndex f</b> , correspondiente a un enlace ARP existente de la dirección IP a la dirección física, el tipo de correlación se establece en 3, o dinámica.
f.1.n.n.n.n	4	Para la interfaz con <b>ifIndex f</b> , correspondiente a un enlace ARP existente de la dirección IP a la dirección física, el tipo de correlación se establece en 4, o estática.

**snmpEnableAuthenTraps**

Indica si el agente **snmpd** está configurado para generar rupturas *authenticationFailure*.

Instancia	Valor	Acción
0	1	El agente <b>snmpd</b> generará rupturas de anomalía de autentificación.
0	2	El agente <b>snmpd</b> no generará rupturas de anomalía de autentificación.

**smuxPstatus**

Estado de un igual de protocolo SMUX (utilizado para suprimir iguales de SMUX).

Instancia	Valor	Acción
n	1	El agente <b>snmpd</b> no hace nada.
n	2	El agente <b>snmpd</b> deja de comunicarse con el igual de SMUX n.

**smuxTstatus**

Estado de un árbol MIB de SMUX (utilizado para suprimir montajes de árbol MIB).

Instancia	Valor	Acción
l.m.m.m._ _ _ .p	1	El agente <b>snmpd</b> no hace nada.
l.m.m.m._ _ _ .p	2	Desmonta el montaje de SMUX del árbol MIB m.m.m... donde l es la longitud de la instancia de árbol MIB y p es smuxTpriority.

Las variables siguientes son variables que se pueden establecer tal como se define en la RFC 1229. El daemon **snmpd** permite al usuario establecer estas variables. Es posible que el dispositivo subyacente no permita el establecimiento de dichas variables. Compruebe cada dispositivo para ver qué se soporta y qué no se soporta.

**ifExtnsPromiscuous**

Estado de la modalidad promiscua en un dispositivo determinado. Se utiliza para habilitar e inhabilitar la modalidad promiscua en un dispositivo determinado. La acción **snmpd** es final y completa. Cuando se indica a **snmpd** que se desactive, la modalidad promiscua se desactiva de forma completa independientemente de las demás aplicaciones de la máquina.

Instancia	Valor	Acción
n	1	Activa la modalidad promiscua para el dispositivo n.
n	2	Desactiva la modalidad promiscua para el dispositivo n.

**ifExtnsTestType**

Variable de iniciación de prueba. Cuando se establece esta variable, se ejecuta la prueba apropiada para dicho dispositivo. Un identificador de objeto es el valor de la variable. El valor específico depende del tipo de dispositivo y de la prueba que se deba ejecutar. Actualmente, la única prueba definida que **snmpd** conoce para ejecutar es la prueba testFullDuplexLoopBack.

Instancia	Valor	Acción
n	oid	Iniciar la prueba especificada por oid.

**ifExtnsRcvAddrStatus**

Variable de estado de dirección. Cuando se establece esta variable, la dirección especificada entra en vigor con el nivel de duración apropiado. **snmpd** sólo permite el establecimiento de direcciones temporales porque no puede establecer registros ODM (Gestor de datos objeto) de dispositivo y sólo se le permite establecer direcciones de difusión o multidifusión.

Instancia	Valor	Acción
n.m.m.m.m.m. m	1	Añadir la dirección como algo distinto de una dirección temporal o permanente.
n.m.m.m.m.m. m	2	Eliminar la dirección del uso.
n.m.m.m.m.m. m	3	Añadir la dirección como dirección temporal.
n.m.m.m.m.m. m	4	Añadir la dirección como dirección permanente.

Las variables listadas más abajo son los valores que se pueden establecer tal como se define en la RFC 1231. El daemon **snmpd** permite al usuario establecer estas variables. Es posible que el dispositivo subyacente no permita el establecimiento de dichas variables. Deberá comprobar cada dispositivo para ver qué se soporta.

**dot5Commands**

El mandato que debe realizar el dispositivo de red en anillo.

Instancia	Valor	Acción
n	1	No realiza nada Devuelto.
n	2	Indica al dispositivo de red en anillo que se abra.
n	3	Indica a la red en anillo que se restablezca.
n	4	Indica a la red en anillo que se cierre.

**dot5RingSpeed**

Velocidad o ancho de banda actual del anillo.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n	1	Velocidad desconocida.
n	2	Velocidad de anillo de 1 megabit.
n	3	Velocidad de anillo de 4 megabits.
n	4	Velocidad de anillo de 16 megabits.

#### **dot5ActMonParticipate**

El objeto especifica si el dispositivo participa en el proceso de selección de supervisor activo.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n	1	Participa.
n	2	No participa.

#### **dot5Functional**

La máscara funcional que permite al dispositivo de red en anillo especificar de qué direcciones recibe tramas.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n	m.m.m.m.m.m	Máscara funcional que se debe establecer.

Las siguientes variables de manipulaciones de temporizador complejas se definen en la RFC como de sólo lectura pero se aconseja que las haga de lectura y grabación. Revise la RFC para obtener información completa de las interacciones. **snmpd** permite al solicitante establecerlas, pero es posible que el dispositivo no lo permita. Para obtener más información, consulte la documentación del controlador de dispositivo. Las variables son:

- dot5TimerReturnRepeat
- dot5TimerHolding
- dot5TimerQueuePDU
- dot5TimerValidTransmit
- dot5TimerNoToken
- dot5TimerActiveMon
- dot5TimerStandbyMon
- dot5TimerErrorReport
- dot5TimerBeaconTransmit
- dot5TimerBeaconReceive.

El daemon SNMP permite al usuario establecer las variables siguientes. El daemon utiliza el estándar del protocolo Station Management (SMT) 7.2 de FDDI para obtener la información y se determina a nivel de microcódigo. Consulte el microcódigo en la documentación de FDDI para asegurarse de que se está utilizando el microcódigo de SMT 7.2.

#### **fddimibSMTUserData**

Variable que contiene 32 bytes de información de usuario.

<b>Instancia</b>	<b>Valor</b>	<b>Acción</b>
n	string	Almacena 32 bytes de información de usuario.

#### **fddimibSMTConfigPolicy**

Estado de las políticas de configuración, específicamente el uso de mantenimiento de política.

Instancia	Valor	Acción
n	0	No utilizar la política de mantenimiento.
n	1	Utilizar la política de mantenimiento.

#### fddimibSMTConnectionPolicy

Estado de las políticas de conexión en el nodo FDDI. Consulte la RFC 1512 para obtener más información sobre los valores específicos que se pueden establecer.

Instancia	Valor	Acción
n	k	Define las políticas de conexión.

#### fddimibSMTTNotify

Temporizador, expresado en segundos, utilizando el protocolo de Notificación de vecino (Neighbor Notification). Tiene un rango de 2 a 30 segundos y el valor predeterminado es de 30 segundos.

Instancia	Valor	Acción
n	k	Define el valor de temporizador.

#### fddimibSMTStatRptPolicy

Estado de la generación de trama de informe de estado.

Instancia	Valor	Acción
n	1	Indica que el nodo genera tramas de informe de estado para sucesos implementados.
n	2	Indica que el nodo no crea tramas de informe de estado.

#### fddimibSMTTraceMaxExpiration

Esta variable define el valor máximo de caducidad de temporizador para el rastreo.

Instancia	Valor	Acción
n	k	Define la caducidad máxima de temporizador en milisegundos.

#### fddimibSMTStationAction

Esta variable hace que la entidad SMT realice una acción específica. Consulte la RFC para obtener información específica sobre esta variable.

Instancia	Valor	Acción
n	k	Define una acción en la entidad SMT. Los valores están en el rango de 1 a 8.

#### fddimibMACRequestedPaths

Define las vías de acceso en las que se debe insertar el MAC (control de acceso al medio).

Instancia	Valor	Acción
n.n	k	Define la vía de acceso solicitada para el MAC.

#### fddimibMACFrameErrorThreshold

Umbral para el momento en que se genera un informe de estado de MAC. Define el número del error que se debe producir antes de que se genere un informe.

Instancia	Valor	Acción
n.n	k	Define el número de errores que se deben observar antes de que se genere un informe de estado de MAC.

#### fddimibMACMAUnitdataEnable

Esta variable determina el valor del distintivo **MA\_UNITDATA\_Enable** en RMT. El valor predeterminado e inicial de este distintivo es true (1).

Instancia	Valor	Acción
n.n	1	Marca el distintivo MA_UNITDATA_Enable como verdadero (true).
n.n	2	Marca el distintivo MA_UNITDATA_Enable como falso (false).

#### fddimibMACNotCopiedThreshold

Umbral para determinar cuándo se genera un informe de condición de MAC.

Instancia	Valor	Acción
n.n	k	Define el número de errores que se deben observar antes de que se genere un informe de condición de MAC.

Las tres variables siguientes son variables de temporizador que son interactivas entre ellas. Antes de cambiar cualquiera de estas variables, deberá conocer con profundidad el significado de las mismas tal como se definen en la **RFC 1512**.

- fddimibPATHTVXLowerBound
- fddimibPATHTMaxLowerBound
- fddimibPATHMaxTReq

#### fddimibPORTConnectionPolicies

Especifica las políticas de conexión para el puerto especificado.

Instancia	Valor	Acción
n.n	k	Define las políticas de conexión para el puerto especificado.

#### fddimibPORTRequestedPaths

Esta variable es una lista de vías de acceso permitidas donde cada elemento de lista define las vías de acceso permitidas por el puerto. El primer octeto corresponde a `none', el segundo octeto a `tree' y el tercer octeto a `peer'.

Instancia	Valor	Acción
n.n	ccc	Define las vías de acceso de puerto.

#### fddimibPORTLerCutoff

Estimación de velocidad de error de enlace en la que se interrumpe una conexión de enlace. Está en un rango de  $10^{**}-4$  a  $10^{**}-15$  y se indica como el valor absoluto del logaritmo de base 10 (valor predeterminado de 7).

Item	Descripción	
Instancia	Valor	Acción

Item	Descripción	
n.n	k	Define el puerto LerCutoff.

#### fddimibPORTLerAlarm

Estimación de velocidad de error de enlace en la que una conexión de enlace genera una alarma. Está en un rango de 10\*\*-4 a 10\*\*-15 y se indica como valor absoluto del logaritmo de base 10 de la estimación (el valor predeterminado es 8).

Instancia	Valor	Acción
n.n	k	Define el puerto LerAlarm.

#### fddimibPORTAction

Esta variable hace que el puerto realice una acción específica. Consulte la RFC para obtener información específica sobre esta variable.

Instancia	Valor	Acción
n	k	Define una acción en el puerto definido. Los valores están en el rango de 1 a 6.

**Nota:** La RFC 1213 describe todas las variables de las tablas *atEntry* e *ipNetToMediaEntry* como de lectura y grabación. El soporte de establecimiento se implementa sólo para las variables de *atEntry*, *atPhysAddress* y *atNetAddress*, y las variables de *ipNetToMediaEntry*, *ipNetToMediaPhysAddress*, *ipNetToMediaNetAddress* e *ipNetToMediaType*. Para aceptar peticiones de establecimiento que pueden especificar los atributos no soportados restantes de estas dos tablas, las peticiones de establecimiento para las variables restantes se aceptan en *atIfIndex* e *ipNetToMediaIfIndex*. No se devuelve ninguna respuesta de error al originador de peticiones de establecimiento, pero una petición de obtención posterior mostrará que se conservan los valores originales.

En la tabla *ipRouteEntry*, la RFC 1213 describe todas las variables excepto *ipRouteProto* como de lectura y grabación. Como se ha mencionado más arriba, el soporte de establecimiento sólo se implementa para las variables *ipRouteDest*, *ipRouteNextHop* e *ipRouteType*. Para aceptar peticiones de establecimiento que pueden especificar varios atributos de ruta no soportados, se aceptan peticiones de establecimiento para las variables restantes de la tabla *ipRouteEntry*: *ipRouteIfIndex*, *ipRouteMetric1*, *ipRouteMetric2*, *ipRouteMetric3*, *ipRouteMetric4*, *ipRouteMetric5*, *ipRouteAge* e *ipRouteMask*. No se devuelve ninguna respuesta de error al originador de peticiones de establecimiento, pero una petición de obtención subsiguiente mostrará que se conservan los valores originales. El daemon **snmpd** no coordina el direccionamiento con el daemon **routed**. Si el daemon **gated** está en ejecución y ha registrado la *tablaRutaIp* en el daemon **snmpd**, no se permiten peticiones de establecimiento a la *tablaRutaIp*.

La RFC 1229 describe las variables que se pueden establecer permitidas por **snmpd**. Consulte las entradas anteriores para conocer las desviaciones reales.

Los ejemplos siguientes utilizan el mandato **snmpinfo**. Se supone que el nombre de comunidad predeterminado **snmpinfo**, público, tiene acceso de lectura y grabación para el subárbol MIB respectivo.

```
snmpinfo -m set sysContact.0="Contacto principal: Bob Smith, teléfono oficina: 555-5555,
teléfono avisos: 9-123-4567. Contacto secundario: John Harris, teléfono: 555-1234."
```

Este mandato establece el valor de *sysContact*.0 en la serie especificada. Si ya existe una entrada para *sysContact*.0, se sustituye.

```
snmpinfo -m set sysName.0="bears.austin.ibm.com"
```

Este mandato establece el valor de *sysName*.0 en la serie especificada. Si ya existe una entrada para *sysName*.0, se sustituye.

```
snmpinfo -m set sysLocation.0="Recinto de Austin, edificio 802, lab 3C-23, esquina  
sureste de la sala."
```

Este mandato establece el valor de `sysLocation.0` en la serie especificada. Si ya existe una entrada para `sysLocation.0`, se sustituye.

```
snmpinfo -m set ifAdminStatus.2=2
```

Este mandato inhabilita el adaptador de interfaz de red que tiene el `ifIndex` de 2. Si el valor asignado es 1, se habilita el adaptador de interfaz.

```
snmpinfo -m set atPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00  
snmpinfo -m set ipNetToMediaPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00
```

Estos dos mandatos cambian la dirección de hardware en la entrada de tabla ARP para `192.100.154.2` a `02:60:8c:2e:c2:00`. Estos dos mandatos afectan a la misma entrada de tabla ARP. La variable MIB `atPhysAddress` es una variable en desuso y se sustituye por la variable MIB `ipNetToMediaPhysAddress`. De este modo, `atPhysAddress` e `ipNetToMediaPhysAddress` acceden a la misma estructura de la tabla ARP de kernel TCP/IP.

```
snmpinfo -m set atNetAddress.2.1.192.100.154.2=192.100.154.3  
snmpinfo -m set ipNetToMediaNetAddress.2.1.192.100.154.2=192.100.154.3
```

Estos mandatos cambian la dirección IP en la entrada de tabla ARP para `192.100.154.2` a `192.100.154.3`. Estos dos mandatos afectan a la misma entrada de tabla ARP. La variable MIB `atNetAddress` es una variable en desuso y se sustituye por la variable MIB `ipNetToMediaNetAddress`. De este modo, `atNetAddress` e `ipNetToMediaNetAddress` acceden a la misma estructura de la tabla ARP de kernel TCP/IP.

```
snmpinfo -m set ipForwarding.0=1
```

Este mandato establece el kernel **TCP/IP** para que pueda reenviar paquetes si el sistema principal de agente tiene más de una interfaz activa. Si el sistema principal sólo tiene una interfaz activa, la petición de establecimiento falla y el agente `snmpd` devuelve el error `badValue`.

```
snmpinfo -m set ipDefaultTTL=50
```

Este mandato permite que un datagrama IP que utiliza el tiempo de vida (TTL) predeterminado pase a través de un máximo de 50 pasarelas antes de que se descarte. Cuando cada pasarela procesa un datagrama, la pasarela resta 1 del campo de tiempo de vida. Además, cada pasarela reduce el campo de tiempo de vida en el número de segundos que el datagrama ha esperado servicio en dicha pasarela antes de que se pasara el datagrama al siguiente destino.

```
snmpinfo -m set ipRouteDest.192.100.154.0=192.100.154.5
```

Este mandato establece la dirección IP de destino de la ruta asociada con `192.100.154.0` en la dirección IP `192.100.154.5`, suponiendo que la ruta `192.100.154` ya exista.

```
snmpinfo -m set ipRouteNextHop.192.100.154.1=129.35.38.47
```

Este mandato establece una ruta al sistema principal `192.100.154.1` utilizando el sistema principal de pasarela `129.35.38.47`, suponiendo que la ruta `192.100.154.1` ya exista.

```
snmpinfo -m set ipRouteNextHop.192.100.154.0=192.100.154.7
```

Este mandato establece una ruta a la red de clase C `192.100.154` utilizando el sistema principal de pasarela `192.100.154.7`, suponiendo que la ruta `192.100.154.0` ya exista. Tenga en cuenta que la parte de sistema principal de la dirección debe ser 0 para indicar una dirección de red.

```
snmpinfo -m set ipRouteType.192.100.154.5=2
```

Este mandato suprime cualquier al sistema principal 192.100.154.5.

```
snmpinfo -m set ipRouteDest.129.35.128.1=129.35.128.1  
          ipRouteType.129.35.128.1=3  
          ipRouteNextHop.129.35.128.1=129.35.128.90
```

Este mandato crea una ruta nueva del sistema principal 129.35.128.90 a 129.35.128.1 como una pasarela.

```
snmpinfo -m set ipNetToMediaType.2.1.192.100.154.11=4
```

Este mandato establece la entrada de tabla ARP para 192.100.154.11 en estática.

```
snmpinfo -m set snmpEnableAuthenTraps=2
```

Este mandato hace que el agente **snmpd** del sistema principal especificado no genere rupturas *authenticationFailure*.

```
snmpinfo -m set smuxPstatus.1=2
```

Este mandato invalida SMUX peer 1. El resultado es que termina la conexión entre el agente **snmpd** y este SMUX peer.

```
snmpinfo -m set smuxTstatus.8.1.3.6.1.2.1.4.21.0=2
```

Este mandato invalida o elimina el montaje del árbol de SMUX 1.3.6.1.2.1.4.21, la tabla *ipRoute*. El primer número de la instancia indica el número de niveles del identificador del árbol de SMUX. El número final de la instancia indica smuxTpriority. En este ejemplo, hay 8 niveles en el identificador de árbol de SMUX: 1.3.6.1.2.1.4.21. La prioridad, 0, es la más alta.

```
snmpinfo -m set ifExtnsPromiscuous.1=1 ifExtnsPromiscuous.2=2
```

Este mandato activa la modalidad promiscua para el primer dispositivo en la tabla de interfaz y desactiva la modalidad promiscua para el segundo dispositivo en la tabla de interfaces.

```
snmpinfo -m set ifExtnsTestType.1=testFullDuplexLoopBack
```

Este mandato indica la prueba testFullDuplexLoopBack en la interfaz 1.

```
snmpinfo -m set ifExtnsRcvAddrStatus.1.129.35.128.1.3.2=2
```

Este mandato indica a la interfaz 1 que elimine la dirección física 129.35.128.1.3.2 de la lista de direcciones aceptables.

```
snmpinfo -m set dot5Commands.1=2
```

Este mandato indica a la primera interfaz que realice una apertura.

```
snmpinfo -m set dot5RingSpeed.1=2
```

Este mandato indica a la primera interfaz que establezca la velocidad de anillo en 1 megabit.

```
snmpinfo -m set dot5ActMonParticipate.1=1
```

Este mandato indica a la primera interfaz que participe en el proceso de selección de supervisor activo.

```
snmpinfo -m set dot5Functional.1=255.255.255.255.255.255
```

Este mandato establece la máscara de dirección funcional para permitirlo todo.

```
snmpinfo -m set fddimibSMTUserData.1="Datos de Gregorio"
```

Este mandato establece los datos de usuario de la primera entidad SMT en "Datos de Gregorio".

```
snmpinfo -m set fddimibMACFrameErrorThreshold.1.1=345
```

Este mandato establece el umbral para los errores de trama en 345 en el primer MAC de la primera entidad SMT.

**Nota:** Todas las variables descritas anteriormente se incluyen en uno de los métodos listados utilizados para establecer la variable.

Consulte el apartado “Address Resolution Protocol (Protocolo de resolución de direcciones)” en la página 150 y el apartado “Direcciones Internet” en la página 179 para obtener más información sobre protocolos y direcciones de Internet.

### Resolución de problemas de daemon SNMP

Los consejos de resolución de problemas para el daemon **SNMP** incluyen la resolución de problemas de terminación, problemas de acceso de variable MIB, problemas de acceso de variable MIB en la entrada de comunidad, problemas de noSuchName, problemas de falta de respuesta del agente y anomalías de daemon.

#### Problema de terminación de daemon

Si el agente **snmpd** no se comporta como se espera, consulte las sugerencias siguientes como ayuda para determinar y corregir el problema. Se recomienda encarecidamente que arranque el agente **snmpd** con algún tipo de registro cronológico. Si al invocar el daemon **snmpd** se producen problemas, se recomienda encarecidamente que el daemon **syslogd** se configure para el registro cronológico en el nivel de recurso de daemon y de gravedad de DEBUG.

Si el daemon **snmpd** termina tan pronto como se invoca, a continuación se proporcionan las razones posibles de la anomalía y las soluciones probables:

- La razón por la que el daemon **snmpd** ha terminado se registrará en el archivo de registro cronológico **snmpd** o el archivo de registro cronológico **syslogd** configurado. Consulte el archivo de registro para ver el mensaje de error **FATAL**.

*Solución:* Corrija el problema y reinicie el daemon **snmpd**.

- El uso de línea de mandatos de **snmpd** era incorrecto. Si se ha invocado el mandato **snmpd** sin el Controlador de recursos del sistema (SRC), la sentencia de uso necesaria se repite en eco en la pantalla. Si el daemon **snmpd** se ha invocado bajo el control de SRC, el mensaje de uso no se repite en eco en la pantalla. Consulte el archivo de registro para ver el mensaje de uso.

*Solución:* Invoque el mandato **snmpd** con la sentencia de uso correcta.

- El usuario root debe invocar el daemon **snmpd**.

*Solución:* Conmute al usuario root y reinicie el daemon **snmpd**.

- El archivo **snmpd.conf** debe ser propiedad del usuario root. El agente **snmpd** verifica la propiedad del archivo de configuración. Si el archivo no es propiedad del usuario root, el agente **snmpd** termina con un error muy grave.

*Solución:* Asegúrese de que es el usuario root, cambie la propiedad del archivo de configuración al usuario root y reinicie el daemon **snmpd**.

- El archivo **snmpd.conf** debe existir. Si el distintivo **-c** no se especifica en el archivo de configuración en la línea de mandatos **snmpd**, el archivo **/etc/snmpd.conf** no existe. Si el archivo **/etc/snmpd.conf** se elimina accidentalmente, vuelva a instalar la imagen **bos.net.tcp.client** o bien reconstruya el archivo con las entradas de configuración apropiadas como se han definido en la página de gestión de archivo **snmpd.conf**. Si el archivo de configuración se especifica con el distintivo **-c** en la línea de mandatos **snmpd**, asegúrese de que el archivo existe y que el archivo es propiedad del usuario root. Se debe especificar la vía de acceso y el nombre de archivo de configuración completos o, de lo contrario, se utilizará el archivo **/etc/snmpd.conf** predeterminado.

*Solución:* Asegúrese de que el archivo de configuración especificado existe y que este archivo es propiedad del usuario root. Reinicie el daemon **snmpd**.

- El udp port 161 ya está vinculado. Asegúrese de que el daemon **snmpd** aún no se esté ejecutando. Emite el mandato **ps -ef | grep snmpd** para determinar si ya se está ejecutando un proceso de daemon **snmpd**. Sólo se puede vincular un agente **snmpd** a udp port 161.

*Solución:* Mate el agente **snmpd** existente o no intente arrancar otro proceso de daemon **snmpd**.

### Problema de anomalía de daemon

Si el daemon **snmpd** falla cuando se emite una señal **refresh** o **kill -1**, las razones posibles de la anomalía y las soluciones probables son las siguientes:

- La razón de que el daemon **snmpd** terminara se anota en el archivo de registro **snmpd** o el archivo de registro **syslogd** configurado. Consulte el archivo de registro para ver el mensaje de error FATAL.

*Solución:* Corrija el problema y reinicie el daemon **snmpd**.

- Asegúrese de que se especifica la vía de acceso y el nombre completos del archivo de configuración cuando se invoca el daemon **snmpd**. El daemon **snmpd** se bifurca y cambia al directorio raíz en la invocación. Si no se especifica el nombre completo de vía de acceso del archivo de configuración, el agente **snmpd** no podrá encontrar el archivo en una renovación. Esto es un error muy grave y hará que el agente **snmpd** termine.

*Solución:* Especifique la vía de acceso y el nombre completos del archivo de configuración **snmpd**.

Asegúrese de que el archivo de configuración es propiedad del usuario root. Reinicie el daemon **snmpd**.

- Asegúrese de que el archivo de configuración **snmpd** aún existe. Es posible que el archivo se haya eliminado accidentalmente después de invocar el agente **snmpd**. Si el agente **snmpd** no puede abrir el archivo de configuración, el agente **snmpd** termina.

*Solución:* Vuelva a crear el archivo de configuración **snmpd**, asegúrese de que el archivo de configuración es propiedad del usuario root y reinicie el daemon **snmpd**.

### Problema de acceso de variables de MIB

Si no se puede acceder a las variables de MIB ( Management Information Base) desde el agente **snmpd**, si el agente **snmpd** está en ejecución pero la aplicación de gestor de **SNMP (Simple Network Management Protocol)** excede el tiempo de espera de una respuesta del agente **snmpd**, intente lo siguiente:

- Compruebe la configuración de red del sistema principal en el que se ejecuta el agente **snmpd** utilizando el mandato **netstat -in**. Verifique que el dispositivo lo0 de bucle de retorno, esté activo. Si el dispositivo está inactivo, se visualiza un \* (asterisco) a la izquierda de lo0. El lo0 debe estar activo para que el agente **snmpd** atienda las peticiones.

*Solución:* Emite el mandato siguiente para arrancar la interfaz de bucle de retorno:

```
ifconfig lo0 inet up
```

- Verifique que el daemon **snmpd** tenga una ruta al sistema principal donde se emiten las peticiones.

*Solución:* En el sistema principal donde se ejecuta el daemon **snmpd**, añada una ruta al sistema principal donde se emite el mandato **route add**. Para obtener más información, consulte el mandato **route**.

- Compruebe que el nombre de sistema principal y la dirección IP de sistema principal tengan el mismo valor.

*Solución:* Restablezca el nombre de sistema principal para que corresponda con la dirección IP de sistema principal.

- Compruebe que **sistemaprincipallocal** esté definido para ser la dirección IP lo0.

*Solución:* Defina **sistemaprincipallocal** para que sea la misma dirección utilizada por la dirección IP lo0 (generalmente 127.0.0.1).

### Problema de acceso de variables de MIB en entrada de comunidad

Si se especifica una entrada de comunidad en el archivo de configuración con un nombre de vista de MIB, pero no se puede acceder a las variables de MIB, compruebe lo siguiente:

- Asegúrese de hacer especificado correctamente la entrada de comunidad. Si ha especificado un nombre de vista en la entrada de comunidad, todos los campos de la comunidad son absolutamente necesarios.

*Solución:* Especifique todos los campos de la entrada de comunidad en el archivo de configuración. Renueve el agente **snmpd** y pruebe la petición otra vez.

- Asegúrese de que la modalidad de acceso de la entrada de comunidad corresponda con el tipo de petición. Si está emitiendo una petición **get** o **get-next**, asegúrese de que la comunidad tiene permiso de sólo lectura o de lectura y grabación. Si está emitiendo una petición **set**, asegúrese de que la comunidad tiene permiso de lectura y grabación.

*Solución:* Especifique la modalidad de acceso correcta en la entrada de comunidad. Renueve el agente **snmpd** y pruebe la petición otra vez.

- Asegúrese de que se especifique una entrada de vista para el nombre de vista especificado en la entrada de comunidad del archivo de configuración. Si hay un nombre de vista especificado en la entrada de comunidad, pero no hay ninguna entrada de vista correspondiente, el agente **snmpd** no permite el acceso para dicha comunidad. Es absolutamente necesaria una entrada de vista para un nombre de vista especificado en una entrada de comunidad en el archivo de configuración.

*Solución:* Especifique una entrada de vista para el nombre de vista especificado en la entrada de comunidad. Renueve el agente **snmpd** y pruebe la petición otra vez.

- Si se especifica **iso** como el subárbol de MIB para la entrada de vista, verifique que se especifique **iso.3**. La instancia de 3 es necesaria para que el agente **snmpd** acceda a la parte **org** del árbol **iso**.

*Solución:* Especifique el subárbol MIB como **iso.3** en la entrada de vista. Renueve el agente **snmpd** y pruebe la petición otra vez.

- Compruebe la *dirección IP* y la *máscara de subred* en la entrada de comunidad. Verifique que el sistema principal que emite la petición SNMP se incluye en la comunidad que se está especificando con el nombre de comunidad.

*Solución:* Cambie los campos *dirección IP* y *máscara de red* en la entrada de comunidad del archivo de configuración para incluir el sistema principal que está emitiendo la petición SNMP.

### Problema porque no hay respuesta del agente

Si la *dirección IP* de la comunidad se especifica como 0.0.0.0, pero no hay ninguna respuesta del agente **snmpd**, intente lo siguiente:

- Compruebe el campo *máscara de red* en la entrada de comunidad. Para el acceso general a este nombre de comunidad, la *máscara de red* debe ser **0.0.0.0**. Si se especifica que la *máscara de red* sea 255.255.255.255, el agente **snmpd** se configura para no permitir ninguna petición con el nombre de comunidad especificado.

*Solución:* Especifique la *máscara de red* en la entrada de comunidad en 0.0.0.0. Renueve el agente **snmpd** e intente la petición otra vez.

- Asegúrese de que la modalidad de acceso de la entrada de comunidad corresponda con el tipo de petición. Al emitir una petición **get** o **get-next**, asegúrese de que la comunidad tiene permiso de lectura sólo o de lectura y grabación. Si está emitiendo una petición **set**, asegúrese de que la comunidad tiene permiso de lectura y grabación.

*Solución:* especifique la modalidad de acceso correcta en la entrada de comunidad. Renueve el agente **snmpd** y pruebe la petición otra vez.

### Problema de noSuchName

Si, al intentar establecer una variable MIB que se supone que el agente **snmpd** soporta, se devuelve un mensaje de error **noSuchName**, la razón puede ser la siguiente:

La petición de establecimiento (set) emitida no incluía un nombre de comunidad para una comunidad válida con acceso de grabación. El protocolo **SNMP** dicta que a una petición de establecimiento con una comunidad con privilegios de acceso no apropiados se le responda con el mensaje de error **noSuchName**.

*Solución:* Emite la petición de establecimiento con un nombre de comunidad para una comunidad que tenga privilegios de grabación e incluya el sistema principal desde el que se ha emitido la petición de establecimiento.

## Sistema de archivos de red

NFS (Network File System - Sistema de archivos de red) es un mecanismo para almacenar archivos en una red. Es un sistema de archivos distribuido que permite a los usuarios acceder a los archivos y directorios ubicados en sistemas remotos y tratar dichos archivos y directorios como si fueran locales.

Por ejemplo, los usuarios pueden utilizar mandatos del sistema operativo para crear, eliminar, leer, grabar y establecer atributos de archivo para archivos y directorios remotos.

El paquete de software NFS incluye mandatos y daemons para NFS, NIS (Network Information Service) y otros servicios. Aunque NFS y NIS se instalan juntos como un paquete, cada uno es independiente y cada uno se configura y se administra individualmente.

AIX 5.3 y posterior soportan los protocolos NFS versión 2, 3 y 4. La versión 4 de NFS es la versión de NFS definida más recientemente y la describe RFC 3530. Más adelante en este apartado se describen detalles adicionales sobre el soporte AIX de NFS versión 4. Los clientes NFS utilizan de forma predeterminada el protocolo de NFS versión 3 .

### Servicios NFS

NFS proporciona los servicios mediante una relación de cliente-servidor.

Los sistemas que dejan los *sistemas de archivos* o los *directorios* y otros recursos disponibles para el acceso remoto se denominan *servidores*. La acción de dejar disponibles los sistemas de archivos se denomina *exportación*. Los sistemas y los procesos que utilizan recursos de servidor se consideran *clientes*. Una vez que un cliente monta un sistema de archivos que un servidor exporta, el cliente puede acceder a los archivos de servidor individuales (el acceso a los directorios exportados puede estar restringido a clientes específicos).

Los principales servicios proporcionados por NFS son:

Tabla 89. Servicios NFS	
Servicio	Descripción
<b>Servicio de montaje</b>	Monta desde el daemon <a href="#"><code>/usr/sbin/rpc.mountd</code></a> en el servidor y el mandato <a href="#"><code>/usr/sbin/mount</code></a> en el cliente. Este servicio sólo está disponible en NFS versión 2 y versión 3.
<b>Acceso a archivos remotos</b>	Accede desde el daemon <a href="#"><code>/usr/sbin/nfsd</code></a> en el servidor y el daemon <a href="#"><code>/usr/sbin/biod</code></a> en el cliente.
<b>Servicio de ejecución remota</b>	Ejecuta desde el daemon <a href="#"><code>/usr/sbin/rpc.rexd</code></a> en el servidor y el mandato <a href="#"><code>/usr/bin/on</code></a> en el cliente.
<b>Servicio de estadísticas de sistema remoto</b>	Compila desde el daemon <a href="#"><code>/usr/sbin/rpc.rstatd</code></a> en el servidor y el mandato <a href="#"><code>/usr/bin/rup</code></a> en el cliente.
<b>Servicio de listado de usuarios remotos</b>	Lista desde el daemon <a href="#"><code>/usr/lib/netsvc/rusers/rpc.rusersd</code></a> en el servidor y el mandato <a href="#"><code>/usr/bin/rusers</code></a> en el cliente.
<b>Servicio de parámetros de arranque</b>	Proporciona parámetros de arranque a clientes sin disco del sistema operativo Sun desde el daemon <a href="#"><code>/usr/sbin/rpc.bootparamd</code></a> en el servidor.
<b>Servicio Wall remoto</b>	Protege frente al daemon <a href="#"><code>/usr/lib/netsvc/rwall/rpc.rwalld</code></a> en el servidor y el mandato <a href="#"><code>/usr/sbin/rwall</code></a> en el cliente.

Tabla 89. Servicios NFS (continuación)	
Servicio	Descripción
<b>Servicio Spray</b>	Envía una corriente de una sola dirección de paquetes de Llamada a procedimiento remoto (RPC) del daemon <b>/usr/lib/netsvc/spray/rpc.sprayd</b> en el servidor y el mandato <b>/usr/sbin/spray</b> en el cliente.
<b>Servicio de autentificación de PC</b>	Proporciona un servicio de autentificación de usuario para PC-NFS desde el daemon <b>/usr/sbin/rpc.pcnfsd</b> en el servidor.
<b>Servicio de seguridad ampliada</b>	Proporciona acceso en el cliente y el servidor a servicios de seguridad más avanzados, por ejemplo Kerberos 5. El <b>/usr/sbin/gssd</b> proporciona a NFS acceso a los servicios de seguridad proporcionados por el Servicio de autentificación de red. Se deben instalar el Servicio de autentificación de red y los catálogos de archivos de Biblioteca criptográfica ( <b>krb5.client.rte</b> , <b>krb5.server.rte</b> y <b>modcrypt.base</b> ). Estos catálogos de archivos se pueden instalar desde el Expansion Pack de AIX.
<b>Servicio de conversión de identidad</b>	Realiza la conversión entre los principales de seguridad, las series de identidad de NFS versión 4 y los ID de sistema numéricos correspondientes. Además, se proporciona información de correlación de identidad de dominios NFS versión 4 externos. Estos servicios los proporciona el daemon <b>/usr/sbin/nfsrgyd</b> .

**Nota:** Un sistema puede ser un servidor NFS y un cliente NFS simultáneamente.

Los servidores NFS versión 2 y 3 son servidores *sin estado*, lo que significa que el servidor no retiene ninguna información de transacción sobre los clientes. Una sola transacción NFS corresponde a una sola operación de archivo completa. NFS necesita que el cliente recuerde cualquier información necesaria para uso posterior de NFS.

Un servidor NFS versión 4 es un servidor con estado debido a las operaciones de apertura de archivo y de bloqueo de archivo definidas en el protocolo NFS versión 4.

## Soporte de Listas de control de acceso de NFS

La implementación de AIX NFS versión 4 soporta dos tipos de ACL: NFS4 y AIXC.

El origen de autorización para la comprobación de acceso se encuentra en el sistema de archivos subyacente exportado por el servidor NFS. El sistema de archivos tiene en cuenta los controles de acceso (ACL o bits de permiso) del archivo, los credenciales del emisor de la llamada y otras restricciones del sistema local que puedan ser aplicables. Las aplicaciones y los usuarios no deben suponer que se puede utilizar el examen solo de ACL o de bits de modalidad de UNIX para pronosticar el acceso de forma concluyente.

Se pueden utilizar los mandatos **aclget**, **aclput** y **acledit** en el cliente para manipular las ACL de NFS o AIX. Para obtener más información, consulte el apartado sobre Listas de control de acceso en la publicación Security.

### NFS RBAC

NFS proporciona soporte al Control de accesos basados en roles (RBAC). Los mandatos del cliente y el servidor NFS están habilitados para RBAC.

Esto permite que los usuarios no root ejecuten mandatos NFS cuando el administrador haya asignado el rol RBAC del mandato al usuario. Para ver la lista de series y privilegios de autorización asociados a los mandatos NFS, consulte el archivo /etc/security/privcmds en el sistema.

### ACL NFS4

ACL NFS4 es la ACL definida por el protocolo de NFS versión 4.

Dado que ACL NFS4 es independiente de la plataforma, le pueden dar soporte los clientes o servidores de otros proveedores. Los clientes y servidores de NFS versión 4 no son necesarios para soportar ACL NFS4.

En un servidor AIX, si una instancia de sistema de archivos físicos subyacente soporta ACL NFS4, el servidor NFS4 de AIX soporta ACL NFS4 para dicha instancia de sistema de archivos. La mayoría de tipos de sistemas de archivos físicos de AIX no soportan ACL NFS4. Estos tipos de sistema de archivos incluyen pero no están limitados a CFS, UDF, JFS y JFS2 con la versión 1 de atributos ampliada. Todas las instancias de JFS2 con la versión 2 de atributos ampliada soportan ACL NFS4.

Los sistemas de archivos de cliente NFS versión 4 pueden leer y grabar la ACL NFS4 si la instancia de sistema de archivos de NFS versión 4 exportada en el servidor soporta ACL NFS4.

### **ACL de AIX**

La ACL de AIXC es una lista de control de acceso que es propietaria de los servidores AIX.

No la define el protocolo de NFS versión 4 y sólo la conocen los servidores y clientes AIX.

En un servidor NFS versión 4, se soporta la ACL de AIXC cuando la instancia de sistema de archivo subyacente soporta la ACL de AIXC. Todas las instancias de JFS y JFS2 soportan la ACL de AIXC.

Un cliente de NFS versión 4 tiene una opción de montaje que habilita o inhabilita el soporte para la ACL de AIX. El valor predeterminado es no soportar la ACL de AIXC. Un usuario de un sistema de archivos de cliente NFS versión 4 puede leer y grabar la ACL de AIXC cuando el cliente y el servidor ejecutan AIX, la instancia de sistema de archivos físico subyacente del servidor soporta la ACL de AIXC y el cliente AIX monta la instancia de sistema de archivos con la ACL de AIXC habilitada. El soporte ACL de AIXC en NFS versión 4 es similar al soporte de ACL de AIXC en las implementaciones de AIX NFS versión 2 y NFS versión 3.

Todas las instancias de un sistema de archivos JFS2 con la versión 2 de atributo ampliado soportan la ACL de AIXC y la ACL de NFS4. Un archivo en este tipo de sistema de archivos sólo puede tener bits de modalidad (no ACL), una ACL de NFS4 o una ACL de AIXC. Pero, no puede tener una ACL de NFS4 y una ACL de AIXC al mismo tiempo.

Se puede utilizar el mandato **ac1gettypes** para determinar los tipos de ACL que se pueden leer y grabar en una instancia de sistema de archivos. Es posible que este mandato devuelva salida diferente cuando se ejecuta localmente en un sistema de archivos físico en un servidor NFS versión 4 que cuando se ejecuta en el mismo sistema de archivos en un cliente NFS versión 4. Por ejemplo, una instancia de sistema de archivos de NFS versión 4 y un servidor NFS versión 4 pueden soportar la ACL de NFS4 y la ACL de AIXC, pero el cliente sólo está configurado para enviar y recibir la ACL de NFS4. En este caso, cuando se ejecuta el mandato **ac1gettypes** desde un sistema de archivos de cliente NFS versión 4, sólo se devuelve NFS4. Asimismo, si un usuario del cliente solicita una ACL de AIXC, se devuelve un error.

### **Soporte de sistema de archivos de antememoria**

El Sistema de archivos de antememoria (CacheFS) es un mecanismo de almacenamiento en antememoria de sistema de archivos de uso general que mejora el rendimiento y la escalabilidad del servidor NFS reduciendo la carga de servidor y de red.

Diseñado como un sistema de archivos de capas, CacheFS proporciona la posibilidad de almacenar un sistema de archivos en la antememoria de otro. En un entorno NFS, CacheFS incrementa la proporción de cliente por servidor, reduce las cargas de servidor y de red y mejora el rendimiento para clientes en enlaces lentos, por ejemplo el protocolo PPP (Point-to-Point Protocol).

Se crea una antememoria en la máquina cliente de modo que se pueda acceder localmente a los sistemas de archivos especificados para montarse en la antememoria en lugar de acceder a ellos a través de la red. Los archivos se colocan en la antememoria cuando un usuario solicita por primera vez acceso a ellos. La antememoria no se llena hasta que el usuario solicita el acceso a un archivo o a archivos. Las peticiones de archivo iniciales pueden parecer lentas, pero es posible que los usos posteriores de los mismos archivos sean más rápidos.

#### **Nota:**

1. No puede almacenar en antememoria los sistemas de archivos / (raíz) o /usr.
2. Sólo puede montar sistemas de archivos que son compartidos. (Consulte el mandato [exportfs](#).)
3. No hay ningún aumento de rendimiento al almacenar en antememoria un sistema de archivos de disco de JFS (Journalized File System - sistema de archivos diario) local.

4. Debe tener autorización de sistema o root para realizar las tareas de la tabla siguiente.

Tabla 90. Tareas de CacheFS		
Tarea	Vía rápida de SMIT	Mandato o archivo
Configurar una antememoria	cachefs_admin_create	<b>cfsadmin -c NombreDirectorioMontaje</b> <sup>1</sup> .
Especificación de archivos para montaje	cachefs_mount	<b>mount -F cachefs -o backfstype=TipoSistArchivos, cachedir= DirectorioAntememoria[,opciones]</b> BackFileSystem <i>NombreDirectorioMontaje</i> <sup>2</sup> o edite /etc/ <b>filesystems</b> .
Modificar la antememoria	cachefs_admin_change	Elimine la antememoria y, a continuación, vuelva a crearla utilizando las opciones de mandato <b>mount</b> apropiadas.
Visualizar información de antememoria	cachefs_admin_change	<b>cfsadmin -l NombreDirectorioMontaje</b> .
Eliminar una antememoria	cachefs_admin_remove	1. Desmonte el sistema de archivos: <b>umount NombreDirectorioMontaje</b> 2. Determine el ID de antememoria: <b>cfsadmin -1 NombreDirectorioMontaje</b> 3. Suprima el sistema de archivos: <b>cfsadmin -d IDAntememoria DirectorioAntememoria</b>
Comprobar integridad del sistema de archivos	cachefs_admin_check	<b>fsck_cachefs</b> <i>DirectorioAntememoria</i> <sup>3</sup> .

#### Notas:

1. Después de haber creado la antememoria, no realice ninguna operación en el propio directorio de antememoria (`cachedir`). Esto produce conflictos en el software CacheFS.
2. Si utiliza la opción de mandato **mount** para especificar archivos para montaje, se deberá volver a emitir el mandato cada vez que se reinicia el sistema.
3. Utilice las opciones **-m** o bien **-o** del mandato **fsck\_cachefs** para comprobar los sistemas de archivos sin realizar ninguna reparación.
4. Tras migrar el sistema a AIX Versión 6.1 o posterior desde versiones anteriores de AIX, los sistemas de archivos de antememoria antiguos que se crean en la versión más antigua de AIX deben eliminarse y volverse a crear.

## Soporte de archivos correlacionados NFS

El soporte de archivos correlacionados NFS permite a los programas de un cliente acceder a un archivo como si estuviera en la memoria.

Mediante la utilización de la subrutina `shmat`, los usuarios pueden correlacionar áreas de un archivo en el espacio de direcciones. Mientras un programa lee y graba en esta región de memoria, el archivo se lee en la memoria del servidor o se actualiza como sea necesario en el servidor.

La correlación de archivos a través de NFS está limitada de tres formas:

- Los archivos no comparten información bien entre clientes.
- Los cambios en un archivo de un cliente utilizando un archivo correlacionado no se ven en otro cliente.
- El bloqueo y el desbloqueo de regiones de un archivo no es un procedimiento efectivo para coordinar datos entre clientes.

Si se debe utilizar un archivo NFS para el compartimiento de datos entre programas de clientes diferentes, utilice el bloqueo de registro y las subrutinas `read` y `write` normales.

Varios programas en el mismo cliente pueden compartir datos de forma efectiva utilizando un archivo correlacionado. El bloqueo de registro de asesoramiento puede coordinar las actualizaciones en el archivo del cliente, a condición de que el archivo entero esté bloqueado. Varios clientes sólo pueden compartir archivos correlacionados de utilización de datos si los datos no cambian nunca, como en una base de datos estática.

## Servicio de proxy NFS

AIX proporciona soporte al servicio de proxy NFS (Network File System). Un servidor de AIX puede exportar simultáneamente sistemas de archivos y exportaciones de proxy accesibles localmente. Los clientes NFS pueden montar la vista de proxy exportada.

El servicio de proxy NFS de AIX utiliza el almacenamiento en antememoria de disco de los datos a los que se accede para atender localmente las peticiones subsiguientes similares con tráfico de red reducido en el servidor de componente de fondo. Potencialmente el servicio de proxy puede ampliar el acceso de datos NFS a redes más lentas y menos fiables con un rendimiento mejorado y un tráfico de red reducido en el servidor primario donde residen los datos. En función de la disponibilidad y de los requisitos de gestión de contenido, el servicio de proxy puede proporcionar una solución para ampliar el acceso de NFS a los límites de red sin necesidad de copiar datos. Puede configurar el servicio de proxy NFS de AIX utilizando el mandato **mknfsproxy**.

El almacenamiento en antememoria de proxy se puede utilizar con los protocolos de NFS v3 y NFS v4. El protocolo entre el proxy y los clientes conectados puede ser NFS v3 o NFS v4 cuando se utiliza el protocolo NFS v4 entre el proxy y el servidor de componente de fondo. Sin embargo, cuando se utiliza el protocolo NFS v3, el protocolo entre el proxy y los clientes conectados debe ser el protocolo NFS v3. Se soportan las lecturas y las grabaciones de datos además de los bloqueos de aviso de rango de bytes.

Se pueden utilizar los métodos de seguridad krb5, krb5i y krb5p entre el servidor proxy y sus clientes conectados. Estos métodos también se pueden utilizar entre el servidor proxy y el servidor principal. Utilizando tecnología de reenvío de tickets mediante proxy, puede autenticarse en el cliente y obtener autenticación para el servidor principal. Para beneficiarse de esta tecnología, utilice el mandato **kinit** con la opción `-f` cuando realice la autenticación de Kerberos. Si se utiliza la seguridad **auth\_sys** entre el proxy y el servidor de componente de fondo, cuando accede al servidor de componente de fondo, el servidor proxy correlaciona accesos de cliente de Kerberos con atributos **auth\_sys**. Para obtener resultados óptimos, el servidor proxy y el servidor de fondo deben compartir las mismas definiciones de identidad de usuario y grupo.

Se aplican las siguientes restricciones al servicio de proxy NFS:

- El servicio de proxy necesita clientes conectados mediante TCP.
- Puesto que el servicio de proxy proporciona un modo para que los clientes de NFS v3 naveguen por el espacio de nombres exportado de NFS v4 sin utilizar los mandatos **mount** y **umount**, debe utilizar el mandato **mknfsproxy** con la opción `mfsid` cuando construya el sistema de archivos de proxy.
- El sistema de archivos de antememoria utilizado con el servicio de proxy debe ser un sistema de archivos JFS ampliado (JFS2).
- El servicio de proxy ejecuta CacheFS sobre un cliente AIX montado en el servidor NFS de fondo. La característica de E/S simultánea (CIO), disponible con el cliente NFS de AIX, mejora el rendimiento de CacheFS. Es posible que los intentos de acceder directamente al montaje de cliente NFS subyacente fallen debido a conflictos con intentos abiertos de CIO.

## Tipos de montajes NFS

Existen tres tipos de montajes NFS: predefinidos, explícitos y automáticos.

Los montajes *predefinidos* se especifican en el archivo `/etc/filesystems`. Cada stanza (o entrada) de este archivo define las características de un montaje. En esta stanza se listan datos tales como el nombre de sistema principal, la vía de acceso remota, la vía de acceso local y cualquier opción de montaje. Se

utilizan montajes predefinidos siempre que se necesitan determinados montajes para el funcionamiento correcto de un cliente.

Los montajes *explícitos* atienden las necesidades del usuario root. Los montajes explícitos se suelen realizar durante cortos períodos de tiempo cuando se necesitan montajes ocasionales no planificados. Los montajes explícitos también se pueden utilizar si se necesita un montaje para tareas especiales y dicho montaje no está normalmente disponible en el cliente NFS. Estos montajes se suelen calificar totalmente en la línea de mandatos utilizando el mandato **mount** con toda la información necesaria. Los montajes explícitos no necesitan actualizar el archivo /etc/filesystems. Los sistemas de archivos montados explícitamente permanecen montados a menos que se desmonten explícitamente con el mandato **umount** o hasta que se reinicia el sistema.

Los montajes *automáticos* los controla el mandato **automount**, que hace que la extensión de kernel **AutoFS** supervise la actividad en directorios especificados. Si un programa o un usuario intenta acceder a un directorio que no está montado actualmente, **AutoFS** intercepta la petición, organiza el montaje del sistema de archivos y, a continuación, atiende la petición.

## Exportación y montaje de NFS

Para administrar NFS se deben conocer las tareas de exportación y montaje de directorios.

Un servidor NFS debe exportar un archivo o directorio, después de lo cual un cliente NFS puede montar ese archivo o directorio. En este apartado se incluyen más detalles sobre estos conceptos.

### Exportaciones de directorio NFS

La exportación de un directorio se realiza en el servidor NFS. La exportación de un directorio declara que un directorio del espacio de nombres del servidor está disponible para las máquinas cliente.

El directorio exportado se conoce como *exportación* e incluye bajo el directorio todos los archivos que residen en el sistema de archivos del directorio exportado.

Cada exportación también define restricciones de acceso. Por ejemplo, se pueden definir las restricciones siguientes:

- qué clientes pueden acceder al directorio exportado
- qué versiones de NFS debe utilizar el cliente para acceder al directorio
- si el cliente puede grabar archivos en la exportación
- qué métodos de seguridad debe utilizar el cliente para acceder a los directorios y archivos en la exportación

Para obtener una descripción completa de las restricciones de exportación permitidas y de la semántica de exportación, consulte la descripción del mandato **exportfs** y la descripción del archivo /etc(exports).

**Nota:** Cuando se modifican los atributos de una exportación, se debe volver a exportar el directorio para que el cambio entre en vigor. Es posible que sea necesario volver a exportar un directorio debido a los cambios en otros archivos o a cambios externos al servidor. Por ejemplo, si un nombre de cliente especificado en una lista de acceso es un grupo de redes (netgroup) definido en el archivo /etc/netgroup y la definición del grupo de clientes cambia, todas las exportaciones que utilicen dicho grupo de redes en una lista de acceso se deben volver a exportar para que el cambio entre en vigor.

De forma similar, si cambia la dirección IP de un cliente, todas las exportaciones que especifiquen dicho cliente en una lista de acceso se deben volver a exportar. La razón de ello es que el servidor NFS mantiene una antememoria de derechos de acceso de cliente en cada exportación. La antememoria se desecha en cada operación de desexportación o re-exportación. Si se modifican los derechos de acceso de una exportación, especialmente si cambia la dirección IP de un cliente o si se elimina un cliente de la lista de acceso, se deberá realizar una desexportación o re-exportación para que el acceso del cliente se refleje correctamente en la antememoria. Dado que el servidor NFS llama al daemon **rpc.mountd** para obtener los derechos de acceso de cada cliente, el daemon **rpc.mountd** debe estar en ejecución en el servidor incluso si el servidor sólo exporta sistemas de archivo para el acceso de NFS versión 4.

## **Montajes de directorio NFS**

Un cliente NFS puede montar un directorio que ha sido exportado por un servidor NFS. El montaje de un directorio deja los archivos que residen en el servidor NFS disponibles para un cliente NFS.

Un cliente puede acceder a los archivos de un servidor si los archivos han sido exportados por el servidor y las restricciones de exportación permiten al cliente tener acceso a los archivos de la exportación. Una vez que un cliente ha montado satisfactoriamente la exportación de un servidor en un punto de montaje del espacio de nombres, los archivos del servidor para dicha exportación existirán en el espacio de nombres del cliente y aparecerán como archivos en el sistema de archivos local.

Por ejemplo, suponga que desea exportar el directorio /tmp del servidor diamond y montar dicho directorio en el cliente clip como el directorio /mnt. En el servidor, escriba el mandato siguiente:

```
exportfs -i -o access=clip /tmp
```

Esto hace que el directorio /tmp esté disponible para el cliente.

En el cliente, escriba el mandato siguiente:

```
mount diamond:/tmp /mnt
```

Ahora los directorios y archivos del directorio /tmp del servidor aparecerán en el directorio /mnt del cliente.

### **Nota:**

1. Existen algunas diferencias entre las versiones 2 y 3 de NFS y la versión 4 de NFS en el modo en que se manejan los montajes. En las versiones 2 y 3 de NFS, el servidor exportaba los directorios que quería dejar disponibles para el montaje. Entonces el cliente de la versión 2 o 3 de NFS tenía que montar explícitamente cada exportación a la que quería acceder.

Con la versión 4 de NFS, el servidor sigue especificando los controles de exportación para cada directorio de servidor o sistema de archivos que se debe exportar para el acceso de NFS. Desde estos controles de exportación, el servidor presenta un solo árbol de directorio de todos los datos exportados llenando los huecos entre los directorios exportados. Este árbol se conoce como pseudosistema de archivos y se inicia en la pseudoráiz del servidor NFS versión 4. El modelo de pseudosistema de archivos NFS versión 4 permite a un cliente NFS versión 4, en función de la implementación, realizar un solo montaje de la pseudoráiz del servidor a fin de acceder a todos los datos exportados del servidor. El cliente NFS AIX soporta esta característica. El contenido real visto por el cliente depende de los controles de exportación del servidor.

2. NFS versión 4 no permite el montaje de archivo a archivo.

## **Montaje de NFS**

Los clientes acceden a los archivos del servidor montando primero los directorios exportados del servidor. Cuando un cliente monta un directorio, no realiza una copia de dicho directorio. En lugar de ello, el proceso de montaje utiliza una serie de llamadas a procedimiento remoto para permitir a un cliente acceder de forma transparente a los directorios del servidor.

A continuación se describe el proceso de montaje:

1. Cuando se inicia el servidor, el script /etc/rc.nfs ejecuta el mandato **exportfs**, que lee el archivo /etc(exports de servidor y, a continuación, indica al kernel qué directorios se deben exportar y qué restricciones de acceso necesitan.
2. Entonces el script /etc/rc.nfs inicia el daemon **rpc.mountd** y varios daemons **nfsd**.
3. A continuación, el script /etc/rc.nfs ejecuta el mandato **mount**, que lee los sistemas de archivo listados en el archivo /etc/filesystems.
4. El mandato **mount** localiza uno o varios servidores que exportan la información que el cliente desea y configura la comunicación entre él y dicho servidor.  
Este proceso se denomina *enlace*.
5. Entonces el mandato **mount** solicita que uno o varios servidores permitan al cliente acceder a los directorios del archivo /etc/filesystems de cliente.

6. El daemon de servidor recibe las peticiones de montaje de cliente y las otorga o las rechaza.

Si el directorio solicitado está disponible para dicho cliente, el daemon de servidor envía al kernel de cliente un identificador denominado *manejador de archivo*.

7. Entonces el kernel de cliente une el manejador de archivos al punto de montaje (un directorio) registrando determinada información en un *registro de montaje*.

La comunicación de cliente con el daemon **rpc.mountd** no se produce con el proceso de montaje de NFS versión 4. Se utilizan las operaciones del protocolo básico de NFS versión 4 para dar servicio a las operaciones de montaje de la parte del cliente. La implementación de servidor de NFS versión 4 utiliza el soporte del daemon **rpc.mountd** como parte del manejo de acceso de NFS versión 4.

## Archivo /etc(exports

El archivo /etc(exports indica todos los directorios que un servidor exporta a los clientes.

Cada línea del archivo especifica un solo directorio. Un directorio se puede especificar dos veces en el archivo /etc(exports: una vez para NFS versión 2 o NFS versión 3, y una vez para NFS versión 4. El servidor exporta automáticamente los directorios listados cada vez que el servidor de NFS se inicie. Entonces los clientes pueden montar estos directorios exportados. La sintaxis de una línea del archivo /etc(exports es:

```
directorio -opción[,opción]
```

El *directorio* es el nombre de vía de acceso completa del directorio. Las opciones pueden designar un distintivo simple, por ejemplo **ro**, o una lista de nombres de sistema principal. El script /etc/rc.nfs no inicia los daemons **nfsd** o el daemon **rpc.mountd** si no existe el archivo /etc(exports.

El ejemplo siguiente ilustra las entradas de un archivo /etc(exports:

```
/usr/games -ro,access=ballet:jazz:tap
/home -root=ballet,access=ballet
/var/tmp
/usr/lib -access=clients
/accounts/database -vers=4,sec=krb5,access=accmachines,root=accmachine1
/tmp -vers=3,ro
/tmp -vers=4,sec=krb5,access=accmachines,root=accmachine1
```

La primera entrada de este ejemplo especifica que el directorio /usr/games lo pueden montar los sistemas denominados **ballet**, **jazz** y **tap**. Estos sistemas pueden leer datos y ejecutar programas del directorio, pero no pueden grabar en el directorio.

La segunda entrada de este ejemplo especifica que el directorio /home lo puede montar el sistema **ballet** y que se permite el acceso de root para el directorio.

La tercera entrada de este ejemplo especifica que cualquier cliente puede montar el directorio /var/tmp. (Advierta la ausencia de una lista de acceso.)

La cuarta entrada de este ejemplo especifica una lista de acceso designada por el grupo de red **clients**. En otras palabras, estas máquinas designadas como pertenecientes al grupo de red **clients** pueden montar el directorio /usr/lib desde este servidor. (Un *grupo de red* es un grupo de toda la red al que se le permite el acceso a determinados recursos de red por seguridad y organización. Los grupos de red se controlan utilizando NIS.)

La quinta entrada permite el acceso al directorio /accounts/database sólo a los clientes del grupo de red **accmachines** utilizando el protocolo de NFS versión 4 y accediendo al directorio utilizando la autenticación de Kerberos 5. El acceso de root sólo se permite desde **accmachine1**.

La sexta y séptima entradas exportan el directorio /tmp utilizando diferentes versiones y opciones. Si existen dos entradas para el mismo directorio con diferentes versiones de NFS en el archivo /etc(exports, el mandato **exportfs** exportará las dos. Si un directorio tiene las mismas opciones para NFS versión 4 y NFS versión 3, puede tener una entrada en el archivo /etc(exports especificando -vers=3:4.

## Archivo /etc/xtab

El archivo /etc/xtab tiene un formato similar al archivo /etc/exports y lista los directorios exportados actualmente.

Siempre que se ejecuta el mandato **exportfs**, cambia el archivo /etc/xtab. Esto le permite exportar un directorio temporalmente sin tener que cambiar el archivo /etc/exports. Si se anula la exportación del directorio exportado temporalmente, se elimina el directorio del archivo /etc/xtab.

**Nota:** El archivo /etc/xtab se actualiza automáticamente y no se debe editar.

## Archivo /etc/nfs/hostkey

El servidor NFS utiliza este archivo para especificar el principal de sistema principal Kerberos y la ubicación del archivo keytab.

Para obtener instrucciones sobre cómo configurar y administrar este archivo, consulte el mandato [\*\*nfshostkey\*\*](#).

## Archivo /etc/nfs/local\_domain

Este archivo contiene el dominio NFS local del sistema.

Queda implícito que los sistemas que comparten el mismo dominio local NFS también comparten los mismos registros de usuario y grupo. Para obtener instrucciones sobre cómo configurar y administrar este archivo, consulte el mandato [\*\*chnfsdom\*\*](#).

## Archivo /etc/nfs/realm.map

El daemon de registro NFS utiliza este archivo para correlacionar principales de Kerberos de entrada que tienen el formato *nombre@región-kerberos* con el formato *nombre@dominio-nfs*.

Entonces puede resolver el *nombre@dominio-nfs* en una credencial UNIX local. Este archivo proporciona un modo simple para correlacionar principales de Kerberos en el registro de usuarios del servidor. Es apropiado cuando los clientes de diferentes regiones de Kerberos van a acceder al servidor, pero el espacio de nombres de usuario es global. El archivo debe contener líneas con el formato siguiente:

```
región1 dominio-nfs  
región2 dominio-nfs
```

para todas las regiones de Kerberos que soporta el servidor. Si el nombre de región de Kerberos es siempre el mismo que el del dominio NFS del servidor, este archivo no es necesario. Si necesita la posibilidad más general de correlación de *usuarioA@región-kerberos* con *usuarioB@dominio-nfs*, utilice el servicio EIM (Enterprise Identity Mapping). Para obtener información adicional, consulte el apartado “Correlación de identidad” en la página 617.

Para añadir, editar o eliminar entradas de este archivo, utilice el mandato [\*\*chnfsrtd\*\*](#).

## Archivo /etc/nfs/princmap

Este archivo correlaciona nombres de sistema principal con principal de Kerberos cuando el principal no es el nombre de dominio totalmente calificado del servidor.

Consta de cualquier número de líneas del formato siguiente:

```
<parte de  
sistema principal del principal> alias1 alias2 ...
```

Para añadir, editar o eliminar entradas en este archivo, utilice el mandato [\*\*nfshostmap\*\*](#).

## Archivo /etc/nfs/security\_default

El archivo /etc/nfs/security\_default contiene la lista de tipos de seguridad que el cliente NFS puede utilizar, en el orden en que se deben utilizar.

Utilice el mandato [\*\*chnfssec\*\*](#) para gestionar este archivo.

## Protocolo de llamada a procedimiento remoto

NFS se implementa en una gran variedad de tipos de máquina, sistemas operativos y arquitecturas de red. NFS logra esta independencia utilizando el protocolo de **RPC (Remote Procedure Call - Llamada a procedimiento remoto)**.

**RPC** es una biblioteca de procedimientos. Los procedimientos permiten que un proceso (el proceso de cliente) indique a otro proceso (el proceso de servidor) que ejecute llamadas de procedimiento como si el proceso de cliente hubiera ejecutado las llamadas en su propio espacio de direcciones. Dado que el cliente y el servidor son dos procesos independientes, no es necesario que estén en el mismo sistema físico (aunque pueden estar).

NFS se implementa como un conjunto de llamadas **RPC** en las que el servidor atiende determinados tipos de llamadas realizadas por el cliente. El cliente realiza dichas llamadas basándose en las operaciones de sistema de archivos realizadas por el proceso de cliente. En este sentido, NFS es una aplicación RPC.

Dado que los procesos de servidor y de cliente pueden residir en dos sistemas físicos diferentes que pueden tener arquitecturas completamente diferentes, **RPC** debe encargarse de la posibilidad de que los dos sistemas puedan no representar los datos del mismo modo. Por esta razón, **RPC** utiliza tipos de datos definidos por el protocolo **eXternal Data Representation (XDR)**.

## Protocolo eXternal Data Representation

El protocolo **eXternal Data Representation (XDR)** es la especificación para una representación estándar de varios tipos de datos.

Mediante la utilización de una representación de tipo de datos estándar, un programa puede estar seguro de que está interpretando los datos correctamente, incluso si el origen de los datos es una máquina con una arquitectura completamente diferente.

En la práctica, la mayoría de los programas no utilizan **XDR** internamente. En su lugar, utilizan la representación de tipo de datos específica de la arquitectura del sistema en el que se ejecuta el programa. Cuando el programa necesita comunicarse con otro programa, convierte los datos al formato **XDR** antes de enviarlos. Y a la inversa, cuando recibe datos, los convierte del formato **XDR** a su propia representación de tipo de datos específica.

## Daemon portmap

El daemon **portmap** ayuda a los clientes a correlacionar pares de número de programa y número de versión con el número de puerto de un servidor.

Cada aplicación RPC tiene asociado un número de programa y un número de versión. Estos números se utilizan para comunicarse con una aplicación de servidor en un sistema. Al realizar una petición desde un servidor, el cliente necesita conocer en qué número de puerto está aceptando peticiones el servidor. Este número de puerto está asociado con el **UDP (User Datagram Protocol)** o **TCP (Transmission Control Protocol)** que el servicio está utilizando. El cliente conoce el número de programa, el número de versión y el nombre de sistema o nombre de sistema principal donde reside el servicio. El cliente necesita un modo de correlacionar el par de número de programa y número de versión con el número de puerto de la aplicación de servidor. Esto se realiza con la ayuda del daemon **portmap**.

El daemon **portmap** se ejecuta en el mismo sistema que la aplicación NFS. Cuando el servidor empieza a ejecutarse, se registra en el daemon **portmap**. Como función de este registro, el servidor proporciona el número de programa, el número de versión y el número de puerto **UDP** o **TCP**. El daemon **portmap** mantiene una tabla de aplicaciones de servidor. Cuando el cliente intenta realizar una petición del servidor, primero se pone en contacto con el daemon **portmap** para averiguar qué puerto está utilizando el servidor. El daemon **portmap** responde al cliente con el puerto del servidor que el cliente está solicitando. Al recibir el número de puerto, el cliente puede realizar todas las peticiones futuras directamente a la aplicación de servidor.

## Aplicaciones y control de NFS

El SRC (System Resource Controller - Controlador de recursos de sistema) controla los daemons NFS y NIS.

Esto significa que debe utilizar mandatos SRC tales como **startsrc**, **stopsrc** y **lssrc** para iniciar, detener y comprobar el estado de los daemons NFS y NIS.

El SRC no controla algunos daemons NFS; específicamente el SRC no controla **rpc.rexd**, **rpc.rusersd**, **rpc.rwalld** y **rpc.rsprayd**. Estos daemons los inicia y detiene el daemon **inetd**.

La tabla siguiente lista los daemons controlados por SRC y los nombres de subsistema.

Vía de acceso de archivo	Nombre de subsistema	Nombre de grupo
/usr/sbin/nfsd	<b>nfsd</b>	nfs
/usr/sbin/biod	<b>biod</b>	nfs
/usr/sbin/rpc.lockd	<b>rpc.lockd</b>	nfs
/usr/sbin/rpc.statd	<b>rpc.statd</b>	nfs
/usr/sbin/rpc.mountd	<b>rpc.mountd</b>	nfs
/usr/sbin/nfsrgyd	<b>nfsrgyd</b>	nfs
/usr/sbin/gssd	<b>gssd</b>	nfs
/usr/lib/netsvc/yp/ypserv	<b>ypserv</b>	yp
/usr/lib/netsvc/yp/ypbind	<b>ypbind</b>	yp
/usr/lib/netsvc/rpc.yppasswdd	<b>yppasswdd</b>	yp
/usr/lib/netsvc/rpc.ypupdated	<b>ypupdated</b>	yp
/usr/sbin/keyserv	<b>keyserv</b>	keyserv
/usr/sbin/portmap	<b>portmap</b>	portmap

## Información relacionada

[Descripción general del controlador de recursos del sistema](#)

### Modificación del número de hebras biod y daemons nfsd

Se puede utilizar el mandato **chnfs** para cambiar el número máximo de daemons **biod** o **nfsd** que se ejecutarán en un sistema.

Por ejemplo, para establecer el número máximo de daemons **nfsd** en 1000, ejecute el mandato siguiente:

```
chnfs -n 1000
```

**Nota:** Este mandato detendrá los daemons actualmente en ejecución, actualizará la información de configuración de SRC y, a continuación, reiniciará los daemons. Como resultado, el servicio NFS no estará disponible temporalmente.

El número máximo de hebras **biod** se puede especificar por cada montaje mediante la opción de montaje **biods=n**.

**Nota:** Si el número de daemons **nfsd** no es suficiente para atender al cliente, se devuelve al cliente un error de operación nonidempotent. Por ejemplo, si el cliente elimina un directorio, se devuelve un error ENOENT aunque se elimine el directorio en el servidor.

### Cambio de argumentos de línea de mandatos para daemons controlados por SRC

Muchos daemons NFS y NIS tienen argumentos de línea de mandatos que se pueden especificar cuando se inicia el daemon. Dado que estos daemons no se inician directamente desde la línea de mandatos, debe actualizar la base de datos SRC para que los daemons se puedan iniciar correctamente.

Para ello, utilice el mandato **chssys**. El mandato **chssys** tiene el formato:

```
chssys -s Daemon -a 'NuevoParámetro'
```

Por ejemplo:

```
chssys -s nfsd -a '10'
```

cambia el subsistema **nfsd** para que cuando se inicie el daemon, la línea de mandatos tenga el aspecto de nfsd 10. Los cambios realizados por el mandato **chssys** no entran en vigor hasta que se detiene y se reinicia el subsistema.

### Inicio de los daemons NFS

El límite de tamaño de los archivos ubicados en un servidor NFS lo define el entorno de proceso cuando se inicia **nfsd**.

Para utilizar un valor específico, edite el archivo `/etc/rc.nfs`. Utilice el mandato **ulimit** con el límite deseado antes que el mandato **startsrc** para el daemon **nfsd**.

Los daemons NFS se pueden iniciar individualmente o todos a la vez. Para iniciar los daemons NFS individualmente, ejecute:

```
startsrc -s Daemon
```

donde *Daemon* es cualquiera de los daemons controlados por SRC. Por ejemplo, para iniciar el daemon **nfsd**, ejecute:

```
startsrc -s nfsd
```

Para iniciar todos los daemons NFS, ejecute:

```
startsrc -g nfs
```

**Nota:** Si el archivo `/etc/exports` no existe, los daemons **nfsd** y **rpc.mountd** no se iniciará. Puede crear un archivo `/etc/exports` vacío ejecutando el mandato `touch /etc/exports`. Esto permitirá que se inicien los daemons **nfsd** y **rpc.mountd**, aunque no se exportará ningún sistema de archivos.

### Detención de los daemons NFS

Los daemons NFS se pueden detener individualmente o todos a la vez.

Para detener los daemons NFS individualmente, ejecute:

```
stopsrc -s Daemon
```

donde *Daemon* es cualquiera de los daemons controlados por SRC. Por ejemplo, para detener el daemon **rpc.lockd**, ejecute:

```
stopsrc -s rpc.lockd
```

Para detener todos los daemons NFS a la vez, ejecute:

```
stopsrc -g nfs
```

### Obtención del estado actual de los daemons NFS

Puede obtener el estado actual de los daemons NFS de forma individual o de todos ellos a la vez.

Para obtener el estado actual de los daemons NFS de forma individual, ejecute:

```
lssrc -s Daemon
```

donde *Daemon* es cualquiera de los daemons controlados por SRC. Por ejemplo, para obtener el estado actual del daemon **rpc.lockd**, ejecute:

```
lssrc -s rpc.lockd
```

Para obtener el estado actual de todos los daemons NFS a la vez, ejecute:

```
lssrc -a
```

## Soporte de NFS versión 4

A partir de AIX 5.3, se incluye soporte para las características de protocolo NFS versión 4.

Las características obligatorias del protocolo se soportan tal como se describen en RFC 3530 con las siguientes excepciones:

- Los mecanismos de seguridad LIPKEY y SPKM-3 no se soportan con la autentificación RPCSEC-GSS RPC. Sólo se soporta el mecanismo de Kerberos V5.
- Los requisitos de UTF-8 no se soportan totalmente. Específicamente, no se garantiza que la transmisión de nombres de archivo y de series de sistemas de archivos, por ejemplo el contenido de enlace simbólico y los nombres de entrada de directorio, estén en formato UTF-8. La transmisión de series de atributos NFS, por ejemplo propietario y grupo de propietarios, está siempre en formato UTF-8. El servidor y cliente NFS realizan la validación de UTF-8 en los datos de series de entrada como se define en RFC 3530. Esta comprobación se puede inhabilitar administrativamente utilizando el mandato **nfs0**. Es posible que sea necesario inhabilitar la comprobación de UTF-8 para utilizar NFS versión 4 en entornos con configuraciones y datos no UTF-8.
- No se soportan UDP, NIM y el cliente sin disco sobre NFS versión 4.

Se soportan las siguientes características opcionales de NFS versión 4:

- El cliente y el servidor NFS soportan las ACL de NFS versión 4. El cliente NFS soporta la gestión de las ACL de NFS versión 4 utilizando los programas de utilidad **acredit**, **aclget** y **aclput**. El servidor NFS es capaz de almacenar y recuperar las ACL de NFS versión 4 de los sistemas de archivos subyacentes que soportan el modelo de ACL de NFS versión 4. Para obtener más información, consulte el apartado ["Soporte de Listas de control de acceso de NFS"](#) en la página 593.
- Se proporciona soporte para correlacionar principales y atributos de propiedad de archivo de un dominio NFS versión 4 con otro. Este soporte está principalmente destinado a utilizar en servidores NFS de AIX. Necesita el despliegue de LDAP. Las correlaciones de NFS se gestionan utilizando el programa de utilidad **chnfsim**.

Hay varias consideraciones al utilizar el acceso simultáneo con NFS versiones 2 y 3 y NFS versión 4. Es posible que el acceso de NFS versión 3 reciba errores debido al estado otorgado de NFS versión 4. Asimismo, es posible que el rendimiento de NFS versión 3 quede afectado cuando se exportan datos para el acceso de NFS versión 4.

## Periodo de gracia del servidor NFS

El protocolo de NFS versión 4 (NFSv4) proporciona funcionalidad que permite a los administradores del sistema habilitar un periodo de gracia en el servidor NFSv4 para el manejo especial de operaciones específicas.

Dentro de este periodo de gracia, los administradores pueden gestionar bloqueos, operaciones de lectura y operaciones de grabación durante todo el periodo de alquiler de servidor. Los clientes pueden recuperar los bloqueos y los estados asociados mediante peticiones de bloqueo de tipo reclamación.

**Nota:** No a todos los estados reclamados por los clientes en el periodo de gracia se les puede garantizar que estén en el estado mantenido por el servidor en la instancia anterior. Se garantiza que el estado que se reclama durante el periodo de gracia sea el correcto que ha definido la RFC NFSv4.

A partir de AIX 5L Versión 5.3 con el nivel de tecnología 5300-05, los administradores pueden utilizar el periodo de gracia en los servidores NFSv4. De forma predeterminada, el periodo de gracia está inhabilitado. Para habilitar el periodo de gracia en el servidor, utilice el menú de SMIT o la interfaz de línea de mandatos **chnfs**.

Cuando el periodo de gracia está habilitado, el servidor NFSv4 registra la información de estado en disco en el archivo /var. El estado registrado se reclama automáticamente cuando se reinicia el servidor.

## Soporte DIO y CIO de NFS

AIX 5L Versión 5.3 con el paquete de mantenimiento recomendado 5300-03 soporta E/S directa y E/S simultánea en el cliente NFS para los protocolos de la versión 3 y 4. DIO y CIO sólo implican al cliente.

Mediante la utilización de DIO y CIO, las cargas de trabajo de centro de datos, por ejemplo bases de datos y aplicaciones de cálculo de alto rendimiento, pueden experimentar un aumento en los niveles de rendimiento, junto con una reducción de recursos de memoria y CPU de sistema, al mismo tiempo que mantienen las ventajas de la centralización del almacenamiento basado en archivo y de la gestión asociada de sistemas de componente de fondo.

Normalmente la E/S no es secuencial y las aplicaciones no se benefician del almacenamiento en antememoria de los datos en el cliente NFS o las aplicaciones realizan todo el almacenamiento en antememoria avanzado. Estas aplicaciones se benefician cuando NFS no se almacena en antememoria, realiza una predicción de lectura o utiliza mecanismos de grabación posterior. Además, algunas aplicaciones, por ejemplo bases de datos, no dependen de la semántica de un solo sitio de POSIX, lo que serializa las lecturas con las grabaciones. Estas aplicaciones emiten lecturas y grabaciones simultáneas, pero son responsables de la coherencia y coordinación de dichas operaciones.

### E/S directa para NFS

DIO permite a las aplicaciones realizar lecturas y grabaciones directamente en el servidor NFS sin pasar a través de la capa de antememoria de cliente NFS (Gestor de memoria virtual) o incurrir en la sobrecarga asociada del almacenamiento en antememoria de datos.

Bajo DIO, las peticiones de E/S de aplicación se atienden utilizando Llamadas a procedimiento remoto (RPC) directas al servidor NFS. Puede establecer DIO utilizando la opción de montaje de AIX `dio`. Sin la opción de montaje, también puede habilitar DIO por archivo utilizando el distintivo AIX `O_DIRECT open()`.

Es posible que el servicio a las E/S directas NFS necesite varias RPC al servidor, en función del tamaño de petición de E/S y del tamaño máximo de transferencia por cable permitidos por el servidor y el cliente. Para obtener más información sobre DIO, consulte la opción -o del mandato `mount`.

### Entrada/Salida simultánea para NFS

Con CIO, las lecturas y grabaciones de aplicación que se emiten simultáneamente se ejecutan simultáneamente sin bloqueo de lecturas durante las grabaciones o a la inversa.

Varias grabaciones también se ejecutan simultáneamente. No se proporcionan las garantías de atomicidad de POSIX. Cuando CIO está en vigor, está implícita la E/S directa. Utilice la opción de montaje AIX `cio` o el distintivo `O_CIO open()` para establecer CIO. Para obtener más información sobre CIO, consulte la opción -o para el mandato `mount`.

En AIX Versión 6.1 con el nivel de tecnología 6100-04 y versiones posteriores, puede ejecutar el mandato `mount`, el mandato `nfs4cl` o la subrutina `open()` para poder abrir archivos de sólo lectura cuando esos archivos ya estén abiertos en CIOR. La opción `cior` y el distintivo `O_CIOR open()` sólo se pueden utilizar junto con CIO.

### Información relacionada

[mount, mandato](#)

### Interacción de aperturas DIO, CIO, regulares y archivos correlacionados para NFS

Existen los siguientes comportamientos entre las diferentes modalidades de acceso que se pueden producir con DIO y CIO.

Cuando las aperturas DIO existentes están en vigor:

- Una apertura normal hace que DIO se desactive hasta que no haya más aperturas normales. Cuando un cierre reduce las aperturas normales a 0, DIO se vuelve a habilitar si todavía hay aperturas DIO pendientes.

- La correlación de un archivo con shmat() o mmap() desactivará DIO en el archivo hasta que el número de correlaciones se reduzca a 0. Entonces, si todavía hay aperturas DIO, se volverá a habilitar DIO.
- Los intentos de apertura del archivo para CIO no se ejecutarán correctamente y devolverán el error EINVAL.

Cuando hay aperturas normales (no CIO o DIO) en vigor:

- La apertura DIO intenta realizarse satisfactoriamente, pero DIO no se activa hasta que la cuenta de aperturas normales se reduce a 0.
- Las aperturas para CIO no se ejecutarán correctamente y devolverán el error EINVAL.

Cuando las aperturas CIO están en vigor:

- Las aperturas normales y DIO así como los intentos de correlacionar el archivo fallarán todos ellos devolviendo el error EINVAL.

Cuando las aperturas CIO|CIOR entran en vigor:

- Las aperturas normales, DIO y los intentos de correlacionar el archivo no realizarán correctamente y devolverán el error EINVAL, excepto, para las aperturas de sólo lectura y CIO|CIOR.

**Nota:** Cuando hay una transición a DIO o CIO, las modificaciones almacenadas en antememoria del cliente se grabarán de nuevo en el servidor NFS antes de suprimir toda la información almacenada en antememoria.

## Duplicación NFS y espacio de nombres global

El protocolo NFS versión 4 (NFSv4) proporciona funciones que le permiten, como administrador del sistema, distribuir datos en varios servidores de un modo que es transparente para los usuarios de dichos datos.

Puede utilizar dos características proporcionadas a partir de AIX 5L Versión 5.3 con el paquete de mantenimiento recomendado 5300-03. La primera es una característica de espacio de nombres global denominada *referencia*. La segunda característica es un medio para especificar ubicaciones donde se pueden encontrar copias de datos, que se denomina *réplica*.

Una *referencia* es un objeto especial que puede crear en el espacio de nombres de un servidor al que se adjunta información de ubicación. El servidor utiliza las características de protocolo de NFSv4 para redirigir a los clientes al servidor especificado en la información de ubicación. La referencia forma un bloque de creación para integrar datos de varios servidores NFS en un solo árbol de espacio de nombres de archivo en el que pueden navegar los clientes NFSv4 que están al corriente de la referencia.

Una *réplica* es una copia de un sistema de archivos de un servidor NFS que se ha puesto en otros servidores NFS diversos (o en una ubicación alternativa, por ejemplo un disco diferente del mismo servidor). Si una ubicación de réplica utilizada por un cliente NFSv4 que está al corriente de la réplica queda no disponible, el cliente comutará a otra réplica disponible. Para obtener más información sobre las réplicas, consulte el apartado “[Réplicas de NFS](#)” en la página 608.

## Referencias de NFS

Los ejemplos siguientes proporcionan casos para ayudarle a comprender las referencias.

En los ejemplos siguientes, hay cuatro servidores:

- El servidor denominado publications contiene archivos de documentación.
- El servidor denominado projects contiene directorios de trabajo de usuario.
- El servidor denominado data contiene bases de datos de información.
- El servidor denominado account1 es el servidor NFS principal que exporta todos los demás archivos y es el servidor que todos los clientes conocen.

## Permitir a todos los clientes acceder a los archivos del servidor NFS principal

El servidor account1 exporta el directorio /work a todos los clientes utilizando la siguiente sentencia en el archivo /etc(exports:

```
/work -vers=4
```

Todos los clientes pueden acceder a los archivos del directorio remoto /work montando / desde el servidor account1 en el directorio /mnt utilizando el mandato siguiente:

```
mount -o vers=4 account1:/ /mnt
```

Cuando el usuario del cliente lista el contenido del directorio /mnt, ve el directorio remoto work en la vía de acceso /mnt/work. El contenido del directorio /mnt/work del cliente es el mismo que el contenido del directorio /work del servidor account1.

### **Permitir a un cliente acceder a los archivos de un servidor específico**

El usuario de cliente también desea acceder al directorio /usr/doc del servidor publications.

En releases anteriores, debe exportar el directorio del servidor y montar el directorio en el cliente.

### **Utilizar referencias para crear un espacio de nombres distribuido**

Puede configurar un servidor de forma que los clientes puedan acceder a los datos de otros servidores sin que el cliente sepa dónde están los datos. Sólo el administrador del servidor de referencia necesita saber dónde están los datos. El servidor de referencia puede redirigir a los clientes a la ubicación del directorio /usr/doc utilizando una referencia. En el servidor publications, se puede exportar el directorio /usr/doc añadiendo la sentencia siguiente al archivo de exportación:

```
/usr/doc -vers=4
```

Esto deja los directorios disponibles para los clientes de NFSv4.

Ahora el servidor account1 puede utilizar referencias para dejar disponibles esos directorios a los clientes añadiendo la siguiente sentencia al archivo de exportación:

```
/usr/doc -vers=4,refer=/usr/doc@publications
```

A continuación, exporte el directorio. En este punto, el cliente que ha montado el directorio /mnt desde el directorio / del servidor account1 tiene acceso al directorio usr cuando el cliente lista el directorio /mnt. El cliente no tiene que realizar ningún montaje en otros servidores. El usuario de cliente no necesita ni siquiera estar al corriente de que los archivos que se encuentran allí no los está proporcionando el servidor account1. Por ejemplo, puede dejar disponibles los directorios de /databases/db del servidor data y /home/accts del servidor projects mediante account1 exportando los directorios de los servidores data y projects y creando en account1 referencias a dichos directorios.

Puesto que un usuario de cliente no está al corriente de la ubicación real de los datos, el administrador puede redirigir los clientes de un servidor a otro simplemente cambiando la sentencia de referencia en el archivo de exportaciones del servidor. El administrador es responsable de la colocación y la correlación de los datos a los que se refieren las referencias con las especificaciones de ubicación.

Los administradores deben estar seguros de que el segundo servidor no remitirá de nuevo la petición al primer servidor, creando una referencia circular. En el ejemplo anterior, si el administrador hubiera creado una referencia en el servidor publications en /usr/doc que hiciera referencia a /usr/doc en el servidor account1, la referencia circular resultante no sería deseable.

Aunque las referencias se crean utilizando exportfs, son diferentes de las exportaciones de datos. Las ubicaciones especificadas para las referencias deben corresponder a los directorios raíz de los sistemas de archivos exportados por NFSv4. Puede crear una referencia en espacios de nombres exportados o en espacios de nombres no exportados. En el ejemplo anterior, la referencia /usr/doc se puede crear en el servidor account1 aunque /usr no se exporte. Esto deja la referencia en el pseudoespacio de NFSv4. Si account1 hubiese exportado /usr, aún se habría permitido la exportación de referencia, en lugar de exportar un directorio denominado doc, lo cual hubiera fallado si hubiera estado en el mismo sistema de archivos. En cualquiera de los casos, la exportación de referencia habría fallado si hubiera existido un

archivo o directorio en `/usr/doc`. No hay ninguna restricción en el número de referencias que se pueden crear en el pseudoespacio de NFSv4 del servidor o en un sistema de archivos exportado.

Dado que una referencia no exporta datos y sólo tiene significado para el protocolo NFSv4, las referencias sólo están disponibles en NFSv4. La exportación de una referencia sin la opción `vers=4` fallará. Aunque este ejemplo sólo especifique una ubicación, se pueden especificar hasta 8 ubicaciones.

La creación de una referencia crea un objeto de referencia especial en la ubicación especificada por el parámetro de directorio. Puesto que el acceso de cliente al objeto lo determina el acceso del cliente al directorio padre del objeto, la mayoría de las opciones de exportación no tienen significado, se permiten y se ignoran. La única excepción es la opción `exname`, que tendrá el comportamiento esperado. Por ejemplo, si el servidor crea la referencia `/n4root/special/users -vers=4,exname=/exported/users,refer=/restricted/users@secrethost`, los clientes que montan / desde el servidor verán la vía de acceso `/mnt/exported/users`, que redirigirá los clientes al directorio `/restricted/users` de `secrethost`. En el servidor de exportación, puesto que el objeto de referencia se creará en realidad en el espacio de nombres local en `/n4root/special/users`, allí no debe existir ningún archivo o directorio cuando se realice la exportación. Se crea un objeto especial en el servidor para que contenga la información de ubicación de referencia. Si no existen, también se crearán los directorios que estén en la vía de acceso de la referencia. Si se elimina la exportación de la referencia, la información de referencia se eliminará del objeto, pero el objeto propiamente dicho no se eliminará. El servidor NFSv4 no permitirá a los clientes acceder al objeto de referencia *obsoleto* o *huérfano* resultante. Devolverá un error de acceso a los clientes que intenten acceder al objeto. Si se desea, el objeto se puede eliminar utilizando `rm`. Una referencia se puede volver a exportar con nueva información de referencia. Esta acción no se recomienda como práctica frecuente porque los clientes que tienen acceso a la referencia pueden tardar cierto tiempo en darse cuenta de que ha cambiado la información de ubicación. El servidor alcanza el directorio padre de la referencia para indicar que la información del directorio ha cambiado. Esto ayuda a los clientes a darse cuenta de que la información que el cliente ha almacenado en antememoria acerca del directorio (y la referencia en el directorio) ha cambiado y que se tiene que volver a captar, pero no hay ninguna garantía del tiempo que tardarán los clientes en advertir dicha situación.

Para obtener información sobre cómo utilizar la opción `refer` para cambiar el orden de ubicaciones especificadas en la lista de ubicaciones del sistema de archivos, consulte el apartado [Reordenación de la lista de ubicaciones del sistema de archivos utilizando la opción scatter](#).

### Réplicas de NFS

La duplicación le permite, como administrador de NFSv4, poner copias de los datos en varios servidores NFSv4 e informar a los clientes de NFSv4 sobre el lugar donde residen las réplicas.

En el caso de que el servidor de datos primario quede inaccesible para los clientes, los clientes pueden utilizar uno de los servidores de réplica para continuar las operaciones en el sistema de archivos replicado. Se supone que los sistemas de archivos de réplica son copias exactas de los datos del servidor primario. Puede configurar un máximo de 8 ubicaciones de réplica. El servidor AIX no especifica cómo se crean los sistemas de archivos de réplica a partir del sistema de archivos primario o cómo se mantienen coherentes los datos. Si va a especificar réplicas como lectura y grabación, debe mantener los datos de las réplicas coherentes con los del sistema de archivos primario.

Una réplica es un servidor que contiene una copia del directorio o de los directorios de otro servidor. Si el servidor primario deja de estar disponible para el cliente, el cliente puede acceder a los mismos archivos de una ubicación de réplica. A continuación se muestra:

Si los archivos del directorio `/data` del servidor `account1` también están disponibles en el directorio `/backup/data` del servidor `inreserve`, los clientes NFSv4 pueden estar al corriente de esto especificando ubicaciones de réplica en la exportación. Añadiendo una sentencia similar a la siguiente en el archivo de exportación, puede exportar el directorio `/data` y especificar la ubicación de la copia de réplica:

```
/data -vers=4,replicas=/data@account1:/backup/data@inreserve
```

Si el servidor `account1` deja de estar disponible, los usuarios de cliente que utilizan archivos del directorio `/data` del servidor `account1` pueden empezar a utilizar archivos del directorio `/backup/data` del servidor `inreserve`, sin darse cuenta de que el cliente ha comutado a un servidor diferente.

Para obtener información sobre cómo utilizar la opción `replicas` para cambiar el orden de las ubicaciones especificadas en la lista de ubicaciones del sistema de archivos, consulte el apartado [Reordenación de la lista de ubicaciones del sistema de archivos utilizando la opción `scatter`](#).

### ***Requisitos de configuración de NFS para permitir la especificación de réplicas***

Debe ser administrador para habilitar, inhabilitar o especificar réplicas de root.

Para habilitar, inhabilitar y especificar réplicas de root, utilice el mandato siguiente:

```
chnfs -R {on|off|host[+host]}
```

Para especificar réplicas, el servidor se debe configurar con **chnfs -R** (**chnfs -R on**) para emitir manejadores de archivos NFSv4 volátiles. Un manejador de archivos es un identificador que los servidores NFS emiten a los clientes para identificar un archivo o directorio en el servidor. De forma predeterminada, el servidor emite manejadores de archivo permanentes. La conmutación entre tipos de manejadores de archivo puede producir errores en aplicaciones en los clientes NFSv4 que utilizan activamente el servidor cuando se realiza la conmutación. Para cambiar la modalidad de manejador de archivos con **chnfs -R**, no se puede exportar ningún sistema de archivos para el acceso NFSv4. El establecimiento de la disposición de manejador de archivos se deberá realizar con un servidor NFS recién suministrado o cuando se pueda minimizar o detener la actividad de NFS. Para clientes conectados activamente a servidores cuando cambia la modalidad, es posible que sea necesario desmontar o volver a montar montajes de NFSv4 en dichos clientes. Para minimizar esta acción, el número de montajes de cliente se puede reducir a un pequeño número de montajes que montan los directorios de nivel superior del espacio de archivo exportado de un servidor NFSv4.

El cliente NFSv4 no puede recuperar tras error en réplicas con propiedades de acceso de exportación diferentes. Los administradores deben asegurarse de que todas las réplicas se especifican con los mismos controles de acceso de exportación y modalidad de acceso (sólo lectura o sólo grabación). Con la posible excepción de GPFS exportados, se espera que los datos replicados se exporten como de sólo lectura. También es responsabilidad del administrador mantener el contenido de datos en todas las ubicaciones de réplica. Los árboles de directorios y todo el contenido de datos se deben mantener idénticos. Será necesario realizar actualizaciones en el contenido de datos del modo que sea más compatible con las aplicaciones que van a utilizar los datos.

Con las réplicas, puede utilizar la opción de exportación `exname` para ocultar detalles del espacio de nombres del sistema de archivos local del servidor a los clientes de NFSv4. Para obtener más detalles, consulte el mandato `exportfs` y el archivo `/etc(exports`.

Puede utilizar la opción `replicas` con los sistemas de archivos de clúster de exportación, por ejemplo GPFS (General Parallel File System - Sistema de archivos de paralelo general) para especificar varios nodos de servidor NFS que ven la misma vista GPFS. En esta configuración la exportación de los datos para el acceso de lectura y grabación puede ser válida. Sin embargo, con las réplicas de lectura y grabación, si se produce una recuperación tras error de réplica mientras están en proceso operaciones de grabación, las aplicaciones que realizan la grabación pueden encontrar errores irrecuperables. De forma similar, una operación `mkdir` o de creación de archivo exclusivo que se ejecute durante una recuperación tras error puede encontrar un error EXISTS.

Una exploración replicada debe exportar un sistema de archivos entero. Esto significa que el directorio que se está exportando debe ser la raíz del sistema de archivos local. El servidor que exporta un sistema de archivos replicado se debe especificar a sí mismo como una de las ubicaciones de la exportación. Para servidores con varias interfaces, esto debe incluir el nombre de sistema principal primario del servidor. Si el servidor que exporta un sistema de archivos replicado no se especifica a sí mismo como una de las ubicaciones para la exportación, el servidor de exportación se añadirá silenciosamente a la lista de ubicaciones de réplica como la primera ubicación de réplica. El orden de las ubicaciones de réplica en la lista de réplicas especifica el orden de preferencia que los clientes deben utilizar al recuperarse tras un error. Por ejemplo, si el usuario en `serverA` desea exportar `/webpages` y hay una réplica de `/webpages` en `serverB` en el directorio `/backup/webpages`, la entrada siguiente del archivo `/etc(exports`

exportará /webpages de serverA e informará a los clientes que hay una copia del sistema de archivos de serverB en /backup/webpages:

```
/webpages -vers=4,ro,replicas=/webpages@serverA:  
/backup/webpages@serverB
```

Se supone que /webpages de serverA y /backup/webpages de serverB son los directorios raíz de los sistemas de archivos. Si serverA no se hubiese listado en la exportación, se hubiera añadido silenciosamente como la primera ubicación de réplica. Esto es porque se supone que el servidor que exporta los datos es el servidor preferido para los datos que está exportando.

Las réplicas sólo las utiliza el protocolo NFSv4. La exportación anterior podía haber especificado NFSv3 (`vers=3:4`), pero la información de réplica no estaría disponible para los clientes de NFSv3. Sin embargo, los clientes que utilizan NFSv3 pueden acceder a la información de /webpages en serverA, pero no se recuperarán tras error en la réplica si serverA queda no disponible.

#### **Sopor te de la parte de cliente NFS para varias ubicaciones**

Cuando el cliente ya no puede acceder a datos replicados del servidor actual, el cliente intenta acceder a los datos del siguiente servidor más favorecido.

El orden en el que se especifican las réplicas en la lista de réplicas lo toma el cliente para que sea el orden de preferencia.

El administrador de cliente puede alterar temporalmente la preferencia de réplica utilizando el submandato **prefer** del mandato **nfs4cl**. El mandato **nfs4cl** visualiza toda la información del sistema de archivos sobre el cliente o modifica las opciones de un sistema de archivos y visualiza o modifica estadísticas y propiedades de NFSv4 actuales.

#### **Consideraciones comunes acerca de NFS para réplicas y referencias**

Si el cliente encuentra dos vías de acceso diferentes que conducen a los mismos datos (sistema de archivos), el cliente trata la segunda vía de acceso como un enlace simbólico al archivo.

Por ejemplo, server A exporta:

```
/tmp/a -vers=4,replicas=/tmp/a@B:/tmp/a@A  
/tmp/b -vers=4,refer=/tmp/a/b@B
```

Y server B exporta:

```
/tmp/a -vers=4  
/tmp/a/b -vers=4
```

En este ejemplo, el cliente monta / del servidor server A en /mnt utilizando el mandato `mount -o vers=4 A:/ /mnt`. El usuario cliente accede a /tmp/a/b en server B mediante `cd /mnt/tmp/a/b` o `cd /mnt/tmp/b`. Si antes el usuario cambia el directorio a `cd /mnt/tmp/a/b`, la vía de acceso /mnt/tmp/b actúa como enlace simbólico a /mnt/tmp/a/b. En este escenario, si el usuario se encuentra en /mnt/tmp/b y utiliza el mandato `/bin/pwd`, `/bin/pwd` devolverá /mnt/tmp/a/b.

**Nota:** La práctica anterior no se recomienda. El administrador debe configurar especificaciones de exportación que producen una sola vía de acceso de espacio de nombres posible a los datos exportados.

Puede listar varias ubicaciones en las referencias si los datos de destino de la referencia están realmente replicados. Los clientes sólo utilizarán las ubicaciones de referencia para buscar el destino de referencia en un servidor disponible. Una vez que el cliente establece el acceso al destino de referencia, obtendrá nueva información de ubicación para los datos encontrados.

Dado que los clientes pueden no detectar inmediatamente los cambios en la información de ubicación de referencias, no se recomienda eliminar o cambiar la ubicación de referencia de manera frecuente. Cuando se reubica el destino de una ubicación de referencia, se sugiere que la nueva ubicación se llene al mismo tiempo que se cambia la información de ubicación en la especificación de referencia de la exportación. Los datos de la ubicación anterior se deberán conservar durante varias horas o incluso días para dar tiempo a los clientes de ver y utilizar la nueva ubicación.

Las réplicas y las referencias sólo se pueden ejecutar en servidores que ejecutan el kernel de 64 bits. Los clientes pueden ejecutarse en los kernels de 32 y de 64 bits.

Si va a especificar réplicas como lectura y grabación, debe mantener los datos de las réplicas coherentes con los del catálogo de archivos primario.

#### **Cómo se recuperan los clientes NFS tras los errores**

Una *recuperación tras error* se produce cuando el cliente comuta de una ubicación de réplica a otra después de determinar que el servidor actual con el que se está comunicando ya no es accesible.

En el comportamiento de la recuperación tras error del cliente NFS influyen los siguientes valores ajustables:

#### **Opción de montaje de NFS `timeo`**

Esta opción de montaje especifica el tiempo que la capa TCP/IP debe esperar antes de volver con una respuesta de tiempo de espera excedido.

#### **Opción de montaje de NFS `retrans`**

Esta opción de montaje especifica el número de veces que la capa RPC de NFS debe reintentar la petición del cliente antes de devolver un error de tiempo de espera de RPC (ETIMEDOUT).

#### **Opción de nfso `nfs_v4_fail_over_timeout`**

Puede utilizar esta opción nfso para especificar la cantidad mínima de tiempo que el cliente debe esperar antes de recuperarse tras error en una réplica. Esta opción es global en el cliente NFS y altera temporalmente el comportamiento predeterminado por montaje. De forma predeterminada, `nfs_v4_fail_over_timeout` no está activo. El valor es 0.

Cuando `nfs_v4_fail_over_timeout` no está activo, el umbral de recuperación tras error se establece en el doble del valor de la opción `timeo` de montaje. Cuando no se han producido llamadas RPC satisfactorias durante este tiempo, el cliente empieza el proceso de recuperación tras error para buscar otra réplica disponible. Sin embargo, el tiempo real que el cliente esperará está influído por la opción `retrans`. Si `retrans` es mayor que 2, probablemente el cliente esperará a recibir un tiempo de espera de RPC basado en el valor de `retrans` multiplicado por el valor de `timeo` (`retrans × timeo`). Por consiguiente, se puede ajustar la combinación de las opciones `timeo` y `retrans` para controlar el comportamiento de recuperación tras error para cada montaje NFS. También puede establecer estas opciones a un nivel más granular utilizando el mandato **`nfs4cl`**.

Cuando `nfso nfs_v4_fail_over_timeout` se establece en un valor distinto de cero, representa el número de segundos que el cliente espera en un servidor no disponible antes de considerar la recuperación tras error de réplica. Si las opciones `timeo` y `retrans` producen un comportamiento de tiempo de espera de RPC más allá del valor de `nfso`, es posible que el proceso de recuperación tras error no se inicie hasta que se haya generado el tiempo de espera de RPC.

Para obtener más información sobre las opciones `retrans`, `timeo` y `nfs_v4_fail_over_timeout`, consulte las opciones específicas de NFS de los mandatos **`mount`**, **`nfs4cl`** y **`nfso`**.

Además de la recuperación tras error de réplica en el caso de un servidor no disponible, hay casos en los que el cliente comutará voluntariamente de una ubicación de réplica a otra. Se da uno de estos casos cuando se utiliza el mandato **`nfs4cl`** para establecer una réplica preferida. En este caso, el cliente inicia una comutación al servidor preferido, si no es el servidor actual que el cliente está utilizando. El cliente también volverá a captar la información de ubicación de réplica del servidor NFS a intervalos de 30 minutos aproximadamente cuando haya habido actividad reciente en los datos asociados. Si el orden de las ubicaciones ha cambiado, el cliente intenta comutar a la primera ubicación, si ésta es diferente del servidor actual que el cliente está utilizando y no se ha establecido una preferencia de réplica con el mandato **`nfs4cl`**.

#### **Montajes NFS flexibles frente al comportamiento de recuperación tras error**

El modelo de montaje predeterminado para NFS es el montaje fijo y en los montajes fijos se aplica el comportamiento de recuperación tras error de réplica. El comportamiento de recuperación tras error es diferente si se utilizan montajes flexibles NFS.

Si los valores de montaje flexible producen un tiempo de espera excedido RPC anterior al periodo de espera establecido para la recuperación tras error de réplica, el tiempo de espera producirá un error

ETIMEDOUT en la aplicación que efectúa la llamada. No se recomienda utilizar montajes flexibles con datos replicados. Si se utilizan montajes flexibles y se ha establecido el valor nfso nfs\_v4\_fail\_over\_timeout, se sugiere que las opciones de montaje retrans y timeo se establezcan para que excedan el valor de nfso. Esto evitará que se devuelva ETIMEDOUT a las aplicaciones para datos replicados.

#### **Reordenación de la lista de ubicaciones del sistema de archivos utilizando la opción scatter**

La opción scatter del mandato **exportfs** permite cambiar el orden de las ubicaciones especificadas en la lista de ubicaciones del sistema de archivos que se establece con la opción refer o replicas del mandato **exportfs**.

La utilización de esta opción genera diferentes combinaciones de ubicaciones de servidor de manera que distintas listas tengan distintos servidores en el orden de preferencia. En consecuencia, distintos clientes tienen listas de ubicaciones de servidor que son diferentes. Esta reordenación ayuda al equilibrio de la carga ya que el primer servidor de la lista de ubicaciones de distintos clientes es un servidor diferente. De la misma manera, si un servidor pasa a estar inactivo, la carga de recuperación tras error se distribuye entre diversos servidores puesto que el servidor en la siguiente ubicación de la lista de ubicaciones de servidor es diferente. La opción scatter sólo se aplica a directorios exportados para el acceso por parte del protocolo de NFS versión 4.

La opción scatter puede tener los siguientes valores:

- **full** - Todos los servidores se reordenan para formar combinaciones de ubicaciones alternativas. El número total de combinaciones está limitado a 12 o al número de servidores, cualquiera que sea el número más alto.
- **partial** - La primera ubicación para todas las combinaciones de servidor generadas es fija para el primer servidor de la lista de servidores. El resto de las ubicaciones se listan como si se utilizase una reordenación completa.
- **none** - No se realiza ninguna reordenación de la lista de ubicaciones del sistema de archivos. Este es el valor predeterminado para la opción scatter. Utilice este valor para inhabilitar cualquier reordenación previa de la lista de ubicaciones.

**Nota:** Si no se especifica el distintivo noauto cuando se está utilizando el mandato **exportfs**, la lista de ubicaciones incluye el nombre de sistema principal primario como una de las ubicaciones de réplica.

Para especificar referencias para el directorio /common/documents en los sistemas principales s1, s2 y s3 y, a continuación, reordenarlas utilizando la opción full, añada la línea siguiente al archivo /etc/exports y, después, exporte el directorio /common/documents:

```
/common/documents -ver=4, refer=/common/documents@s1:/common/document@s2a:/common/documents@s3,scatter=full
```

Para especificar réplicas para el directorio /common/documents en los sistemas principales s1, s2, s3 y s4, y reordenarlas parcialmente (el primer servidor de recuperación tras error es s1 para todas las combinaciones), añada la línea siguiente al archivo /etc/exports y, a continuación, exporte el directorio /common/documents:

```
/common/documents -vers=4, replicas=/common/documents@s1:/common/documents@s2:/common/documents@s3:/common/documents@s4,scatter=partial
```

## **Delegación de servidor-cliente NFS**

La *delegación* es la posibilidad del servidor de delegar determinadas responsabilidades al cliente.

A partir de AIX 5L Versión 5.3 con el paquete de mantenimiento recomendado 5300-03, puede utilizar la delegación. Cuando el servidor otorga una delegación para un archivo a un cliente, se garantiza al cliente determinada semántica respecto al compartimiento de dicho archivo con otros clientes. Cuando se abre un archivo, el servidor puede proporcionar al cliente una delegación de lectura para el archivo. Si se otorga al cliente una delegación de lectura, se asegura que ningún otro cliente tenga la posibilidad de grabar en el archivo durante el tiempo que dura la delegación. Si se otorga al cliente una delegación de grabación, se asegura al cliente que ningún otro cliente tenga acceso de lectura o grabación al archivo. El

servidor AIX sólo otorga delegaciones de lectura. El servidor AIX sólo soporta la delegación con el kernel de AIX de 64 bits. El cliente de AIX soporta delegaciones de lectura y grabación.

Para que el servidor otorgue una delegación al cliente, primero el cliente debe proporcionar una dirección de devolución de llamada al servidor. Cuando se vuelve a llamar una delegación, el servidor enviará una petición de rellamada a esta dirección. De forma predeterminada, el cliente indicará la dirección IP que se está utilizando para las comunicaciones normales con el servidor. Para clientes con varias interfaces de red, se puede especificar una dirección específica en el archivo `/etc/nfs/nfs4_callback.conf`. El formato de las entradas de este archivo es:

*sistral-servidor dirección-ip-cliente*

Donde *sistral-servidor* es el nombre o la dirección de un servidor NFSv4 y *dirección-ip-cliente* es la dirección de cliente que se debe utilizar al proporcionar la información de devolución de llamada de servidor. Si el nombre *sistral-servidor* es la dirección de IPv4 0.0.0.0 o la dirección de IPv6 0::0, se utilizará la *dirección-ip-cliente* especificada para todos los servidores que no se listan en el archivo. Si este archivo no existe o si no se encuentra una entrada para el servidor (o una entrada predeterminada), el cliente selecciona una dirección basándose en la conexión existente con el servidor.

El servidor puede volver a llamar las delegaciones. Si otro cliente solicita acceso al archivo de tal forma que el acceso está en conflicto con la delegación otorgada, el servidor puede informar al cliente inicial y volver a llamar a la delegación. Para ello es necesario que exista una vía de acceso de devolución de llamada entre el servidor y el cliente. Si no existe esta vía de acceso de devolución de llamada, no se pueden otorgar delegaciones. Si se ha otorgado una delegación de archivos, el acceso desde otros clientes NFSv4, clientes NFS versiones 2 y 3, y los accesos locales al archivo en el servidor de archivos pueden hacer que se vuelva a llamar a la delegación. Si GPFS se está exportando mediante NFSv4, un acceso en el nodo GPFS de la red puede hacer que se vuelva a llamar a la delegación.

La esencia de una delegación es que permite al cliente atender localmente las operaciones tales como OPEN, CLOSE, LOCK, LOCKU, READ y WRITE sin ninguna interacción inmediata con el servidor.

La delegación de servidor está habilitada de forma predeterminada. La delegación de servidor se pueden inhabilitar con el mandato `nfsd -o server_delegation=0`. Los administradores pueden utilizar la opción **exportfs** `deleg=yes | no` para inhabilitar o habilitar la concesión de delegaciones por sistema de archivos, lo que alterará temporalmente el valor de **nfsd**.

La delegación de cliente se puede inhabilitar con el mandato `nfsd -o client_delegation=0`. La delegación de cliente se debe establecer antes de que tenga lugar cualquier montaje en el cliente.

Si el administrador está exportando un sistema de archivos donde muchos clientes grabarán en muchos archivos comunes, es posible que el administrador inhabilite las delegaciones para dicho sistema de archivos.

Si no se puede contactar con el cliente (por ejemplo, si se produce una interrupción en la red o el cliente) es posible que otros clientes se retarden al acceder a los datos.

### **Establecimiento de principales genéricos de sistema principal para vías de devolución de llamada protegidas por Kerberos**

Puede configurar una vía de devolución de llamada para IBM Network Authentication Service (Kerberos).

El cliente que recibe la delegación debe ser un cliente completo con su propio principal de sistema principal. Sin embargo, puede establecer un principal genérico de sistema principal para que lo utilicen todos los clientes para las devoluciones de llamada.

Si desea establecer un principal genérico de sistema principal para que lo utilicen todos los clientes para las devoluciones de llamada, realice estos pasos:

1. Para crear un principal de servicio (por ejemplo, `nfs/client`) utilizando el mismo método utilizado para crear un principal de sistema principal, consulte el apartado [Creación de un principal de Kerberos](#) en la publicación *Security*.
2. Cree una entrada keytab para ese principal de servicio.  
Por ejemplo, para crear un keytab denominado `slapd_krb5.keytab`, realice lo siguiente:

```
kadmin.local: ktadd -k /etc/security/slapd_krb5.keytab ldap/plankton.austin.ibm.com
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type Triple DES cbc mode with HMAC/sha1 added to keytab
WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type ArcFour with HMAC/md5 added to keytab WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type AES-256 CTS mode with 96-bit SHA-1 HMAC added to keytab
WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type DES cbc mode with RSA-MD5 added to keytab WRFILE:/etc/security/
slapd_krb5.keytab.
kadmin.local:
```

3. Distribuya este keytab a todos los clientes que lo utilizarán.

4. Configure los clientes con el mandato **nfshostkey**.

Este proceso es idéntico al proceso de configuración de un servidor para utilizarlo con Kerberos, pero el principal genérico no se puede utilizar para los servidores; cada servidor debe tener un principal propio con el formato *nfs/nombre\_sistpral*.

## Sistemas de archivos de red a corto plazo STNFS

Un sistema de archivos de red a corto plazo STNFS es una copia de seguridad de sistema de archivos que hace Network File System (NFS) y el sistema de archivos STNFS permite modificaciones locales en los archivos. Las modificaciones no se guardan en el servidor.

### Notas:

**1**

Muchos de los clientes STNFS pueden compartir la misma imagen de sistema de archivos desde un servidor, pero las modificaciones sólo las verá el cliente que realiza la modificación.

**2**

Las modificaciones efectuadas por un cliente se pierden cuando el sistema de archivos está montado o cuando el cliente vuelva a arrancar.

**3**

Las grabaciones desde STNFS no se ejecutarán correctamente cuando la memoria del sistema esté por debajo del umbral predeterminado. Este umbral es interno en STNFS y no se puede configurar externamente.

## Montaje de un sistema de archivos a corto plazo NFS

El mandato **montaje** se utiliza para montar un sistema de archivos NFS a corto plazo. Por ejemplo, escriba el mandato siguiente:

```
mount -v stnfs -o options server:/remote-path /local-path
```

Las opciones disponibles son las siguientes:

### **vers=3**

Utilice NFS versión 3 para establecer comunicación con el servidor.

### **vers=4**

Utilice NFS versión 4 para establecer comunicación con el servidor.

### **rsize=size**

Establezca los bytes de tamaño de lectura.

### **proto=udp**

Utilice UDP para establecer comunicación con el servidor NFS.

### **proto=tcp**

Utilice TCP para establecer comunicación con el servidor NFS.

### **hard**

Utilice montajes fijos NFS.

**soft**

Utilice montajes flexibles NFS.

**sec**

Utilice la clasificación de seguridad especificada.

Las opciones predeterminadas son:

```
vers=3  
rsize=32768  
proto=tcp  
hard  
sec=sys
```

## **Lista de comprobación para configurar NFS**

Después de instalar el software NFS en los sistemas, estará preparado para configurar NFS. Siga estos pasos para configurar NFS.

Se debe instalar la biblioteca de kernel CLiC (CryptoLite in C) antes de configurar NFS para utilizar los siguientes tipos de seguridad:

- krb5
- krb5i
- krb5p

Cada paso se describe con más detalles a continuación.

1. Determine qué sistemas de la red deben ser servidores y qué sistemas deben ser clientes (un sistema se puede configurar como servidor y cliente).
2. Determine qué versión de NFS va a utilizar.
3. Decida si va a utilizar la seguridad RPCSEC-GSS. En caso afirmativo, consulte las consideraciones del apartado [“Configuración de una red para RPCSEC-GSS” en la página 618](#).
4. Para cada sistema (cliente o servidor), siga las instrucciones del apartado [“Iniciar los daemons NFS en el arranque de sistema” en la página 615](#).
5. Para cada servidor NFS, siga las instrucciones del apartado [“Configuración de un servidor NFS” en la página 616](#).
6. Para cada cliente NFS, siga las instrucciones del apartado [“Configuración de un cliente NFS” en la página 616](#).
7. Si desea que los sistemas personales de la red tengan acceso a los servidores NFS (además de poder montar sistemas de archivos), configure PC-NFS siguiendo las instrucciones del apartado [“PC-NFS” en la página 631](#).
8. Si piensa utilizar NFS versión 4, consulte las consideraciones del apartado [“Soporte de NFS versión 4” en la página 604](#).

## **Iniciar los daemons NFS en el arranque de sistema**

De forma predeterminada, los daemons NFS no se inician durante la instalación.

Cuando se instalan, todos los archivos se colocan en el sistema, pero no se realizan los pasos para activar NFS. Puede iniciar los daemons NFS en el arranque del sistema mediante:

- La vía de acceso rápida de SMIT, `smit mknfs`
- El mandato **mknfs**.

Todos estos métodos colocan una entrada en el archivo `inittab` para que el script `/etc/rc.nfs` se ejecute cada vez que se reinicie el sistema. Este script, a su vez, inicia todos los daemons NFS necesarios para un sistema determinado.

## Configuración de un servidor NFS

Utilice este procedimiento para configurar un servidor NFS.

Para configurar un servidor NFS:

1. Cree el archivo `/etc(exports`. Consulte el apartado “[Archivo /etc/exports](#)” en la página 599.
2. Si está utilizando Kerberos, configure el servidor NFS como cliente Kerberos. Consulte el apartado “[Configuración de una red para RPCSEC-GSS](#)” en la página 618.
3. Si está utilizando NFS versión 4, establezca el dominio NFS versión 4 utilizando el mandato [\*\*chnfsdom\*\*](#). Inicialmente, puede especificar el dominio de internet del servidor en el archivo. Sin embargo, es posible definir un dominio NFS versión 4 que sea diferente del dominio de internet del servidor. Si desea una aclaración sobre esto, consulte en el mandato [\*\*nfsrgyld\*\*](#) la documentación sobre el daemon de registro NFS.
4. Si está utilizando NFS versión 4 con Kerberos, es posible que necesite crear el archivo `/etc/nfs/realm.map`. Consulte el apartado “[Archivo /etc/nfs/realm.map](#)” en la página 600.
5. Si desea utilizar la autenticación de Kerberos en el servidor, debe habilitar la seguridad ampliada en el servidor. Puede habilitar la seguridad ampliada mediante la utilización de SMIT o utilizando el mandato [\*\*chnfs -S -B\*\*](#).

## Configuración de un cliente NFS

Utilice este procedimiento para configurar un cliente NFS.

1. Inicie NFS utilizando las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.
2. Establezca el punto de montaje local utilizando el mandato [\*\*mkdir\*\*](#).

Para que NFS complete un montaje satisfactoriamente, debe existir un directorio que actúe como punto de montaje (o espacio reservado) de un montaje NFS. Este directorio debe estar vacío. Este punto de montaje se puede crear como cualquier otro directorio y no se necesitan atributos especiales.

**Nota:** Los puntos de montaje de todos los montajes NFS deben existir en el sistema antes de montar un sistema de archivos, con una excepción. Si se utiliza el daemon [\*\*automount\*\*](#), no es necesario crear puntos de montaje.

3. Si utiliza Kerberos, siga estos pasos:

- a) Configure el cliente NFS en una región de Kerberos.

Esto se realiza con el mandato [\*\*config.krb5\*\*](#). Consulte la publicación *IBM Network Authentication Service Administrator's and User's Guide* para obtener detalles de configuración.

- b) Cree principales de Kerberos para todos los usuarios del cliente que va a acceder a los archivos a través de montajes Kerberos.

Esto se realiza con el mandato [\*\*kadmin\*\*](#). Consulte la publicación *Network Authentication Service Administrator's and User's Guide* para obtener una descripción de cómo crear principales de Kerberos.

- c) El establecimiento de un principal de Kerberos para la propia máquina cliente es opcional.

Un cliente sin principal se conoce como *cliente limitado* y un cliente con un principal se denomina *cliente completo*. Los clientes limitados utilizan una seguridad NFS RPC más floja al realizar determinadas operaciones de gestión de contexto de cliente a servidor de NFS versión 4 que se utilizan para la gestión de estado. En función de la configuración, un cliente completo puede utilizar la seguridad de RPC basada en Kerberos más potente. Las configuraciones de cliente limitado necesitan menos sobrecarga administrativa y pueden ser suficientes para muchos entornos. Los despliegues que necesitan los niveles más altos de seguridad pueden elegir ejecutar configuraciones de cliente completo.

4. Si está utilizando NFS versión 4, también debe establecer un dominio NFS versión 4 utilizando el mandato [\*\*chnfsdom\*\*](#).

Inicialmente, puede especificar el dominio de internet del cliente en el archivo. Sin embargo, es posible definir un dominio NFS versión 4 que sea diferente del dominio de internet del cliente. Si desea una aclaración sobre esto, consulte la documentación para el daemon de registro NFS **nfsrgyd**.

5. Si desea utilizar la autenticación de Kerberos en el cliente, debe habilitar la seguridad ampliada en el cliente.

Puede habilitar la seguridad ampliada utilizando SMIT o utilizando el mandato **chnfs -S -B**. Para obtener más información sobre **chnfs**, consulte la página de consulta del mandato **chnfs**.

6. Establezca y monte los montajes predefinidos siguiendo las instrucciones del apartado “[Establecimiento de montajes NFS predefinidos](#)” en la página 625.

## Correlación de identidad

La correlación de identidad proporciona un método para que el cliente y servidor NFS locales conviertan a los usuarios y grupos externos en usuarios y grupos locales.

Para realizar la correlación de identidad, AIX utiliza la tecnología EIM, que se basa en LDAP. Todos los datos de correlación de identidad NFS se almacenan en un servidor LDAP.

Para configurar un cliente EIM, se deben instalar los catálogos de archivos `bos.eim.rte` y `ldap.client`. El servidor EIM también necesita el conjunto de archivos `ldap.server`. Después de que se hayan instalado los catálogos apropiados, se utiliza `/usr/sbin/chnfsim` para configurar EIM. Las opciones de configuración mínimas son las siguientes:

```
/usr/sbin/chnfsim -c -a -t [tipo] -h [servidor EIM] -e [dominio LDAP/EIM] -f [sufijo LDAP] -w [contraseña administrador]
```

Esto configura los clientes y servidores EIM para utilizar un servidor EIM específico para la correlación de identidad. Si el nombre de sistema principal especificado en el mandato es el nombre de sistema principal local, también se configurará un servidor LDAP.

Cuando se ha completado el paso de configuración, el administrador EIM puede llenar el servidor LDAP con los datos de correlación de identidad NFS. Un usuario o grupo individual, por ejemplo John Doe, se conoce como una identidad de correlación. La serie de propietario NFS de dicho usuario, `johndoe@austin.ibm.com`, se conoce como una correlación de identidad. Para entrar estos datos en el servidor LDAP, se deberá ejecutar el siguiente mandato:

```
/usr/sbin/chnfsim -a -u -i "John Doe" -n johndoe -d austin.ibm.com
```

La identidad de correlación es el nombre descriptivo del usuario o grupo y la correlación de identidad es la serie de propietario NFS `nombre@dominio`. Las correlaciones entre región y dominio también se almacenan en el servidor LDAP. Para establecer que la región de Kerberos `kerb.austin.ibm.com` se correlacione con el dominio NFS `austin.ibm.com`, se debe ejecutar el mandato siguiente:

```
/usr/sbin/chnfsim -a -r kerb.austin.ibm.com -d austin.ibm.com
```

Para configurar NFS de forma que utilice los datos de correlación en EIM, es necesario reiniciar el daemon de registro NFS. El daemon de registro NFS comprueba al arrancar si hay un servidor EIM disponible y, si encuentra alguno, todas las funciones de correlación pasan a través de EIM y dejan de utilizarse todas las correlaciones locales.

Para obtener información sobre EIM, consulte la [Correlación de identidad de empresa](#) en la publicación *Security*.

## Exportación de un sistema de archivos NFS

Puede exportar un sistema de archivos NFS utilizando los procedimientos siguientes.

- Para exportar un sistema de archivos NFS utilizando la SMIT:

1. Verifique que el NFS ya esté en ejecución escribiendo el mandato `lssrc -g nfs`. La salida debe indicar que los daemons **nfsd** y **rpc.mountd** están activos. Si no lo están, inicie NFS utilizando las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.

2. En una línea de mandatos, escriba lo siguiente y pulse Intro:

```
smmit mknfsexp
```

3. Especifique los valores apropiados en los campos Nombre de vía de acceso del directorio que desea exportar, Modalidad para exportar directorio y Exportar directorio ahora, en el rearranque del sistema o ambos.
  4. Especifique otras características opcionales que desee o acepte los valores predeterminados dejando los campos restantes tal como están.
  5. Cuando haya terminado de realizar cambios, SMIT actualizará el archivo /etc(exports. Si el archivo /etc(exports no existe, se crea.
  6. Repita los pasos 3 a 5 para cada directorio que desee exportar.
- Para exportar un sistema de archivos NFS utilizando un editor de texto:
    1. Abra el archivo /etc(exports con el editor de texto que prefiera.
    2. Cree una entrada para cada directorio que se debe exportar utilizando el nombre de vía de acceso completa del directorio. Liste cada directorio que se debe exportar empezando en el margen izquierdo. Ningún directorio debe incluir ningún otro directorio que ya se haya exportado. Consulte el archivo /etc(exports en la publicación *Referencia de archivos* para obtener una descripción de la sintaxis completa de las entradas del archivo /etc(exports.
    3. Guarde y cierre el archivo /etc(exports.
    4. Si NFS está en ejecución, escriba el mandato siguiente y pulse Intro.

```
/usr/sbin/exportfs -a
```

La opción **-a** indica al mandato **exportfs** que envíe toda la información del archivo /etc(exports al kernel. Si NFS no está en ejecución, inicie NFS utilizando las instrucciones del apartado “Inicio de los daemons NFS” en la página 603.

- Para exportar temporalmente un sistema de archivos NFS (sin cambiar el archivo /etc(exports), escriba el mandato siguiente y pulse Intro:

```
exportfs -i /nombredir
```

donde *nombredir* es el nombre del sistema de archivos que desea exportar. El mandato **exportfs -i** especifica que no se debe comprobar el archivo /etc(exports para el directorio especificado y que todas las opciones se toman directamente de la línea de mandatos.

El soporte de AIX NFS versión 4 permite al administrador crear y controlar un espacio de nombres alternativo que el servidor NFS presenta a los clientes. Esto se realiza utilizando la opción de exportación **exname**. Este soporte también se puede utilizar para ocultar a los clientes NFS los detalles del espacio de nombres del sistema de archivos local del servidor.

## Configuración de una red para RPCSEC-GSS

La red que se está configurando en este caso de ejemplo contiene cinco servidores y se configura para RPCSEC-GSS.

Los cinco servidores de la red son los siguientes:

- kdc.austin.ibm.com
- alpha.austin.ibm.com
- beta.austin.ibm.com
- gamma.austin.ibm.com
- zeta.austin.ibm.com

El sistema kdc.austin.ibm.com se configurará como servidor KDC (Key Distribution Center - Centro de distribución de claves) y se creará la región de Kerberos AUSTIN.IBM.COM, en la que todos los sistemas

excepto kdc.austin.ibm.com y zeta.austin.ibm.com serán servidores NFS ofreciendo sistemas de archivos exportados con RPCSEC-GSS.

Los sistemas alpha.austin.ibm.com y beta.austin.ibm.com tienen un enlace adicional entre ellos; a través de ese enlace, aparecen uno ante el otro como fast\_alpha.test.austin.com y fast\_beta.test.austin.ibm.com. Por esta razón, será necesario realizar un paso de configuración adicional.

Además, esta red tiene los siguientes usuarios, que se han configurado en algunos de los sistemas:

- adam
- brian
- charlie
- dave
- eric

**Nota:** La configuración siguiente se proporciona como ejemplo y es posible que no sea apropiada para todos los entornos. Consulte la Guía del administrador y del usuario para conocer el Servicio de autenticación de red antes de intentar configurar una nueva región de Kerberos.

**Nota:** Kerberos requiere que la hora de sistema sea razonablemente parecida en toda la red. Antes de ejecutar este procedimiento, deberá configurar un mecanismo para sincronizar automáticamente la hora en toda la red, por ejemplo el daemon AIX **timed** o una configuración de NTP.

### 1. Configure el servidor KDC.

**Nota:** Idealmente el servidor KDC no se deberá utilizar con ningún otro fin; si KDC está comprometido, todos los principales de Kerberos estarán comprometidos.

En este caso, kdc.austin.ibm.com se configurará como el servidor KDC. La configuración siguiente es para **des3**. Si, por razones de rendimiento, se prefiere **des**, añada el argumento -e des-cbc-crc:normal a las llamadas addprinc y ktadd para **kadmin** más abajo.

Para configurar la red con cifrado **aes**, añada el argumento -e aes256-cts:normal a las llamadas addprinc y ktadd para el mandato **kadmin**.

a) Instale el catálogo de archivos **krb5.server.rte** en **kdc.austin.ibm.com**.

b) Configure el servidor KDC. En este caso, se ha utilizado el mandato siguiente:

```
config.krb5 -S -d austin.ibm.com -r AUSTIN.IBM.COM
```

Después de ejecutar este mandato, el sistema solicitará una contraseña de base de datos maestra y una contraseña para el principal administrativo.

c) Cree principales para cada usuario y sistema principal ejecutando el mandato **/usr krb5/sbin/kadmin.local** en el servidor KDC. Este ejemplo crea principales de Kerberos que coinciden con el nombre del usuario de UNIX asociado. NFS correlacionará el nombre de principal con el nombre de usuario para determinar la credencial de UNIX asociada con el principal. Para obtener una descripción de cómo utilizar correlaciones más generales entre los principales y los nombres de usuario, consulte el apartado “[Correlación de identidad](#)” en la página 617. Para esta red, hemos creado los siguientes principales:

- adam
- brian
- charlie
- dave
- eric
- nfs/alpha.austin.ibm.com
- nfs/beta.austin.ibm.com
- nfs/gamma.austin.ibm.com

**Nota:** Los nombres de principal de usuario elegidos deben coincidir con los nombres de usuario correspondientes del registro de usuarios configurado del sistema (/etc/passwd, **LDAP**, **NIS**, etc). NFS utiliza el nombre de principal como nombre de usuario para obtener los ID de usuario y de grupo del sistema local. Si los nombres no coinciden, el acceso se tratará como un acceso anónimo.

KDC ya se ha configurado.

2. Cada cliente y servidor NFS se configurarán ahora como clientes de Kerberos utilizando el mandato **config.krb5**.

El modo de llevar a cabo esta acción depende del modo en que se haya configurado KDC. En este caso hemos ejecutado el mandato siguiente en cada sistema NFS:

```
config.krb5 -C -d austin.ibm.com -r AUSTIN.IBM.COM -c kdc.austin.ibm.com  
-s kdc.austin.ibm.com
```

Ahora es posible ejecutar **kinit** como cualquiera de los principales de usuario en cualquiera de los sistemas configurados. Por ejemplo, para ejecutar **kinit** como el usuario adam, ejecute el mandato siguiente:

```
/usr/krb5/bin/kinit adam
```

Necesitará especificar la contraseña de Kerberos, no de AIX, de adam.

Este ejemplo utiliza **kinit** para autenticar al usuario. Es posible configurar AIX para utilizar la autenticación de Kerberos durante el inicio de sesión del sistema. Para obtener más información, consulte el apartado Authenticating to AIX Using Kerberos en la publicación *Security*.

3. Ahora cada servidor NFS se configurará con la entrada keytab apropiada.

En este caso, hemos configurado la entrada keytab para alpha.austin.ibm.com como ejemplo; se utilizará el mismo proceso exacto en beta.austin.ibm.com y gamma.austin.ibm.com.

- a) Desde alpha.austin.ibm.com, ejecute el mandato **kadmin**. A continuación, ejecute el mandato siguiente:

```
ktadd nfs/alpha.austin.ibm.com
```

Esto crea un archivo keytab.

- b) A continuación, configure el daemon **gssd** para utilizar el archivo keytab que acaba de crear con el mandato **nfshostkey**.

En este caso, hemos ejecutado lo siguiente:

```
nfshostkey -p nfs/alpha.austin.ibm.com -f /etc/krb5/krb5.keytab
```

- c) Configure el daemon **gssd** para arrancar automáticamente ejecutando el siguiente mandato:

```
chnfs -S -B
```

Repita esta configuración para cada sistema.

4. Aunque en este punto el servidor NFS no funcionará, todos los usuarios pasarán como nobody. Es aconsejable que todos los usuarios existan en todos los servidores con los mismos uid y gid; los usuarios que no existan sólo tendrán acceso al directorio exportado como nobody. Para que los nombres de usuario se correlacionen correctamente, debe configurar el daemon de registro NFS.

- a) Configure el dominio utilizando el mandato **chnfsdom**. En este caso, se ha ejecutado el mandato siguiente en todos los servidores NFS para configurar austin.ibm.com como dominio:

```
chnfsdom austin.ibm.com
```

- b) Configure el archivo /etc/nfs/realm.map; este archivo debe contener una línea, con el nombre de región seguido del dominio local.

Para la red de ejemplo, estos dos archivos tendrán este aspecto en todos los servidores NFS:

```
realm.map AUSTIN.IBM.COM
```

```
austin.ibm.com
```

Dado que la entrada de región (realm) de este archivo no es sensible a las mayúsculas y minúsculas, técnicamente esta entrada no es necesaria.

- c) Para zeta.austin.ibm.com, que no será un servidor NFS, arranque el daemon **gssd** utilizando el mandato chnfs -S -B. Antes de intentar cualquier operación de cliente de Kerberos, el usuario debe utilizar **kinit** para obtener credenciales válidos.
5. En este caso, hay una configuración de enlace de red rápido entre alpha.austin.ibm.com y beta.austin.ibm.com. A través de este enlace, beta.austin.ibm.com verá alpha.austin.ibm.com como fast\_alpha.test.austin.ibm.com y alpha.autsin.ibm.com verá beta.austin.ibm.com como fast\_beta.test.austin.ibm.com. Puesto que nfs/fast\_alpha.test.austin.ibm.com y nfs/fast\_beta.test.austin.ibm.com no son principales válidos, no podrán utilizar este enlace para los montajes.

Para corregir esto, se utilizará el mandato **nfshostmap**, que correlacionará el principal para manejar esta situación.

- a) En alpha.austin.ibm.com, hemos ejecutado el mandato siguiente:

```
nfshostmap -a beta.austin.ibm.com fast_beta.test.austin.ibm.com
```

Esto indica a alpha.austin.ibm.com que el principal de fast\_beta.test.austin.ibm.com es para beta.austin.ibm.com.

- b) En beta, hemos ejecutado el mandato siguiente:

```
nfshostmap -a alpha.austin.ibm.com fast_alpha.test.austin.ibm.com
```

Los servidores pueden tener varios principales de sistema principal. Presuponiendo que la dirección IP para fast\_alpha sea 10.0.0.1 y que la dirección IP para fast\_beta sea 10.0.0.2, complete los pasos siguientes para añadir varios principales de sistema principal:

- a) Añada los principales nfs/fast\_alpha.test.austin.ibm.com y nfs/fast\_beta.test.austin.ibm.com a los archivos keytab apropiados.
- b) Ejecute el mandato **nfshostkey** en el servidor alpha, de la siguiente manera:

```
nfshostkey -a -p nfs/fast_alpha.test.austin.ibm.com -i 10.0.0.1
```

- c) Ejecute el mandato **nfshostkey** en el servidor beta, de la siguiente manera:

```
nfshostkey -a -p nfs/fast_beta.test.austin.ibm.com -i 10.0.0.2
```

## Eliminación de la exportación de un sistema de archivos NFS

Puede eliminar la exportación de un directorio NFS utilizando los procedimientos siguientes.

- Para eliminar la exportación de un directorio NFS utilizando SMIT:
  - Escriba lo siguiente en un indicador de mandatos y pulse Intro:

```
smit rmmfsexp
```

- Entre el nombre de vía de acceso apropiado en el campo de Vía de acceso del directorio exportado que se debe eliminar.

Ahora el directorio se elimina del archivo /etc/exports y se elimina su exportación.

Si el directorio se exporta a los clientes utilizando NFS versión 4, es posible que falle la eliminación de la exportación debido al estado de archivo en el servidor. El estado de archivo significa que un cliente abre los archivos de los directorios exportados. Puede realizar alguna acción para hacer que las aplicaciones dejen de utilizar esos datos o puede forzar la eliminación de la exportación (**exportfs -F**) de los datos, lo que puede producir anomalías en las aplicaciones que están utilizando activamente los datos.

- Para eliminar la exportación de un directorio NFS utilizando un editor de texto:
  - Abra el archivo `/etc(exports` con el editor de texto que prefiera.
  - Busque la entrada correspondiente al directorio cuya exportación desea eliminar y suprima dicha línea.
  - Guarde y cierre el archivo `/etc(exports`.
  - Si NFS se está ejecutando actualmente, entre:

```
exportfs -u nombredir
```

donde *nombredir* es el nombre de vía de acceso completo del directorio que acaba de suprimir de los archivos `/etc(exports`. Si falla la eliminación de la exportación debido al acceso por parte de clientes NFS V4, puede añadir una opción `-F` para forzar que se elimine la exportación del directorio.

## Cambio de un sistema de archivos exportado

Cambie un sistema de archivos NFS exportado utilizando los siguientes procedimientos.

- Para cambiar un sistema de archivos NFS exportado utilizando SMIT:

1. Para eliminar la exportación del sistema de archivos, escriba:

```
exportfs -u /nombredir
```

donde *nombredir* es el nombre del sistema de archivos que desea cambiar.

2. Escriba:

```
smit chnfsexp
```

3. Entre el nombre de vía de acceso apropiado en el campo PATHNAME del directorio exportado.

4. Realice los cambios que desee.

5. Salga de SMIT.

6. Vuelva a exportar el sistema de archivos entrando:

```
exportfs /nombredir
```

donde *nombredir* es el nombre del sistema de archivos que acaba de cambiar.

- Para cambiar un sistema de archivos NFS exportado utilizando un editor de texto:

1. Para eliminar la exportación del sistema de archivos, escriba:

```
exportfs -u /nombredir
```

donde *nombredir* es el nombre del sistema de archivos que desea cambiar.

2. Abra el archivo `/etc(exports` con el editor de texto que prefiera.

3. Realice los cambios que desee.

4. Guarde y cierre el archivo `/etc(exports`.

5. Vuelva a exportar el sistema de archivos entrando:

```
exportfs /nombredir
```

donde *nombredir* es el nombre del sistema de archivos que acaba de cambiar.

## Acceso de usuario root a un sistema de archivos exportado

Cuando se exporta un sistema de archivos, de forma predeterminada no se otorga al usuario root el acceso de root a ese sistema de archivos exportado.

Cuando un usuario root de un sistema principal solicita el acceso a un archivo determinado de NFS, NFS correlaciona el ID de usuario del solicitante con el ID del usuario nobody (nobody es uno de los nombres de usuario colocados en el archivo /etc/password de forma predeterminada). Los derechos de acceso del usuario nobody son los mismos que los proporcionados al público (*others*) para un archivo determinado. Por ejemplo, si *others* sólo tiene permiso de ejecución para un archivo, el usuario nobody sólo puede ejecutar el archivo.

Para habilitar el acceso de usuario root a un sistema de archivos exportado, siga las instrucciones del apartado “Cambio de un sistema de archivos exportado” en la página 622. Si utiliza el método de SMIT, especifique en el campo de acceso de root permitido HOSTS el nombre del host en el que desea otorgar acceso de root. Si edita el archivo con un editor de texto, añada el cualificador -root=nombressistpral en la entrada de sistema de archivos. Por ejemplo,

```
/usr/tps -root=hermes
```

especifica que el usuario root del sistema principal hermes puede acceder al directorio /usr/tps con privilegios de root.

## Montaje explícito de un sistema de archivos NFS

Para montar un directorio NFS explícitamente, utilice el procedimiento siguiente:

1. Verificar que el servidor NFS ha exportado el directorio:

```
showmount -e NombreServidor
```

donde *NombreServidor* es el nombre del servidor NFS. Este mandato visualiza los nombres de los directorios exportados actualmente del servidor NFS. Si el directorio que desea montar no se lista, exporte el directorio del servidor.

**Nota:** El mandato **showmount** no funcionará para sistemas de archivos que se han exportado solamente como sistemas de archivos NFS versión 4. Para NFS versión 4, el cliente puede montar el sistema de archivos raíz para el servidor y atravesar la estructura de directorios exportados. Los sistemas de archivos individuales exportados no tienen que montarse explícitamente para que el cliente acceda a ellos.

2. Establezca el punto de montaje local utilizando el mandato **mkdir**.

Debe existir un directorio nulo (vacío) que actúa como punto de montaje (o espacio reservado) de un montaje NFS para que NFS realice un montaje satisfactoriamente. Este punto de montaje se puede crear como cualquier otro directorio y no se necesitan atributos especiales.

3. Escriba:

```
mount NombreServidor:/remote/directorio /local/directorio
```

donde *NombreServidor* es el nombre del servidor NFS, */remote/directorio* es el directorio del servidor NFS que desea montar y */local/directorio* es el punto de montaje en el cliente NFS.

4. En la máquina cliente, escriba la siguiente vía de acceso rápida de SMIT:

```
smit mknfsmnt
```

5. En los campos siguientes realice los cambios que sean apropiados para la configuración de red. Es posible que la configuración no necesite completar todas las entradas de esta pantalla.

**Nota:** Si se está utilizando la interfaz SMIT, pulse la tecla Tabulador para cambiar al valor correcto para cada campo, pero *no* pulse Intro hasta que realice el paso 7.

- NOMBRE DE VÍA DE ACCESO de punto de montaje.
- NOMBRE DE VÍA DE ACCESO de directorio remoto.
- SISTEMA PRINCIPAL donde reside el directorio remoto.
- ¿MONTAR ahora, añadir entrada a /etc/filesystems o ambas acciones?
- La entrada /etc/filesystems montará el directorio en el REINICIO del sistema.

- MODALIDAD para este sistema de archivos NFS.
- Cambie o utilice los valores predeterminados para las entradas restantes, en función de la configuración de NFS.
  - Cuando haya terminado de realizar todos los cambios en esta pantalla, SMIT montará el sistema de archivos NFS.
  - Cuando el campo **Mandato:** muestre el estado OK, salga de SMIT.

Ahora el sistema de archivos NFS está preparado para utilizarse.

## Subsistema automount

El subsistema **automount** permite a los usuarios no root montar sistemas de archivos remotos una vez que el usuario root ha especificado los puntos de montaje iniciales.

El archivo `/etc/auto_master` especifica esta información. Estos puntos de montaje, conocidos como claves, tienen una correlación correspondiente que determina qué sistema de archivos remoto está montado sobre él. El formato del archivo `/etc/auto_master` es el siguiente:

```
/key      correlación
```

**Nota:** El archivo `/etc/auto_master` se lee cuando el mandato **automount** se ejecuta inicialmente y los cambios efectuados en el mismo no entrarán en vigor hasta que se ejecute otra vez el mandato **automount**.

Las correlaciones más comunes son las correlaciones directas, correlaciones indirectas y correlaciones de sistema principal.

### Correlaciones directas

Las correlaciones directas necesitan una clave especial (/ -) en el archivo `/etc/auto_master`.

La correlación es un archivo con el formato siguiente:

```
/clavedirecta  [-opciones]  servidor:/dir
```

Cuando un usuario acceda al directorio `/clavedirecta`, el daemon **automount** montará `servidor:/dir` sobre `/clavedirecta`.

### Correlaciones indirectas

Otra clase de correlación que determina qué sistema de archivos remoto está montado sobre un punto de montaje es una correlación indirecta.

Las correlaciones indirectas tienen el formato siguiente:

```
claveindirecta  [-opciones]  servidor:/dir
```

Cuando un usuario acceda al directorio `/key/claveindirecta`, el daemon **automount** montará `servidor:/dir` sobre `/key/claveindirecta`.

### Correlaciones de sistema principal

Las correlaciones de sistema principal necesitan una correlación especial (-hosts) en el archivo `/etc/auto_master`.

El daemon **automount** creará un subdirectorio bajo el directorio `/key` para cada servidor listado en el archivo `/etc/hosts`. Cuando un usuario acceda al directorio `/key/server`, el daemon **automount** montará los directorios exportados del servidor sobre el directorio `/key/server`.

### Utilización de AutoFS para montar automáticamente un sistema de archivos

**AutoFS** se basa en el uso del mandato **automount** para propagar la información de configuración de montaje automático en la extensión de kernel **AutoFS** e iniciar el daemon **automountd**.

Mediante la propagación de configuración, la extensión monta de forma automática y transparente sistemas de archivos siempre que se abre un archivo o un directorio de dicho sistema de archivos. La

extensión informa al daemon **automountd** de las peticiones de montaje y desmontaje y el daemon **automountd** realiza realmente el servicio solicitado.

Dado que el enlace de nombre a ubicación es dinámico dentro del daemon **automountd**, las actualizaciones en una correlación de NIS (Network Information Service) utilizada por el daemon **automountd** son transparentes para el usuario. Asimismo, no es necesario montar previamente sistemas de archivos compartidos para aplicaciones que tienen referencias establecidas en el código a archivos y directorios, ni es necesario mantener registros de los sistemas principales que se deben montar para aplicaciones determinadas.

**AutoFS** permite montar sistemas de archivos como sea necesario. Con este método de montaje de directorios, no es necesario que todos los sistemas de archivos estén montados todo el tiempo; sólo se montan los que se están utilizando.

Por ejemplo, para montar un directorio NFS automáticamente:

1. Verifique que el servidor NFS ha exportado el directorio entrando:

```
showmount -e NombreServidor
```

donde *NombreServidor* es el nombre del servidor NFS. Este mandato visualiza los nombres de los directorios exportados actualmente del servidor NFS.

2. Cree un archivo maestro **AutoFS** y un archivo de correlación. **AutoFS** monta y desmonta los directorios especificados en estos archivos de correlación.

Por ejemplo, suponga que desea que **AutoFS** monte los directorios /local/dir1 y /local/dir2 que sean necesarios del servidor **serve1** en los directorios /remote/dir1 y /remote/dir2, respectivamente. La entrada de archivo *auto\_master* será la siguiente:

```
/remote          /tmp/mount.map
```

El entrada de archivo /tmp/mount.map será la siguiente:

```
dir1    -rw    serve1:/local/dir1
dir2    -rw    serve1:/local/dir2
```

3. Asegúrese de que la extensión de kernel **AutoFS** se cargue y el daemon **automountd** esté en ejecución. Esto se puede llevar a cabo de dos maneras:

a) Utilizando el mandato **automount**: Emita /usr/sbin/automount -v.

b) Utilizando **SRC**: Emita lssrc -s automountd. Si el subsistema **automountd** no está en ejecución, emita startsrc -s automountd.

**Nota:** Si se inicia el daemon **automountd** con el mandato **startssrc**, se ignorarán los cambios que se han realizado en el archivo *auto\_master*.

4. Para detener el daemon **automount**, emita el mandato stopsrc -s automountd.

Si, por alguna razón, se ha iniciado el daemon **automountd** sin utilizar **SRC**, emita:

```
kill PID_automountd
```

donde *PID\_automountd* es el ID de proceso del daemon **automountd**. (Al ejecutar el mandato ps -e, se visualiza el ID de proceso del daemon **automountd**.) El mandato **kill** envía una señal SIGTERM al daemon **automountd**.

## Establecimiento de montajes NFS predefinidos

Puede establecer montajes NFS predefinidos utilizando uno de los procedimientos siguientes.

**Nota:** Defina las opciones **bg** (segundo plano) e **intr** (interrumpible) en el archivo /etc/filesystems al establecer un montaje predefinido que se monta durante el arranque del sistema. Los montajes que no son interrumpibles y que se ejecutan en el primer plano pueden colgar el cliente si la red o el servidor está inactivo cuando arranca el sistema cliente. Si un cliente no puede acceder a la red o al servidor, el usuario debe iniciar la máquina otra vez en modalidad de mantenimiento y editar las peticiones de montaje apropiadas.

- Para establecer montajes predefinidos mediante SMIT:

a) Escriba:

```
smit mknfsmnt
```

b) Especifique valores en esta pantalla para cada montaje que desea predefinir. Especifique un valor para cada campo necesario (los marcados con un asterisco (\*) en el margen izquierdo). Asimismo especifique valores para los demás campos o acepte los valores predeterminados.

Este método crea una entrada en el archivo /etc/filesystems para el montaje deseado e intenta el montaje.

- Para establecer los montajes predeterminados NFS editando el archivo /etc/filesystems:

a) Abra el archivo /etc/filesystems con un editor de texto.

b) Añada entradas para cada uno de los sistemas de archivos remotos que se deben montar cuando se inicia el sistema. Por ejemplo:

```
/home/jdoe:
dev = /home/jdoe
mount = false
vfs = nfs
nodename = mach2
options = ro,soft
type = nfs_mount
```

Esta stanza indica al sistema que monte el directorio remoto /home/jdoe sobre el punto de montaje local del mismo nombre. El sistema de archivos se monta como sólo de lectura (ro). Dado que también se monta como soft, se devuelve un error en el caso de que el servidor no responda. Si se especifica el parámetro type como nfs\_mount, el sistema intenta montar el archivo /home/jdoe (junto con cualquier otro sistema de archivos que se especifique en el grupo type = nfs\_mount) cuando se emite el mandato **mount -t nfs\_mount**.

La stanza de ejemplo siguiente indica al sistema que monte el sistema de archivos /usr/games en el arranque del sistema. Si falla el montaje, el sistema continúa intentando montarlo en segundo plano.

```
/usr/games:
dev = /usr/games
mount = true
vfs = nfs
nodename = gameserver
options = ro,soft,bg
type = nfs_mount
```

Los parámetros siguientes son necesarios para stanzas que pertenecen a montajes NFS:

*Tabla 92. Parámetros necesarios para las stanzas que pertenecen a montajes NFS*

Item	Descripción
dev=nombre_sistema_archivos	Especifica el nombre de vía de acceso del sistema de archivos remoto que se está montando.
mount=[true false]	Si se especifica true, el sistema de archivos NFS se monta cuando arranca el sistema. Si se especifica false, el sistema de archivos NFS no se monta cuando arranca el sistema.
nodename=nombresistpral	Especifica la máquina de sistema principal en la que reside el sistema de archivos remoto.
vfs=nfs	Especifica que el sistema de archivos virtual que se está montando es un sistema de archivos NFS.

Los parámetros siguientes son opcionales para stanzas que pertenecen a montajes NFS:

Item	Descripción
<code>type=nombre_tipo</code>	Define el sistema de archivos que se está montando como parte del grupo de montaje <i>nombre_tipo</i> . Este parámetro se utiliza con el mandato <b>mount -t</b> , que monta grupos de sistemas de archivos especificados al mismo tiempo.
<code>options=opciones</code>	<p>Especifica uno o varios de los siguientes parámetros <i>opciones</i>:</p> <p><b>biods=N</b> Especifica el número máximo de daemons <b>biod</b> a utilizar. El valor predeterminado es siete para NFS versión 2 y cuatro para NFS versión 3 y versión 4.</p> <p><b>bg</b> Especifica que se intente el montaje otra vez en el segundo plano si falla el primer intento de montaje.</p> <p><b>fg</b> Especifica que se intente el montaje otra vez en el primer plano si falla el primer intento de montaje.</p> <p><b>noacl</b> Inhabilita, sólo para este montaje, el soporte de Lista de control de accesos (ACL) proporcionado por sistema de archivos de diario de NFS. Cuando se utiliza entre dos sistemas, NFS soporta las listas de control de accesos. Si se utiliza la opción noacl al montar un sistema de archivos, NFS no utiliza las ACL. El efecto de la opción noacl es igual a lo que sucede cuando un cliente NFS de un sistema monta desde un servidor NFS que no soporta las ACL. Para obtener más información sobre las ACL, consulte el apartado <a href="#">“Soporte de Listas de control de acceso de NFS”</a> en la página 593.</p> <p><b>retry=n</b> Establece el número de veces que se debe intentar el montaje.</p> <p><b>rsize=n</b> Establece el tamaño de almacenamiento intermedio de lectura en el número de bytes especificado por <i>n</i>.</p> <p><b>wsize=n</b> Establece el tamaño de almacenamiento intermedio de grabación en el número de bytes especificado por <i>n</i>.</p>

Item	Descripción
	<p><b>timeo=n</b> Establece el tiempo de espera de NFS en las décimas de segundo especificadas por <i>n</i>. Utilice esta variable para evitar situaciones que se pueden producir en las redes donde la carga de servidor puede provocar un tiempo de respuesta inadecuado.</p> <p><b>retrans=n</b> Establece el número de retransmisiones NFS en el número especificado por <i>n</i>.</p> <p><b>port=n</b> Establece el puerto de servidor en el número especificado por <i>n</i>.</p> <p><b>soft</b> Devuelve un error si el servidor no responde.</p> <p><b>hard</b> Continúa intentando la petición hasta que el servidor responde. <b>Nota:</b> Cuando especifique un montaje hard, es posible que el proceso pueda colgarse mientras espera una respuesta. Para poder interrumpir el proceso y finalizarlo desde el teclado, utilice la variable <b>intr</b> en las variables de montaje.</p> <p><b>intr</b> Permite interrupciones de teclado en montajes fijos (hard).</p> <p><b>ro</b> Establece la variable de sólo lectura.</p>

Item	Descripción
	<p><b>rw</b>        Establece la variable de lectura y grabación. Utilice la variable <b>hard</b> junto con esta variable para evitar condiciones de error que pueden estar en conflicto con aplicaciones si se intenta un montaje <b>soft</b> como de lectura y grabación. Consulte el apartado “Resolución de problemas de NFS” en la página 638 para obtener información sobre los problemas de montajes fijos (<b>hard</b>) y flexibles (<b>soft</b>).</p> <p><b>secure</b>        Especifica que se utilice un protocolo más seguro para las transacciones NFS.</p> <p><b>sec</b>        La opción <b>sec</b> especifica la lista de tipos de seguridad para el montaje NFS. Los tipos disponibles son <b>des</b>, <b>unix</b>, <b>sys</b>, <b>krb5</b>, <b>krb5i</b> y <b>krb5p</b>. Esta opción sólo se aplica a AIX 5.3 o posterior.</p> <p><b>actimeo=n</b>        Amplía el tiempo de vaciado en <i>n</i> segundos para archivos y directorios normales.  <b>Nota:</b> La antememoria de atributo conserva los atributos de archivo en el cliente. A los atributos para un archivo se les asigna un tiempo para borrarlos. Si el archivo se modifica antes del tiempo de vaciado, se amplía dicho tiempo en la cantidad de tiempo transcurrido desde la modificación anterior (bajo la suposición que es probable que los archivos que se han cambiado recientemente cambien otra vez pronto). Hay extensiones de tiempo de vaciado mínimas y máximas para los archivos normales y para los directorios.</p> <p><b>vers</b>        Especifica la versión de NFS. El valor predeterminado es la versión del protocolo NFS utilizado entre el cliente y el servidor y es la más alta disponible en ambos sistemas. Si el servidor NFS no soporta NFS Versión 3, el montaje de NFS utilizará NFS Versión 2. Utilice la opción <b>vers</b> para seleccionar la versión de NFS. De forma predeterminada, el montaje de NFS no utilizará nunca NFS Versión 4 a menos que se especifique.</p> <p><b>acregmin=n</b>        Mantiene los atributos en antememoria durante un mínimo de <i>n</i> segundos después de la modificación de archivo.</p> <p><b>acregmax=n</b>        Mantiene los atributos en antememoria durante un tiempo que no supere <i>n</i> segundos después de la modificación de archivo.</p> <p><b>acdirmmin=n</b>        Mantiene los atributos en antememoria durante un mínimo de <i>n</i> segundos después de la actualización de directorio.</p> <p><b>acdirmmax=n</b>        Mantiene los atributos en antememoria durante un tiempo que no supere <i>n</i> segundos después de la actualización de directorio.</p>

Item	Descripción
	<p><b>cio</b>        Especifica el sistema de archivos que se debe montar para lectores y grabadores simultáneos. La E/S en archivos de este sistema de archivos se comportará como si éstos se hubieran abierto especificando <code>O_CIO</code> en la llamada de sistema <code>open()</code>. La utilización de esta opción evitirá el acceso de cualquier modo distinto de CIO. Es imposible utilizar E/S en antememoria en un sistema de archivos montado con la opción <code>cio</code>. Esto significa que los mandatos de correlación tales como <code>mmap()</code> y <code>shmat()</code> fallarán con <code>EINVAL</code> cuando se utilicen en cualquier archivo de un sistema de archivos montado con la opción <code>cio</code>. Un efecto secundario de esto es que es imposible ejecutar binarios fuera de un sistema de archivos montado con <code>cio</code>, porque es posible que el cargador utilice <code>mmap()</code>.</p> <p><b>dio</b>        Especifica que la E/S del sistema de archivos se comportará como si todos los archivos se hubieran abierto especificando <code>O_DIRECT</code> en la llamada de sistema <code>open()</code>.</p> <p><b>Nota:</b> La utilización de los distintivos <code>-dio</code> o bien <code>-ocio</code> puede ayudar al rendimiento en determinadas cargas de trabajo, pero los usuarios deben estar al corriente de que la utilización de estos distintivos impedirán el almacenamiento en antememoria de archivos para estos sistemas de archivos. Dado que la lectura avanzada está inhabilitada para estos sistemas de archivos, esto puede reducir el rendimiento para lecturas secuenciales extensas.</p> <p><b>maxpout=n</b>        Especifica el nivel de salida de página para archivos de este sistema de archivos en el que se deben conservar hebras. Si se especifica <b>maxpout</b>, también debe especificar <b>minpout</b>. Este valor no debe ser negativo y mayor que <b>minpout</b>. El valor predeterminado es el nivel <b>maxpout</b> de kernel.</p> <p><b>minpout=n</b>        Especifica el nivel de salida de página para archivos de este sistema de archivos en el que las hebras deben estar listas. Si se especifica <b>minpout</b>, también debe especificar <b>maxpout</b>. Este valor no debe ser negativo. El valor predeterminado es el nivel <b>minpout</b> de kernel.</p> <p><b>rbr</b>        Utiliza la posibilidad de liberar hacia atrás al leer. Cuando se detecta la lectura secuencial de un archivo de este sistema de archivos, las páginas de memoria reales utilizadas por el archivo se liberan una vez que las páginas se han copiado en almacenamientos intermedios internos.</p>

Item	Descripción
	<p><b>Nota:</b> Si no establece las opciones siguientes, el kernel las establece automáticamente en estos valores predeterminados:</p> <pre data-bbox="719 291 894 587">fg retry=10000 rsize=8192 wsize=8192 timeo=7 retrans=5 port=NFS_PORT hard secure=off acregmin=3 acregmax=60 acdirmmin=30 acdirmmax=60</pre>

- c) Elimine las entradas de directorio que no desee montar automáticamente en el arranque del sistema.
- d) Guarde el archivo y ciérrelo.
- e) Ejecute el mandato **mount -a** para montar todos los directorios especificados en el archivo /etc/filesystems.

## Desmontaje de un sistema de archivos montado explícita o automáticamente

Se puede utilizar el procedimiento siguiente para desmontar un directorio NFS montado explícita o automáticamente.

Para desmontar un directorio NFS montado de forma explícita o automática, escriba:

```
umount /directory/to/unmount
```

## Eliminación de montajes NFS predefinidos

Puede eliminar un montaje NFS predefinido utilizando los procedimientos siguientes.

- Para eliminar un montaje NFS predefinido mediante SMIT:

1. Escriba:

```
smit rmnfsmnt
```

- Para eliminar un montaje NFS predefinido editando el archivo /etc/filesystems:

1. Entre el mandato: umount /directory/to/unmount.
2. Abra el archivo /etc/filesystems con el editor que prefiera.
3. Busque la entrada para el directorio que acaba de desmontar y, a continuación, suprímala.
4. Guarde el archivo y ciérrelo.

## PC-NFS

PC-NFS es un programa para sistemas personales que permite al sistema personal montar sistemas de archivos exportados por un servidor NFS (Network File System).

El sistema personal también puede solicitar direcciones de red y nombres de sistema principal del servidor NFS. Adicionalmente, si el servidor NFS está ejecutando el daemon **rpc.pcnfsd**, el sistema personal puede acceder a servicios de autentificación y de spooling de impresión.

Es posible que desee configurar el daemon **rpc.pcnfsd** en lo siguiente:

- Sistemas que realizan servicios de autentificación de usuario
- Sistemas que ofrecen spooling de impresión

- Todos los servidores maestros y esclavos de NIS (Network Information Service).

**Nota:** Dado que normalmente las redes NIS se configuran para que PC-NFS pueda elegir cualquier servidor NIS como servidor predeterminado, es importante que todos los servidores tengan el daemon **rpc.pcnfsd** en ejecución. Si la ejecución de este daemon en todos los servidores NIS no es práctica o si desea limitar las peticiones en un servidor específico, añada un mandato **net pcnfsd** en el archivo autoexec.bat de cada sistema personal para forzarle a utilizar un servidor NIS específico.

### Información relacionada

[Network Information Services \(NIS\)](#)

### Servicio de autentificación PC-NFS

De forma predeterminada, PC-NFS se presenta a sí mismo a los servidores NFS como el usuario nobody. Con los privilegios nobody, todos los archivos de usuario de sistema personales aparecen como propiedad de nobody y, en consecuencia, no se puede distinguir entre diferentes usuarios de sistemas personales.

La posibilidad de autentificación del daemon **rpc.pcnfsd** le permite supervisar los recursos del sistema y la seguridad reconociendo usuarios individuales y asignándoles diferentes privilegios.

Con el daemon **rpc.pcnfsd** en ejecución, un usuario de PC-NFS puede emitir el mandato **net name** desde un sistema personal para iniciar la sesión en PC-NFS del mismo modo que un usuario puede iniciar la sesión en este sistema operativo. El daemon **rpc.pcnfsd** verifica el nombre de usuario y la contraseña. Este procedimiento de autentificación no hace que un servidor sea más seguro, pero proporciona más control sobre el acceso a los archivos que están disponibles mediante NFS.

### Servicio de spooling de impresión de PC-NFS

El servicio de spooling de impresión del daemon **rpc.pcnfsd** permite a los sistemas personales que ejecutan PC-NFS imprimir en impresoras que no están directamente conectadas al sistema personal.

Especificamente, PC-NFS redirige archivos destinados a impresoras de sistema personal a un archivo de un servidor NFS. Este archivo se coloca en un directorio de spool del servidor NFS. Entonces el daemon **rpc.pcnfsd** invoca el recurso de impresión de servidor. (El directorio de spooling debe estar en un sistema de archivos exportado para que los clientes PC-NFS puedan montarlo.) Cuando PC-NFS solicita que el daemon **rpc.pcnfsd** imprima el archivo, proporciona la información siguiente:

- Nombre del archivo que se debe imprimir
- ID de inicio de sesión del usuario del cliente
- Nombre de la impresora que se debe utilizar.

### Configuración del daemon rpc.pcnfsd

Para obtener el mejor rendimiento, configure el daemon **rpc.pcnfsd** utilizando estos pasos.

Para configurar el daemon **rpc.pcnfsd**:

1. Instale el programa PC-NFS en el sistema personal.

2. Seleccione una ubicación para el directorio de spool en el servidor NFS.

El directorio de spool predeterminado es /var/tmp. El directorio de spool debe tener como mínimo 100 K bytes de espacio libre.

3. Exporte el directorio de spool. En el directorio exportado no ponga restricciones de acceso que puedan causar problemas de acceso en la red.

Para obtener detalles de este procedimiento, consulte el apartado [“Exportación de un sistema de archivos NFS” en la página 617](#).

4. Inicie el daemon **rpc.pcnfsd** siguiendo las instrucciones del apartado [“Inicio del daemon rpc.pcnfsd” en la página 633](#).

5. Verifique que el daemon **rpc.pcnfsd** esté accesible siguiendo las instrucciones del apartado [“Verificación de que el daemon rpc.pcnfsd es accesible” en la página 633](#).

**Nota:** Dado que a veces las peticiones de redirección de impresora hacen que los listados de archivos de longitud cero se dejen en los directorios de spool de PC-NFS, borre periódicamente los directorios de spooling de estas entradas.

### Inicio del daemon **rpc.pcnfsd**

Para iniciar el daemon **rpc.pcnfsd** utilizando el directorio de spooling predeterminado, utilice el siguiente procedimiento.

1. Con un editor de texto, elimine la marca de comentario de la siguiente entrada en el archivo `/etc/inetd.conf`:

```
pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
```

2. Guarde el archivo y salga del editor de texto.

Para iniciar el daemon **rpc.pcnfsd** utilizando un directorio que es diferente del valor predeterminado:

1. Utilice un editor de texto para añadir la entrada siguiente en el archivo `/etc/rc.nfs`:

```
if [ -f /usr/sbin/rpc.pcnfsd ] ; then  
/usr/sbin/rpc.pcnfsd -s dirspool ; echo ' rpc.pcnfsd\c'  
fi
```

donde *dirspool* especifica el nombre de vía de acceso completa del directorio de spool.

2. Guarde el archivo y salga del editor de texto.

3. Utilizando un editor de texto, comente la entrada siguiente en el archivo `/etc/inetd.conf`:

```
#pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
```

Si pone un signo de almohadilla (#) al principio de la línea evitara que el daemon **inetd** inicie el daemon **rpc.pcnfsd** utilizando el directorio de spool predeterminado.

4. Inicie el spoller de impresión del daemon **rpc.pcnfsd** escribiendo lo siguiente en la línea de mandatos:

```
/usr/sbin/rpc.pcnfsd -s dirspool
```

donde *dirspool* especifica el nombre de vía de acceso completa del directorio de spool.

Para obtener más información sobre cómo actualizar la base de datos de configuración **inetd**, consulte el apartado “[Configuración del daemon inetd](#)” en la página 431.

**Nota:** El directorio predeterminado que el daemon **rpc.pcnfsd** utiliza no se puede cambiar desde el archivo `inetd.conf`.

### Verificación de que el daemon **rpc.pcnfsd** es accesible

Siga este procedimiento para determinar si el daemon **rpc.pcnfsd** es accesible.

Para verificar que el daemon **rpc.pcnfsd** es accesible, escriba:

```
rpcinfo -u sistpral 150001
```

donde *sistpral* especifica que el nombre de sistema principal del sistema en el que está configurando **rpc.pcnfsd** y 15001 es el número de programa RPC del daemon **rpc.pcnfsd**. Después de entrar el mandato, recibirá un mensaje que indica que el programa está preparado y esperando.

## Correlaciones de montaje automático de LDAP

Puede configurar el subsistema de montaje automático para recuperar las correlaciones de un servidor LDAP.

Para administrar correlaciones de montaje automático en LDAP, añada la línea siguiente al archivo /etc/irs.conf:

```
automount nis_ldap
```

Para administrar las correlaciones de montaje automático en LDAP, necesita crear los archivos LDIF apropiados. Puede convertir archivos de correlación de montaje automático locales a formato LDIF utilizando el mandato **nistoldif**. Por ejemplo, si el servidor LDAP se denomina ldapserver, el sufijo base es dc=suffix y el archivo de correlación /etc/auto\_home contiene las líneas siguientes:

```
user1      server1:/home/user1
user2      server1:/home/user2
user3      server1:/home/user3
```

Utilice los mandatos siguientes para crear el archivo LDIF para el archivo de correlación /etc/auto\_home y añadirlo al servidor LDAP:

```
nistoldif -d dc=suffix -sa -f /etc/auto_home > /tmp/auto_home.ldif
ldapadd -D cn=admin -w passwd -h ldapserver -f /tmp/auto_home.ldif
```

Para editar o eliminar entradas de montaje automático existentes de un servidor LDAP, los archivos LDIF se deben crear manualmente. Por ejemplo, si el directorio inicial de user2 está ahora en server2, se deberá crear el siguiente LDIF:

```
# cat /tmp/ch_user2.ldif
dn: automountKey=user2,automountMapName=auto_home,dc=suffix
changetype: modify
replace: automountInformation
automountInformation: server2:/home/user2
```

Después de crear el LDIF anterior, ejecute el mandato siguiente:

```
ldapmodify -D cn=admin -w passwd -h ldapserver -f /tmp/ch_user2.ldif
```

También debe crear un archivo LDIF para eliminar un usuario. Por ejemplo, para eliminar user3, cree el siguiente LDIF:

```
# cat /tmp/rm_user3.ldif
dn: automountKey=user3,automountMapName=auto_home,dc=suffix
changetype: delete
```

Después de crear el LDIF anterior, ejecute el mandato siguiente:

```
ldapmodify -D cn=admin -w passwd -h ldapserver -f /tmp/rm_user3.ldif
```

## WebNFS

El sistema operativo proporciona la posibilidad de servidor NFS para WebNFS.

WebNFS, definido por Oracle, es una extensión simple del protocolo NFS que permite el acceso más fácil a los servidores y clientes a través de los cortafuegos de Internet.

Un navegador web mejorado con WebNFS puede utilizar un localizador universal de recursos (URL) NFS para acceder a los datos directamente desde el servidor. Un ejemplo de URL NFS es:

```
nfs://www.SuEmpresa.com/
```

WebNFS funciona en tandem con protocolos basados en web existentes para proporcionar datos a los clientes.

WebNFS también aprovecha la escalabilidad de los servidores NFS.

## Gestor de bloqueos de red

El gestor de bloqueos de red es un recurso que funciona en cooperación con NFS (Network File System) para proporcionar un estilo de System V de bloqueo de archivos y registros de aviso a través de la red.

El gestor de bloqueos de red (**rpc.lockd**) y el supervisor de estado de red (**rpc.statd**) son daemons de servicio de red. El daemon **rpc.statd** es un proceso de nivel de usuario mientras que el daemon **rpc.lockd** se implementa como un conjunto de hebras de kernel (similar al servidor NFS). Ambos daemons son esenciales para que el kernel pueda proporcionar servicios de red fundamentales.

### Nota:

1. Los bloqueos obligatorios o forzados no se soportan en NFS.
2. El gestor de bloqueos de red es específico de NFS Versión 2 y Versión 3.

### Arquitectura de gestor de bloqueos de red

El gestor de bloqueos de red contiene funciones de servidor y cliente.

Las funciones de cliente son responsables de procesar peticiones de las aplicaciones y de enviar peticiones al gestor de bloqueos de red en el servidor. Las funciones de servidor son responsables de aceptar las peticiones de bloqueo de los clientes y de generar las llamadas de bloqueo apropiadas en el servidor. Entonces el servidor responderá a la petición de bloqueo del cliente.

A diferencia de NFS, que no tiene estado, el gestor de bloqueos de red tiene un estado implícito. En otras palabras, el gestor de bloqueos de red debe recordar si el cliente tiene un bloqueo actualmente. El supervisor de estado de red, **rpc.statd**, implementa un protocolo simple que permite al gestor de bloqueos de red supervisar el estado de otras máquinas de la red. Al tener información de estado precisa, el gestor de bloqueos de red puede mantener un estado coherente en el entorno de NFS sin estado.

### Proceso de bloqueo de archivos de red

Cuando una aplicación desea obtener un bloqueo en un archivo local, envía la petición al kernel utilizando las subrutinas **lockf**, **fcntl** o **flock**.

Entonces el kernel procesa la petición de bloqueo. Sin embargo, si una aplicación de un cliente NFS realiza una petición de bloqueo para un archivo remoto, el cliente de Gestor de bloqueos de red genera una Llamada a procedimiento remoto (RPC) al servidor para manejar la petición.

Cuando el cliente recibe una petición de bloqueo remota inicial, registra el interés en el servidor con el daemon **rpc.statd** del cliente. Lo mismo es cierto para el gestor de bloqueos de red en el servidor. En la petición inicial de un cliente, registra el interés en el cliente con el supervisor de estado de red local.

### Proceso de recuperación de detención anormal

El daemon **rpc.statd** de cada máquina informa de sus actividades al daemon **rpc.statd** de todas las demás máquinas. Cuando el daemon **rpc.statd** recibe el aviso de que otra máquina se ha detenido anormalmente o se ha recuperado, informa al daemon **rpc.lockd**.

Si un servidor se detiene anormalmente, los clientes con archivos bloqueados deben poder recuperar los bloqueos. Si un cliente se detiene anormalmente, los servidores deben mantener los bloqueos de cliente mientras él se recupera. Adicionalmente, para conservar la transparencia general de NFS, la recuperación de la detención anormal debe producirse sin necesitar la intervención de las propias aplicaciones.

El procedimiento de recuperación de detención anormal es simple. Si se detecta la anomalía de un cliente, el servidor libera los bloqueos del cliente anómalo suponiendo que la aplicación cliente solicitará los bloqueos otra vez cuando sean necesarios. Si se detecta la detención anormal y la recuperación de un servidor, el gestor de bloqueos de cliente vuelve a transmitir todas las peticiones de bloqueo otorgadas anteriormente por el servidor. El servidor utiliza esta información retransmitida para reconstruir el estado de bloqueo durante un periodo de gracia. (El periodo de gracia, 45 segundos de forma predeterminada, es un periodo de tiempo dentro del cual un servidor permite a los clientes reclamar los bloqueos).

El daemon **rpc.statd** utiliza los nombres de sistema principal mantenidos en **/var/statmon/sm** y **/var/statmon/sm.bak** para hacer el seguimiento de los sistemas principales a los que se debe informar cuando la máquina necesita recuperar operaciones.

## **Inicio del gestor de bloqueos de red**

De forma predeterminada, el script /etc/rc.nfs inicia los daemons **rpc.lockd** y **rpc.statd** junto con los demás daemons de NFS.

Si NFS ya está en ejecución, puede verificar que los daemons **rpc.lockd** y **rpc.statd** se estén ejecutando siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS en la página 603](#)”. El estado de estos dos daemons debe ser *activo*. Si los daemons **rpc.lockd** y **rpc.statd** no están activos y, por consiguiente, no están en ejecución, realice lo siguiente:

1. Utilizando el editor de texto que prefiera, abra el archivo /etc/rc.nfs.
2. Busque las líneas siguientes:

```
if [ -x /usr/sbin/rpc.statd ]; then
    startsrc -s rpc.statd
fi
if [ -x /usr/sbin/rpc.lockd ]; then
    startsrc -s rpc.lockd
fi
```

3. Si hay un signo de almohadilla (#) al principio de cualquiera de estas líneas, suprima el carácter y, a continuación, guarde el archivo y salga del mismo. A continuación, inicie los daemons **rpc.statd** y **rpc.lockd** siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.

**Nota:** La secuencia es importante. Inicie siempre el daemon **statd** en primer lugar.

4. Si NFS está en ejecución y las entradas del archivo /etc/rc.nfs son correctas, detenga y reinicie los daemons **rpc.statd** y **rpc.lockd** siguiendo las instrucciones del apartado “[Detención de los daemons NFS](#)” en la página 603 y del apartado “[Inicio de los daemons NFS](#)” en la página 603.

**Nota:** La secuencia es importante. Inicie siempre el daemon **statd** en primer lugar.

Si los daemons **rpc.statd** y **rpc.lockd** aún no se están ejecutando, consulte el apartado “[Resolución de problemas del gestor de bloqueos de red](#)” en la página 636.

## **Resolución de problemas del gestor de bloqueos de red**

Algunos problemas del gestor de bloqueos de red que se encuentran se pueden resolver siguiendo los siguientes consejos.

Si en un cliente recibe un mensaje similar a:

```
clnttcp_create: RPC: Error de sistema remoto - Conexión rechazada
rpc.statd: no se puede hablar con statd en {servidor}
```

la máquina considera que hay otra máquina que necesita que se le informe de que puede tener que tomar medidas de recuperación. Cuando una máquina se reinicia o cuando los daemons **rpc.lockd** y **rpc.statd** se detienen y se reinician, los nombres de máquina se mueven de /var/statmon/sm a /var/statmon/sm.bak y el daemon **rpc.statd** intenta informar a cada máquina correspondiente a cada entrada de /var/statmon/sm.bak que se necesitan procedimientos de recuperación.

Si el daemon **rpc.statd** puede alcanzar la máquina, se elimina la entrada en /var/statmon/sm.bak. Si el daemon **rpc.statd** no puede alcanzar la máquina, seguirá intentándolo a intervalos regulares. Cada vez que la máquina no pueda responder, el tiempo de espera excedido genera el mensaje anterior. En beneficio de la integridad de bloqueo, el daemon continuará intentándolo; sin embargo, esto puede tener un efecto adverso para el rendimiento de bloqueo. El manejo es diferente, en función de si la máquina de destino es simplemente indiferente o está fuera de producción de forma semipermanente. Para eliminar este mensaje:

1. Verifique que los daemons **statd** y **lockd** del servidor se están ejecutando siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS](#)” en la página 603. (El estado de estos dos daemons debe ser *activo*).
2. Si estos daemons no están en ejecución, inicie los daemons **rpc.statd** y **rpc.lockd** en el servidor siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.

**Nota:** La secuencia es importante. Inicie siempre el daemon **statd** en primer lugar.

Después de haber reiniciado los daemons, recuerde que hay un periodo de gracia. Durante este tiempo, dado que los daemons **lockd** permiten que lleguen peticiones de reclamación de otros clientes que anteriormente han mantenido bloqueos con el servidor, es posible que no obtenga un nuevo bloqueo inmediatamente después de iniciar los daemons.

Alternativamente, elimine el mensaje realizando lo siguiente:

1. Detenga los daemons **rpc.statd** y **rpc.lockd** en el cliente siguiendo las instrucciones del apartado “[Detención de los daemons NFS](#)” en la página 603.
2. En el cliente, elimine la entrada de máquina de destino del archivo `/var/statmon/sm.bak` especificando:

```
rm /var/statmon/sm.bak/NombreMáquinaDestino
```

Esta acción impide que la máquina de destino esté al corriente de que puede necesitar participar en la recuperación de bloqueo. Sólo se deberá utilizar cuando se pueda determinar que la máquina no tiene aplicaciones en ejecución que participan en el bloqueo de red con la máquina afectada.

3. Inicie los daemons **rpc.statd** y **rpc.lockd** en el cliente siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.

Si no puede obtener un bloqueo de un cliente, realice lo siguiente:

1. Utilice el mandato **ping** para verificar que el cliente y el servidor se pueden alcanzar y reconocer entre ellos. Si las máquinas están ambas en ejecución y la red está intacta, compruebe los nombres de sistema principal listados en el archivo `/var/statmon/hosts` para cada máquina. Los nombres de sistema principal deben coincidir exactamente entre el servidor y cliente para el reconocimiento de máquina. Si se está utilizando un servidor de nombres para la resolución de nombres de sistema principal, asegúrese de que la información de sistema principal es exactamente igual que la del archivo `/var/statmon/hosts`.
2. Verifique que los daemons **rpc.lockd** y **rpc.statd** estén en ejecución en el cliente y el servidor siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS](#)” en la página 603. El estado de estos dos daemons debe ser *activo*.
3. Si no están activos, inicie los daemons **rpc.statd** y **rpc.lockd** siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.
4. Si están activos, es posible que necesite restablecerlos en los clientes y los servidores. Para ello, detenga todas las aplicaciones que están solicitando bloqueos.
5. A continuación, detenga los daemons **rpc.statd** y **rpc.lockd** en el cliente y el servidor siguiendo las instrucciones del apartado “[Detención de los daemons NFS](#)” en la página 603.
6. A continuación, reinicie los daemons **rpc.statd** y **rpc.lockd**, primero en el servidor y, a continuación, en el cliente, siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.

**Nota:** La secuencia es importante. Inicie siempre el daemon **statd** en primer lugar.

Si el procedimiento no soluciona el problema de bloqueo, ejecute el daemon **lockd** en modalidad de depuración, realizando lo siguiente:

1. Detenga los daemons **rpc.statd** y **rpc.lockd** en el cliente y el servidor siguiendo las instrucciones del apartado “[Detención de los daemons NFS](#)” en la página 603.
2. Inicie el daemon **rpc.statd** en el cliente y el servidor siguiendo las instrucciones del apartado “[Inicio de los daemons NFS](#)” en la página 603.
3. Inicie el daemon **rpc.lockd** en el cliente y el servidor escribiendo:

```
/usr/sbin/rpc.lockd -d1
```

Cuando se invoca con el distintivo **-d1**, el daemon **lockd** proporciona mensajes de diagnóstico en syslog. Al principio, habrá varios mensajes que traten del periodo de gracia; espere a que exceda el tiempo de espera de los mismos. Cuando haya excedido el tiempo de espera del periodo de gracia en

el servidor y los clientes, ejecute la aplicación que está teniendo problemas de bloqueo y verifique que se transmite una petición de bloqueo del cliente al servidor y del servidor al cliente.

Puede restringir el rango de números de puertos IP utilizados por el cliente NFS para las comunicaciones con el servidor NFS estableciendo la variable NFS\_PORT\_RANGE en el archivo /var/statmon/environment.

### Rangos de puerto NFS

Se puede utilizar la variable de entorno NFS\_PORT\_RANGE para limitar el puerto de origen de las llamadas de red que el cliente realiza al servidor.

Si se utiliza, esta variable de entorno se debe añadir al archivo /etc/environment. El formato de la variable de entorno es el siguiente:

```
NFS_PORT_RANGE=udp[4000-5000]:tcp[7000-8000]
```

En este ejemplo, los paquetes UDP enviados por el cliente tendrán un puerto de origen en el rango de 4000 a 5000 y las conexiones TCP tendrán un puerto de origen en el rango de 7000 a 8000. Para evitar problemas de reutilización de puertos, los números de puerto que se especifican en este rango no se pueden utilizar como números de puerto corregidos para cualquier daemon de NFS (Network File System) en el archivo /etc/services.

## Seguridad de NFS

Se puede encontrar información sobre la seguridad de NFS en varios lugares.

El tema Seguridad de Network File System de Security explica los detalles sobre la seguridad de DES.

Para obtener información sobre la seguridad de Kerberos, consulte el apartado “Configuración de una red para RPCSEC-GSS” en la página 618.

## Resolución de problemas de NFS

Como sucede con otros servicios de red, se pueden producir problemas en máquinas que utilizan NFS (Network File System - Sistema de archivos de red). Para resolver estos problemas es necesario conocer las estrategias para realizar el seguimiento de problemas NFS, reconocer los mensajes de error relacionados con NFS y seleccionar las soluciones apropiadas.

Al hacer el seguimiento de un problema de NFS, aísle cada uno de los tres puntos principales de anomalía para determinar cuál de ellos no funciona: el servidor, el cliente o la propia red.

**Nota:** Consulte el apartado “Resolución de problemas del gestor de bloqueos de red” en la página 636 para ver los problemas de bloqueo de archivo.

### Problemas de archivo de montaje fijo y de montaje flexible

Cuando la red o el servidor tiene problemas, los programas que acceden a archivos remotos de montaje fijo fallan de un modo diferente de los que acceden a archivos remotos de montaje flexible.

Si un servidor no puede responder a una petición de montaje fijo, NFS imprime el mensaje:

```
El servidor NFS nombresistpral no responde, se sigue intentando
```

Los sistemas de archivos remotos de montaje fijo hacen que los programas se cuelguen hasta que el servidor responde porque el cliente reintenta la petición de montaje hasta que la realiza satisfactoriamente. Utilice el distintivo **-bg** con el mandato **mount** al realizar un montaje fijo de modo que, si el servidor no responde, el cliente reintente el montaje en segundo plano.

Si un servidor no puede responder a una petición de montaje flexible, NFS imprime el mensaje:

```
Tiempo excedido de conexión
```

Los sistemas de archivos remotos de montaje flexible devuelven un error después de intentarlo sin éxito durante un periodo de tiempo. Desafortunadamente, dado que muchos programas no comprueban las condiciones de retorno en las operaciones de sistema de archivos, no verá este mensaje de error al acceder a archivos de montaje flexible. Sin embargo, este mensaje de error NFS se imprime en la consola.

## Identificación de problemas de NFS

Si tiene problemas de NFS, siga estos pasos.

Si un cliente tiene problemas de NFS, realice lo siguiente:

1. Verifique que las conexiones de red sean correctas.
2. Verifique que los daemons **inetd**, **portmap** y **biod** se están ejecutando en el cliente, siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS](#)” en la página 603.
3. Verifique que existe un punto de montaje válido para el sistema de archivos que se está montando. Para obtener más información, consulte el apartado “[Configuración de un cliente NFS](#)” en la página 616.
4. Verifique que el servidor esté activo y en ejecución ejecutando el siguiente mandato en el indicador de shell del cliente:

```
/usr/bin/rpcinfo -p nombre_servidor
```

Si el servidor está activo, se imprime una lista de programas, versiones y números de puerto similar la siguiente:

programa	vers	proto	puerto	servicio
100000	2	tcp	111	portmapper
100000	2	udp	111	portmapper
100005	1	udp	1025	mountd
100001	1	udp	1030	rstated
100001	2	udp	1030	rstated
100001	3	udp	1030	rstated
100002	1	udp	1036	rusersd
100002	2	udp	1036	rusersd
100008	1	udp	1040	walld
100012	1	udp	1043	sprayd
100005	1	tcp	694	mountd
100003	2	udp	2049	nfs
100024	1	udp	713	status
100024	1	tcp	715	status
100021	1	tcp	716	nlockmgr
100021	1	udp	718	nlockmgr
100021	3	tcp	721	nlockmgr
100021	3	udp	723	nlockmgr
100020	1	udp	726	llockmgr
100020	1	tcp	728	llockmgr
100021	2	tcp	731	nlockmgr

Si no se devuelve una respuesta similar, inicie la sesión en el servidor en la consola de servidor y compruebe el estado del daemon **inetd** siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS](#)” en la página 603.

5. Verifique que los daemons **mountd**, **portmap** y **nfsd** estén en ejecución en el servidor NFS entrando los mandatos siguientes en el indicador de shell de cliente:

```
/usr/bin/rpcinfo -u nombre_servidor mount  
/usr/bin/rpcinfo -u nombre_servidor portmap  
/usr/bin/rpcinfo -u nombre_servidor nfs
```

Si los daemons se ejecutan en el servidor, se devuelven las respuestas siguientes:

programa	versión	versión	versión	versión
100005	1	2	2	2
100000	2	2	2	2
100003	2	2	2	2

Los números de programa corresponden a los mandatos, respectivamente, como se muestran en el ejemplo anterior. Si no se devuelve una respuesta similar, inicie la sesión en el servidor en la consola de servidor y compruebe el estado de los daemons siguiendo las instrucciones del apartado “[Obtención del estado actual de los daemons NFS](#)” en la página 603.

6. Verifique que el archivo **/etc/exports** del servidor liste el nombre del sistema de archivos que el cliente desea montar y que se exporte el sistema de archivos. Para ello, entre el mandato:

```
showmount -e nombre_servidor
```

Este mandato lista todos los sistemas de archivos actualmente exportados por *nombre\_servidor*.

7. Para NFS versión 4, verifique que el dominio NFSv4 esté establecido correctamente.
8. Para NFS versión 4, verifique que el daemon **nfsrgyd** esté en ejecución.
9. Si está utilizando la seguridad mejorada, consulte el apartado “[Determinación de problemas de RPCSEC-GSS](#)” en la página 645.

### Errores de grabación asíncrona

Cuando un programa de aplicación graba datos en un archivo de un sistema de archivos montado mediante NFS, el daemon **biod** planifica la operación de grabación para el proceso asíncrono.

Si se produce un error en el servidor NFS al mismo tiempo que los datos se están grabando realmente en el disco, se devuelve el error al cliente NFS y el daemon **biod** guarda el error internamente en las estructuras de datos de NFS. El error almacenado se devuelve subsiguentemente al programa de aplicación la siguiente vez que llama a las funciones `fsync` o `close`. Como consecuencia de tales errores, no se informa a la aplicación del error de grabación hasta que el programa cierra el archivo. Por ejemplo, este suceso se produce típicamente cuando un sistema de archivos del servidor está lleno, haciendo que fallen las grabaciones intentadas por un cliente.

### Mensaje de error nfs\_server

Cuando el almacenamiento intermedio de transmisión es demasiado pequeño, se devuelve un mensaje de error.

Si los almacenamientos intermedios de transmisión de la red son insuficientes, se emitirá el siguiente mensaje de error:

```
nfs_server: bad sendreply
```

Para aumentar los almacenamientos intermedios de transmisión, utilice la vía de acceso rápida System Management Interface Tool (SMIT) `smit commodev`. A continuación, seleccione el tipo de adaptador y aumente el número de almacenamientos intermedios de transmisión.

### Mensajes de error de mount

Un proceso de montaje remoto puede fallar de varias formas. Aquí se describen los mensajes de error asociados con anomalías de montaje.

#### **mount: ... ya montado**

El sistema de archivos que está intentando montar ya está montado.

#### **mount: ... no encontrado en /etc/filesystems**

El nombre de directorio o sistema de archivos especificado no se puede comparar.

Si emite el mandato **mount** con un nombre de directorio o de sistema de archivos pero no ambos, el mandato busca en el archivo `/etc/filesystems` una entrada cuyo campo de directorio o sistema de archivos coincide con el argumento. Si el mandato **mount** encuentra una entrada como la siguiente:

```
/dancer.srcl
  dev=/usr/src
  nodename = d61server
  type    = nfs
  mount   = false
```

realiza el montaje como si se hubiera entrado lo siguiente en la línea de mandatos:

```
/usr/sbin/mount -n dancer -o rw,hard /usr/src /dancer.srcl
```

#### **... no está en la base de datos de sistemas principales**

En una red sin NIS (Network Information Service), este mensaje indica que el sistema principal especificado en el mandato **mount** no está en el archivo `/etc/hosts`. En una red que ejecuta NIS, el mensaje indica que NIS no ha podido encontrar el nombre de sistema principal en la base de datos `/etc/hosts` o que el daemon **ypbind** de NIS de la máquina se ha cancelado. Si el archivo `/etc/resolv.conf` existe de forma que el servidor de nombres se está utilizando para la

resolución de nombres de sistema principal, es posible que haya un problema en la base de datos **named**. Consulte el apartado “Resolución de nombres de sistema principal en un servidor NFS” en la página 644.

Compruebe la ortografía y la sintaxis del mandato **mount**. Si el mandato es correcto, la red no ejecuta NIS y sólo obtiene este mensaje para este nombre de sistema principal, compruebe la entrada en el archivo /etc/hosts.

Si la red ejecuta NIS, asegúrese de que el daemon **ypbind** se ejecuta entrando lo siguiente en la línea de mandatos:

```
ps -ef
```

Deberá ver el daemon **ypbind** en la lista. Intente utilizar el mandato **rlogin** para iniciar la sesión de forma remota en otra máquina o utilice el mandato **rcp** para copiar de forma remota algo en otra máquina. Si esto también falla, probablemente el daemon **ypbind** se ha detenido o se ha colgado.

Si sólo obtiene este mensaje para este nombre de sistema principal, compruebe la entrada /etc/hosts en el servidor NIS.

**mount: ... el servidor no está respondiendo: anomalía en correlacionador de puertos - RPC ha excedido el tiempo de espera**

El servidor desde el que está intentando realizar el montaje está inactivo o el correlacionador de puertos se ha detenido o se ha colgado. Intente reiniciar el servidor para activar los daemons **inetd**, **portmap** y **ypbind**.

Si no puede iniciar la sesión en el servidor de forma remota con el mandato **rlogin** pero el servidor está activo, compruebe la conexión de red intentando iniciar la sesión de forma remota en alguna otra máquina. Compruebe también la conexión de red del servidor.

**mount: ... el servidor no está respondiendo: programa no registrado**

Esto significa que el mandato **mount** ha pasado por el correlacionador de puerto, pero el daemon de montaje NFS **rpc.mountd** no se había registrado.

**mount: acceso rechazado ...**

El nombre de máquina no está en la lista de exportación para el sistema de archivos que está intentando montar desde el servidor.

Puede obtener una lista de los sistemas de archivos exportados de servidor ejecutando el siguiente mandato en la línea de mandatos:

```
showmount -e nombreSistpral
```

Si el sistema de archivos que desea no está en la lista o el nombre de máquina o nombre de grupo de red no está en la lista de usuarios para el sistema de archivos, inicie la sesión en el servidor y consulte en el archivo /etc(exports la entrada de sistema de archivos correcta. Un nombre de sistema de archivos que aparece en el archivo /etc(exports, pero no en la salida del mandato **showmount**, indica una anomalía en el daemon **mountd**. El daemon no ha podido analizar esa línea del archivo, no ha podido encontrar el directorio o el nombre de directorio no era un directorio montado localmente. Si el archivo /etc(exports parece correcto y la red ejecuta NIS, compruebe el daemon **ypbind** en el servidor. Es posible que se haya detenido o colgado.

**mount: ....: Permiso denegado**

Este mensaje es una indicación genérica de que alguna parte de la autentificación ha fallado en el servidor. En el ejemplo anterior, puede ser que no esté en la lista de exportación, el servidor no haya podido reconocer el daemon **ypbind** de máquina o que el servidor no acepte la identidad que ha proporcionado.

Compruebe el archivo /etc(exports del servidor y, si es aplicable, el daemon **ypbind**. En este caso, simplemente puede cambiar el nombre de sistema principal con el mandato **hostname** y volver a intentar el mandato **mount**.

**mount: ...: No es un directorio**

La vía de acceso remota o la vía de acceso local no es un directorio. Compruebe la ortografía del mandato e intente ejecutarlo en ambos directorios.

**mount: ...: No está permitido**

Debe tener autorización de root o ser miembro del grupo de sistema para ejecutar el mandato **mount** en la máquina porque ello afecta al sistema de archivos de todos los usuarios de dicha máquina. Los montajes y desmontajes de NFS sólo están permitidos para usuarios root y miembros del grupo de sistema.

**Información relacionada**

[Network Information Services \(NIS\)](#)

**Causas de tiempos de acceso lentos para NFS**

Si el acceso a archivos remotos parece inusualmente lento, asegúrese de que el tiempo de acceso no está siendo inhibido por un daemon fuera de control, una línea **tty** incorrecta o un problema similar.

**Conexiones de red**

Utilice el mandato **nfsstat** para recopilar información sobre las conexiones de red.

El mandato **nfsstat** determina si se están eliminando paquetes. Utilice los mandatos **nfsstat -c** y **nfsstat -s** para determinar si el cliente o el servidor está retransmitiendo bloques grandes. Las retransmisiones son siempre una posibilidad debido a los paquetes perdidos o los servidores ocupados. Una velocidad de retransmisión de cinco por ciento o más se considera alta.

La probabilidad de retransmisiones se puede reducir cambiando los parámetros de cola de transmisión de adaptador de comunicaciones. Para cambiar estos parámetros se puede utilizar el menú de la SMIT. Para obtener más información, consulte el apartado [Available system management interfaces in Sistema operativo y gestión de dispositivos](#).

Se recomiendan los valores siguientes para los servidores NFS.

**Nota:**

1. Aplique estos valores a los clientes NFS si persisten las retransmisiones.
2. Todos los nodos de una red deben utilizar el mismo tamaño de MTU.

*Tabla 93. Tamaños de Unidad máxima de transmisión (MTU) y de cola de transmisión de adaptador de comunicaciones*

Adaptador	MTU	Cola de transmisión
Red en anillo		
4 Mb	1500 3900	50 40 (Incrementar si el mandato <b>nfsstat</b> excede el tiempo de espera.)
16 Mb	1500 8500	40 (Incrementar si el mandato <b>nfsstat</b> excede el tiempo de espera.) 40 (Incrementar si el mandato <b>nfsstat</b> excede el tiempo de espera.)
Ethernet	1500	40 (Incrementar si el mandato <b>nfsstat</b> excede el tiempo de espera.)

Los tamaños de MTU mayores para cada velocidad de Red en anillo reducen el uso de procesador y mejoran significativamente las operaciones de lectura y grabación.

### **Establecimiento de tamaños de MTU**

Para establecer un tamaño de MTU, utilice la vía rápida de SMIT, `smit chif`.

Seleccione el adaptador apropiado y entre un valor de MTU en el campo Tamaño máximo de paquete IP.

Se puede utilizar el mandato **ifconfig** para establecer el tamaño de MTU (y se *debe* utilizar para establecer el tamaño de MTU en 8500). El formato del mandato **ifconfig** es:

```
ifconfig trn NombreNodo up mtu TamañoMTU
```

donde `trn` es el nombre de adaptador, por ejemplo `tr0`.

Otro método de establecimiento de tamaños de MTU combina el mandato **ifconfig** con SMIT.

1. Añada el mandato **ifconfig** para las redes en anillo, como se muestra en el ejemplo anterior, al archivo `/etc/rc.bsdnet`.
2. Entre la vía de acceso rápida `smit setbootup_option`. Commute el campo **Utilizar estilo BSD** a **sí**.

### **Tamaños de cola de transmisión**

Los tamaños de cola de transmisión de adaptador de comunicaciones se establecen con SMIT.

Entre la vía rápida `smit chgtok`, seleccione el adaptador apropiado y entre un tamaño de cola en el campo de transmisión.

### **Programas colgados**

Si los programas se cuelgan durante el trabajo relacionado con archivos, el servidor NFS se puede haber detenido.

En este caso, es posible que se visualice el siguiente mensaje de error:

```
El servidor NFS nombresistpral no responde, se sigue intentando
```

El servidor NFS (`nombresistpral`) está inactivo. Esto indica un problema con el servidor NFS, la conexión de red o el servidor NIS.

Compruebe los servidores de los que ha montado los sistemas de archivos si la máquina se cuelga por completo. Si uno o varios de ellos está inactivo, no se preocupe. Cuando el servidor vuelva a estar activo, los programas continuarán automáticamente. No se ha destruido ningún archivo.

Si un servidor con un montaje flexible muere, el resto del trabajo no queda afectado. Los programas que exceden el tiempo de espera al intentar acceder a archivos remotos con montajes flexibles fallan con el mensaje `errno`, pero siguen pudiendo acceder a los demás sistemas de archivos.

Si están en ejecución todos los servidores, determine si otros usuarios que utilizan los mismos servidores tienen problemas. Si hay más de una máquina que tiene problemas de servicio, esto indica un problema con los daemons **nfsd** en el servidor. En este caso, inicie la sesión en el servidor y ejecute el mandato **ps** para ver si el daemon **nfsd** está en ejecución y está acumulando tiempo de CPU. En caso negativo, es posible que pueda detener y, a continuación, reiniciar el daemon **nfsd**. Si esto no funciona, tendrá que reiniciar el servidor.

Compruebe la conexión de red y la conexión del servidor si parece que otros sistemas están activos y en ejecución.

### **Permisos y esquemas de autenticación**

A veces, después de que se hayan establecido los montajes satisfactoriamente, hay problemas al leer, grabar o crear archivos o directorios remotos. Dichas dificultades se deben normalmente a los permisos o a problemas de autenticación.

La causa de los problemas de permisos y autenticación puede variar en función de que se esté utilizando NIS y se hayan especificado montajes seguros.

El caso más simple se produce cuando se especifican montajes no seguros y no se utiliza NIS. En este caso, los ID de usuario (UID) y los ID de grupo (GID) se correlacionan solamente mediante el archivo /etc/passwd de servidor y el archivo /etc/group de cliente. En este esquema, para que un usuario denominado B se identifique en el cliente y en el servidor como B, el usuario B debe tener el mismo número de UID en el archivo /etc/passwd. A continuación se muestra un ejemplo de cómo esto puede causar problemas:

```
El usuario B es el uid 200 en el cliente foo.  
El usuario B es el uid 250 en el servidor bar.  
El usuario G es el uid 200 en el servidor bar.
```

El directorio /home/bar se monta desde el servidor bar en el cliente foo. Si el usuario B está editando archivos en el sistema de archivos remotos /home/bar en el cliente foo, se produce confusión cuando guarda los archivos.

El servidor bar cree que los archivos pertenecen al usuario G, porque G es el UID 200 en bar. Si B inicia la sesión directamente en bar utilizando el mandato **rlogin**, es posible que no pueda acceder a los archivos que acaba de crear mientras trabaja en el sistema de archivos montado de forma remota. Sin embargo, G puede hacerlo porque las máquinas arbitran los permisos por UID, no por nombre.

La única solución permanente para esto es reasignar los UID coherentes en las dos máquinas. Por ejemplo, proporcione a B el UID 200 en el servidor bar o 250 en el cliente foo. Los archivos que son propiedad de B necesitarán que se ejecute en ellos el mandato **chown** para que coincida el nuevo ID en la máquina apropiada.

Debido a los problemas para mantener la coherencia en las correlaciones de UID y GID en todas las máquinas de una red, normalmente se utiliza NIS para realizar las correlaciones apropiadas a fin de evitar este tipo de problema.

#### **Resolución de nombres de sistema principal en un servidor NFS**

Cuando un servidor NFS atiende una petición de montaje, busca el nombre del cliente que realiza la petición. El servidor toma la dirección de Internet Protocol (IP) del cliente y busca el nombre de sistema principal correspondiente que coincide con dicha dirección.

Cuando se ha encontrado el nombre de sistema principal, el servidor busca en la lista de exportaciones el directorio solicitado y comprueba la existencia del nombre de cliente en la lista de accesos del directorio. Si existe una entrada para el cliente y la entrada coincide exactamente con lo que se ha devuelto para la resolución de nombres, pasa esa parte de la autentificación de montaje.

Si el servidor no puede realizar la resolución de dirección IP con nombre de sistema principal, el servidor rechaza la petición de montaje. El servidor debe ser capaz de encontrar alguna coincidencia para la dirección IP de cliente que realiza la petición de montaje. Si el directorio se exporta teniendo acceso a todos los clientes, el servidor debe seguir siendo capaz de realizar la búsqueda de nombres inversa para permitir la petición de montaje.

El servidor también debe poder buscar el nombre correcto del cliente. Por ejemplo, si existe una entrada en el archivo /etc/exports como la siguiente:

```
/tmp -access=silly:funny
```

en el archivo /etc/hosts existirán las siguientes entradas correspondientes:

150.102.23.21	silly.domain.name.com
150.102.23.52	funny.domain.name.com

Fíjese que los nombres no se corresponden exactamente. Cuando el servidor busca las coincidencias de dirección IP con nombre de sistema principal para los sistemas principales silly y funny, los nombres de serie no coinciden exactamente con las entradas de la lista de accesos de la exportación. Este tipo de problema de resolución de nombres se produce generalmente cuando se utiliza el daemon **named** para la resolución de nombres. La mayoría de base de datos de daemon **named** tienen alias para los nombres de dominio completos de los sistemas principales para que los usuarios no tengan que entrar nombres completos al referirse a los sistemas principales. Aunque existan estas entradas de nombre de sistema

principal con dirección IP para los alias, es posible que la búsqueda inversa no exista. Normalmente la base de datos para la búsqueda de nombres inversa (dirección IP con nombre de sistema principal) tiene entradas que contienen la dirección IP y el nombre de dominio completo (no el alias) de dicho sistema principal. A veces, las entradas de exportación se crean con el nombre de alias más corto, lo que causa problemas cuando los clientes intentan montarse.

#### **Limitaciones en el número de grupos de la estructura NFS**

En sistemas que utilizan NFS Versión 2 o 3, los usuarios no pueden ser miembros de más de 16 grupos sin complicaciones.

El mandato **groups** define los grupos. Si un usuario es miembro de 17 grupos o más y el usuario intenta acceder a archivos que son propiedad del grupo 17 (o un número mayor), el sistema no permite que se lea o se copie el archivo. Para permitir al usuario acceder a los archivos, reorganice el orden del grupo.

La información anterior describe el comportamiento predeterminado. Consulte el parámetro **maxgroups** del mandato **mount** para obtener más detalles.

#### **Servidores NFS con versiones anteriores de NFS**

Un cliente NFS Versión 3 no puede montarse en un servidor NFS Versión 4.

Cuando se monta un sistema de archivos de un servidor NFS anterior a la Versión 3 en un cliente NFS de la versión 3, se produce un problema cuando el usuario del cliente que ejecuta el montaje es miembro de más de ocho grupos. Algunos servidores no pueden tratar correctamente con esta situación y rechazan la petición del montaje. La solución consiste en cambiar la calidad de miembro de grupo del usuario a un número menor que ocho y, a continuación, reintentar el montaje. El mensaje de error siguiente es característico de este problema de grupo:

```
RPC: Error de autentificación; why=Credencial de cliente no válida
```

#### **Determinación de problemas de RPCSEC-GSS**

Tenga en cuenta las soluciones siguientes cuando tenga problemas con RPCSEC-GSS.

- Utilice el mandato **klist** en el cliente para asegurarse de que tiene credenciales actuales válidas.
- Asegúrese de que los relojes del cliente, servidor y KDC están sincronizados. Se recomienda utilizar una configuración NTP o equivalente para asegurar una hora coherente en toda la región de Kerberos.
- Asegúrese de que el servidor tiene un archivo keytab y un principal de sistema principal válidos. Si el mandato siguiente falla, el servidor no funcionará:

```
kinit -kt 'tail -n 1 /etc/nfs/hostkey' 'head -n 1 /etc/nfs/hostkey'
```

- Asegúrese de que el daemon **gssd** está en ejecución y responde en el cliente y el servidor con el mandato siguiente:

```
rpcinfo -u localhost 400234
```

Si el daemon **gssd** no responde, RPCSEC-GSS fallará; es posible que este problema se corrija deteniendo y reiniciando el daemon **gssd**.

- Si está obteniendo errores con la integridad o privacidad de grabación, asegúrese de que está utilizando el módulo de kernel. La integridad y la privacidad no se soportan sin el módulo de kernel. (El módulo de kernel es el módulo de kernel de Kerberos, `/usr/lib/drivers/nfs.ext`. Se instala con el conjunto de archivos `modcrypt.base` del paquete de ampliación.)
- Si usuarios específicos reciben rechazos al acceder a datos a los que deben tener acceso, verifique que los principales implicados en el KDC se sincronicen correctamente con el nombre de cuenta de AIX del usuario.
- Active el registro cronológico del sistema. Se registrarán la mayoría de los errores de RPCSEC-GSS. Los errores tienen dos partes: la primera es el código de error GSS (consulte RFC 2744 para obtener detalles) y la segunda es un código de error de Kerberos.

**Nota:** Es posible que al activar el registro cronológico del sistema quede afectado el rendimiento del sistema; por consiguiente, se deberá desactivar el registro cronológico cuando se haya completado la determinación de problemas.

A continuación se proporcionan algunos códigos de error comunes y las soluciones:

#### KRB5\_CC\_NOTFOUND

No se han podido encontrar credenciales válidos de Kerberos. Es posible que el mandato **kinit** arregle este problema.

#### KRB5\_KDC\_UNREACH

No se puede alcanzar el KDC. Asegúrese de que el KDC está activo y que no hay problemas de red entre el cliente o servidor y el KDC.

#### KRB5\_KT\_NOTFOUND

No se ha encontrado la entrada keytab para el principal de servidor. Utilice el mandato **nfskey -l** para asegurarse de que está utilizando el principal (debe ser nfs/<nombre de dominio totalmente calificado>) y el archivo keytab correctos. Utilice **klist -ke** para consultar en el archivo keytab de servidor la entrada apropiada.

#### KRB5KRB\_AP\_ERR\_TKT\_NYV

Lo más probable es que indique un problema de reloj

#### KRB5KRB\_AP\_WRONG\_PRINC y KRB5KDC\_ERR\_S\_PRINCIPAL\_UNKNOWN

Estos dos errores indican que el principal que el cliente está utilizando para el cliente no coincide con el principal de sistema principal del servidor.

#### KRB5KRB\_AP\_WRONG\_PRINC

Indica que el cliente ha resuelto satisfactoriamente el nombre de sistema principal del servidor en un principal existente con el formato nfs/<nombre de dominio totalmente calificado>, pero el principal de sistema principal del servidor no coincide con este principal.

#### KRB5KDC\_ERR\_S\_PRINCIPAL\_UNKNOWN

Indica que el cliente no ha podido resolver el nombre de sistema principal del servidor en un principal existente. Utilice el mandato **nfskey -l** para comprobar el servidor a fin de asegurarse de que tiene el principal correcto. Si es así, la tabla de correlaciones de sistemas principales del cliente necesitará actualizarse; consulte el mandato **nfsmap** para obtener detalles.

### Determinación de problemas de EIM

Cuando solucione problemas de EIM, tenga en cuenta los consejos siguientes.

Tenga en cuenta lo siguiente cuando tenga problemas con EIM:

- Si los mandatos **nfsrgyd** o **chnfsim** no se pueden conectar al servidor LDAP EIM, asegúrese de que el proceso **ibmslapd** se esté ejecutando en el servidor LDAP EIM escribiendo el mandato siguiente:

```
ps -ef | grep ibmslapd
```

Si el proceso **ibmslapd** no se está ejecutando, escriba el mandato siguiente para activarlo:

```
/usr/sbin/ibmslapd
```

- Si los mandatos **nfsrgyd** o **chnfsim** pueden conectarse al servidor LDAP EIM pero no pueden realizar ninguna operación de correlación de identidad, asegúrese de que el proceso **ibmslapd** no se esté ejecutando en modalidad de sólo configuración.

Esto puede suceder si la base de datos **ldapdb2** no está en ejecución cuando se inicia el servidor **ibmslapd**. Siga estos pasos:

a) Inicie la sesión en el servidor LDAP EIM como usuario root.

b) Visualice el archivo **/var/ldap/ibmslapd.log**. Compruebe cuándo se ha iniciado el proceso **ibmslapd** por última vez. Compruebe también si el servidor se ha iniciado en modalidad de sólo configuración porque no se ha podido conectar a la base de datos **ldapdb2**.

Si el servidor no ha podido conectarse a la base de datos **ldapdb2**, es necesario iniciar la base de datos. Siga estos pasos para iniciar la base de datos **ldapdb2**:

- a) Inicie la sesión en el servidor LDAP EIM como usuario root.
- b) Escriba el mandato siguiente para comprobar si el proceso `ibmslapd` está activo:

```
ps -ef | grep ibmslapd
```

Si está activo, inhabilitelo ejecutando el mandato siguiente:

```
kill ibmslapd pid
```

donde `pid` es el ID de proceso que se ha devuelto del mandato `ps -ef`.

- c) Cuando se haya inhabilitado el proceso `ibmslapd`, inicie la base de datos `ldapdb2`:
  - a. Inicie la sesión en el servidor LDAP EIM como el usuario `ldapdb2`.
  - b. Escriba `db2start`.
- d) Cuando la base de datos `ldapdb2` se haya iniciado, active el proceso `ibmslapd`:
  - a. Inicie la sesión en el servidor LDAP EIM como usuario root.
  - b. Escriba `ibmslapd`.

#### **Problemas que se producen si no se carga la extensión de kernel NFS**

Algunos mandatos NFS no se ejecutan correctamente si no se ha cargado la extensión de kernel NFS. Algunos mandatos que tienen esta dependencia son: **nfsstat**, **exportfs**, **mountd**, **nfsd** y **biod**.

Cuando se instala NFS en el sistema, la extensión de kernel se pone en el archivo `/usr/lib/drivers/nfs.ext`. Entonces este archivo se carga como extensión de kernel NFS cuando se configura el sistema. El script que realiza esta extensión de kernel carga el archivo `/etc/rc.net`. En este script se realizan otras acciones, entre las cuales se encuentra la carga de la extensión de kernel NFS. Es importante tener en cuenta que la extensión de kernel de **TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de control de transmisiones/Protocolo Internet)** y el archivo `nfs_kdes_null.ext` se deben cargar antes de que se cargue la extensión de kernel NFS.

**Nota:** Para cargar la extensión de kernel NFS en el kernel, se utiliza el mandato **gfsinstall** cuando el sistema arranca inicialmente. Este mandato se puede ejecutar más de una vez por arranque del sistema y no causará ningún problema. El sistema se envía actualmente con el mandato **gfsinstall** utilizado en los archivos `/etc/rc.net` y `/etc/rc.nfs`. No es necesario eliminar ninguna de estas llamadas.

#### **Problemas que se producen si no se instala el soporte de kerberos**

Si no se instala el soporte de kerberos, el daemon **gssd** no se inicia.

Asegúrese de que estén instalados los catálogos de archivos `krb5.client.rte` y `modcrypt.base`. Si uno de ellos no está instalado, el daemon **gssd** no se ejecutará.

#### **Elementos a comprobar si el daemon de registro no está en ejecución**

El daemon **nfsrgyd** no se ejecuta si no se ha configurado el dominio NFS versión 4.

Para obtener información sobre cómo configurar el dominio de NFS versión 4, consulte el apartado “[Archivo /etc/nfs/local\\_domain](#)” en la página 600.

## **Archivos NFS**

Aquí se pueden consultar los archivos NFS y las descripciones de los mismos.

<b>Item</b>	<b>Descripción</b>
<code>bootparams</code>	Lista clientes que los clientes sin disco pueden utilizar para arrancar.
<code>exports</code>	Lista los directorios que se pueden exportar a clientes NFS.
<code>filesystem</code>	Lista todos los sistemas de archivo y se montan en el reinicio de sistema. S
<code>hostkey</code>	Especifica el principal de sistema principal Kerberos y la ubicación del archivo keytab.

<b>Item</b>	<b>Descripción</b>
local_doma in	Contiene el dominio NFS local del sistema.
networks	Contiene información sobre redes de la red Internet.
pcnfsd.con f	Proporciona opciones de configuración para el daemon <b>rpc.pcnfsd</b> .
princmap	Correlaciona nombres de sistema principal con principales de Kerberos cuando el principal no es el nombre de dominio totalmente calificado del servidor.
realm.map	Lo utiliza el daemon de registro NFS para correlacionar principales de Kerberos de entrada.
rpc	Contiene información de base de datos para los programas RPC (Remote Procedure Call - Llamada a procedimiento remoto).
security_d efault	Contiene los valores predeterminados de seguridad NFS.
xtab	Lista los directorios que se exportan actualmente.

## Mandatos NFS

Aquí se pueden consultar los mandatos NFS y las descripciones de los mismos.

<b>Item</b>	<b>Descripción</b>
<b>chnfs</b>	Inicia un número especificado de daemons <b>biod</b> y <b>nfsd</b> .
<b>chnfsdom</b>	Cambie el dominio NFS local.
<b>chnfsim</b>	Cambia las correlaciones de identidad externa de NFS
<b>chnfssec</b>	Cambia el tipo de seguridad externa utilizado por el cliente NFS
<b>chnfsrnd</b>	Cambia las correlaciones de región con dominio NFS locales.
<b>mknfs</b>	Configura el sistema para que ejecute NFS e inicia los daemons NFS.
<b>nfso</b>	Configura las opciones de red NFS.
<b>automount</b>	Monta un sistema de archivos NFS automáticamente.
<b>chnfsexp</b>	Cambia los atributos de un directorio exportado por NFS.
<b>chnfsmnt</b>	Cambia los atributos de un directorio montado por NFS.
<b>exportfs</b>	Exporta y elimina la exportación de directorios a clientes NFS.
<b>lsnfsexp</b>	Visualiza las características de los directorios que se exportan con NFS.
<b>lsnfsmnt</b>	Visualiza las características de sistemas NFS montados.
<b>mknfsexp</b>	Exporta un directorio utilizando NFS.
<b>mknfsmnt</b>	Monta un directorio utilizando NFS.
<b>nfshostkey</b>	Configura la clave de sistema principal para un servidor NFS.
<b>nfs4cl</b>	Visualiza información sobre los sistemas de archivos a los que está accediendo un cliente utilizando NFS versión 4.
<b>nfs4smct1</b>	Administra la revocación de estado de NFS versión 4
<b>rmnfs</b>	Detiene los daemons NFS.
<b>rmnfsexp</b>	Elimina los directorios exportados por NFS de la lista de exportaciones de un servidor.
<b>rmnfsmnt</b>	Elimina sistemas de archivos montados por NFS de la lista de montajes de un cliente.

## NFS, daemons

Aquí se pueden consultar los daemons NFS y las descripciones de los mismos.

### Daemons de bloqueo

Item	Descripción
------	-------------

**lockd** Procesa las peticiones de bloqueo mediante el paquete RPC.

**statd** Proporciona funciones de anomalía y recuperación para los servicios de bloqueo en NFS.

### Daemons y programas de utilidad de servicio de red

Item	Descripción
------	-------------

**biod** Envía las peticiones de lectura y grabación del cliente al servidor.

**mountd** Responde las peticiones de los clientes para los montajes de sistema de archivos.

**nfsrgyrd** Realiza la conversión entre los principales de seguridad, las series de identidad de NFS versión 4 y los ID de sistema numéricos correspondientes. Además, se proporciona información de correlación de identidad de dominios NFS versión 4 externos.

**nfsd** Inicia los daemons que manejan las peticiones de operaciones de sistema de archivos efectuadas por un cliente.

**nfsstat** Visualiza información sobre la posibilidad de recibir llamadas para una máquina determinada.

**on** Ejecuta mandatos en máquinas remotas.

**pcnfsd** Maneja peticiones de servicio de clientes PC-NFS.

**portmap** Correlaciona números de programa RPC con números de puerto de Internet.

**rexld** Acepta la petición de ejecución de programas desde máquinas remotas.

**rpcgen** Genera el código C para implementar un protocolo RPC.

**rpcinfo** Informa del estado de los servidores RPC.

**rstatd** Devuelve las estadísticas de rendimiento obtenidas del kernel.

**rup** Muestra el estado de un sistema principal remoto en la red local.

**rusers** Informa de una lista de usuarios conectados a las máquinas remotas.

**rusersd** Responde a las consultas del mandato **rusers**.

**rwall** Envía mensajes a todos los usuarios de la red.

**rwalld** Maneja peticiones del mandato **rwall**.

**showmount** Visualiza una lista de todos los clientes que han montado sistemas de archivos remotos.

**spray** Envía un número especificado de paquetes a un sistema principal.

**sprayd** Recibe los paquetes enviados por el mandato **spray**.

### Daemons y programas de utilidad de red seguros

Item	Descripción
------	-------------

**chkey** Cambia la clave de cifrado del usuario.

**gssd** Proporciona a NFS acceso a los servicios de seguridad proporcionados por Network Authentication Services.

**keyenvoy** Proporciona un intermediario entre los procesos de usuario y el servidor de claves.

**keylogin** Descifra y almacena la clave secreta de usuario.

<b>Item</b>	<b>Descripción</b>
<b>keyserv</b>	Almacena claves públicas y privadas.
<b>mkkeyserv</b>	Inicia el daemon <b>keyserv</b> y elimina la marca de comentario en las entradas apropiadas en el archivo /etc/rc.nfs.
<b>newkey</b>	Crea una clave nueva en el archivo publickey.
<b>rmkeyserv</b>	Detiene el daemon <b>keyserv</b> y comenta la entrada para el daemon <b>keyserv</b> en el archivo /etc/rc.nfs.
<b>ypupdated</b>	Actualiza información en las correlaciones de NIS (Network Information Service).

Para obtener información adicional sobre la seguridad de NFS, consulte el apartado [Network File System security](#) en la publicación *Security*.

### Soporte de cliente sin disco de Sun

<b>Item</b>	<b>Descripción</b>
<b>bootparamd</b>	Proporciona la información necesaria para arrancar en clientes sin disco.

## Subrutinas NFS

Aquí se describen las subrutinas NFS.

<b>Item</b>	<b>Descripción</b>
cbc_crypt, des_setparity o ecb_crypt	Implementa las rutinas DES (Data Encryption Standard - Estándar de cifrado de datos).

## Protocolo SMB

El protocolo SMB (Server Message Block) es un protocolo de comunicación cliente-servidor que se utiliza para el acceso compartido a archivos, directorios, impresoras, puertos serie y otros recursos de una red. También proporciona un mecanismo de comunicación entre procesos (IPC) autenticado.

### Sistema de archivos de bloque de mensajes de servidor

El sistema de archivos de bloque de mensajes de servidor permite acceder a compartimientos de servidores SMB como sistemas de archivos locales en el sistema operativo AIX utilizando el protocolo SMB versión 1.0.

En este sistema de archivos, el usuario puede crear, suprimir leer, grabar y modificar los tiempos de acceso de los archivos y directorios. No se pueden cambiar el propietario ni la modalidad de acceso de los archivos y directorios.

Se puede utilizar SMBFS para acceder a archivos de un servidor SMB. El servidor SMB es un servidor que ejecuta Samba o un servidor o estación de trabajo Windows XP, Windows NT o Windows 2000. Cada uno de estos tipos de servidor permite que un directorio se exporte como un compartimiento. Entonces este compartimiento se puede montar en un sistema AIX utilizando SMBFS.

### Instalación del sistema de archivos SMB

Para instalar SMBFS en un sistema AIX, instale el paquete bos.cifs\_fs.

Al instalar el paquete bos.cifs\_fs, se crea el dispositivo nsmb0. Este dispositivo permite al mandato **mount** establecer una conexión entre el servidor SMB y el cliente que utiliza el protocolo CMB versión 1.0.

## Montaje del sistema de archivos SMB

Puede montar el SMBFS utilizando el mandato AIX **mount**. Por ejemplo:

```
mount -v cifs -n pezman/user1/pass1 -o uid=201,fmode=750 /home /mnt
```

Puede especificar opciones de montaje utilizando el distintivo **-o**. Las opciones de línea de mandatos sólo se deberán separar con una coma, no una coma y un espacio. Las opciones para el sistema de archivos son:

Item	Descripción
fmode	Establece el archivo o directorio en modalidad octal. El valor predeterminado es 755.
uid	Asigna un ID de usuario a los archivos durante el montaje. El valor predeterminado es <b>root</b> .
gid	Asigna un ID de grupo a los archivos durante el montaje. El valor predeterminado es <b>system</b> .
wrkgrp	Grupo de trabajo al que pertenece el servidor SMB.
op	Establezca el valor en 1 si se utiliza el bloqueo oportunista. Establezca el valor en 0 si no se utiliza el bloqueo oportunista.
opfs	Nombre del sistema de archivos de antememoria a utilizar para almacenar archivos de antememoria de bloqueo.
opsz	Tamaño de archivos de antememoria individuales utilizados para el bloqueo oportunista.
opfssz	Tamaño de sistema de archivos de antememoria utilizado en el bloqueo oportunista.

También puede montar el sistema de archivos utilizando el programa de utilidad SMIT, **smit cifs\_fs**, que ejecuta el mandato **mount** después de recopilar toda la información necesaria.

Para montar un SMBFS, es necesario proporcionar un nombre de usuario y una contraseña para autenticarse en el servidor. Este nombre de usuario y esta contraseña se utilizan para realizar todas las operaciones de archivo necesarias en el servidor. El campo **Contraseña** en el panel de SMIT no está marcado como necesario. Si el campo de contraseña no se rellena, se busca en el archivo **cifscred** credenciales coincidentes para el usuario o el servidor que se proporciona. Si existe una coincidencia, se utiliza la contraseña almacenada del archivo **cifscred**; de lo contrario, se solicita al usuario una contraseña mediante el indicador de solicitud de contraseña estándar de AIX. De este modo, el usuario puede proporcionar una contraseña sin dejarla visible.

**Nota:** La contraseña utilizada para montar SMBFS puede tener una longitud de hasta 14 caracteres y la contraseña puede contener caracteres especiales.

Siempre que se invoca un mandato de sistema de archivos, por ejemplo **read**, en un archivo en el punto de montaje SMBFS, se envía una petición al servidor para leer el archivo. El nombre de usuario y la contraseña envían como parte de esta petición para que el servidor pueda determinar si el usuario tiene permiso en el servidor para realizar una operación de lectura en dicho archivo. Por consiguiente, la autorización final de permitir una operación en un archivo es el servidor quien la otorga.

Sin embargo, la opción **fmode** del mandato **mount** proporciona un modo para que el usuario **root** del sistema cliente controle el acceso a los archivos del servidor antes de que se consulte el servidor. Si el usuario no proporciona la opción **fmode**, el valor predeterminado es 755. La tabla siguiente ilustra cómo funciona la opción **fmode** utilizando una petición de grabación:

Tabla 94. Cinco casos en los que se ha permitido o rechazado el acceso a los usuarios basándose en los permisos proporcionados.

Número de caso	Usuario autentificado en servidor	Usuario del lado de cliente que desea acceso de grabación	Propietario, grupo y modalidad de montaje	Propietario, grupo y modalidad en el servidor	Acceso permitido
Caso 1	user1	user2	user1, staff rwxr-xr-x	user1, staff rwxrwxr-x	no
Caso 2	user1	root	user1, staff rwxr-xr-x	user2, staff rwxr-xr-x	no
Caso 3	user1	user1	user1, staff rwxr-xr-x	user2, staff rwxrwxr-x	sí
Caso 4	user1	user1	user1, staff rwxr-xr-x	root, system rwx-----	no
Caso 5	user1	user1	user1, staff rwxr-xr-x	root, system rwxrwxrwx	sí

En el Caso 1, se rechaza el acceso porque el propietario, el grupo y la modalidad en el montaje en el cliente no permitían el acceso de grabación a user2.

En el Caso 2, se rechaza el acceso porque, aunque root tiene acceso a todos los elementos en el lado del servidor, el usuario autentificado por el servidor, user1, no tiene acceso al archivo del servidor.

En el Caso 3, se otorga el acceso porque user1 era el propietario en el montaje y user1, como miembro del grupo staff del servidor, tiene acceso al archivo del servidor.

En el Caso 4, se rechaza el acceso porque, aunque user1 era el propietario en el montaje, el archivo es propiedad de root en el servidor, sin acceso por parte de grupo u otro.

En el Caso 5, se otorga el acceso porque user1 era el propietario en el montaje y user1 tenía acceso al archivo del servidor mediante otros permisos.

#### Notas:

1. El cliente SMBFS de AIX sólo admite SMBv1.
2. En el sistema de archivos montado, una operación de copia de un archivo a otro es satisfactoria para un archivo de tamaño 4 GB + 4096 bytes o menos. Para archivos con un tamaño superior, se imprime un mensaje de aviso y 4 GB + 4096 bytes del archivo original se copian en el destino.
3. En el sistema de archivos montado, los caracteres siguientes no se pueden utilizar en un nombre de archivo: tecla de barra inclinada invertida {\}, tecla de barra inclinada {/}, dos puntos {:}, asterisco {\*} , signo de interrogación {?} , tecla de menor que {<} , tecla de mayor que {>} , tecla de barra vertical { | } .

#### Contraseñas almacenadas

SMBFS puede almacenar credenciales de server/user/password en el archivo /etc/cifs\_fs/cifscred para permitir la recuperación automática de las contraseñas al montar SMBFS.

En este archivo se pueden añadir, cambiar y eliminar credenciales con los mandatos **mkcifscred**, **chcifscred** y **rmcifscred** (ubicados en el archivo /usr/sbin). Las contraseñas añadidas a este archivo están cifradas. Cuando se intenta un montaje sin proporcionar una contraseña, se buscan en el archivo cifscred las credenciales que coincidan. Si existe una coincidencia, se utiliza la contraseña

almacenada del archivo `cifscred`; de lo contrario, se solicita al usuario una contraseña mediante el indicador de solicitud de contraseña estándar de AIX.

El soporte para las contraseñas almacenadas tiene las limitaciones siguientes:

- Para que la recuperación de contraseñas almacenadas funcione correctamente, el convenio de denominación de servidor debe ser coherente. Por ejemplo, si las credenciales se añaden con una dirección IP en lugar de un nombre de sistema principal o un nombre de dominio totalmente calificado (FQDN), las contraseñas sólo se recuperarán cuando se realice el montaje por dirección IP.
- No se soporta la autenticación de contraseña de texto sin formato con el método de recuperación de contraseña almacenada. Si el servidor necesita contraseñas de texto sin formato, la autenticación fallará.

### **Soporte a /etc/filesystems**

SMBFS proporciona soporte a `/etc/filesystems` para permitir el montaje automatizado durante el arranque del sistema.

El soporte a `/etc/filesystems` también proporciona acceso a los datos sobre el servidor almacenado, el usuario, la contraseña y las opciones durante el montaje. Utilice los mandatos `mkcifsmnt`, `chcifsmnt`, `rmcifsmnt` y `lscifsmnt` (que se encuentran en `/usr/sbin`) para añadir, modificar, eliminar y listar, respectivamente, stanzas de cifs en `/etc/filesystems`. Las credenciales deben almacenarse en el archivo `cifscred`.

### **Resolución de problemas de SMBFS**

Si el mandato `mount` o la vía de acceso rápida `smit cifs_fs` devuelve un error, tenga en cuenta lo siguiente:

- Asegúrese de que el nombre de usuario y la contraseña son correctos. El nombre de usuario y la contraseña necesitan permitir el acceso al compartimiento del servidor.
- Asegúrese de que el nombre de servidor es correcto. Si el nombre de servidor es correcto, utilice el nombre de sistema principal totalmente calificado en el caso de que el servidor no forme parte de la misma subred que el cliente. También puede intentar utilizar la dirección IP de servidor.
- Asegúrese de que el mandato `lsdev -L | grep nsmb` devuelve un nombre de dispositivo. Si un dispositivo nsmb no está disponible, el cliente AIX no podrá establecer una conexión con el servidor SMB.
- Asegúrese de que el nombre de servidor es correcto. Si el compartimiento no existe en el servidor o no se puede acceder al mismo con el nombre de usuario y la contraseña que se han proporcionado, el servidor SMB rechazará la petición de conexión.
- Utilice el ID de suceso 525 para recopilar datos de rastreo de sistema para SMBFS.
- Asegúrese de que el servidor se ha configurado para aceptar contraseñas NTLM, LM o de texto sin formato. Éstos son los únicos tipos de cifrado de contraseña soportados por SMBFS.
- Si desea realizar la autenticación en un dominio, se debe especificar el nombre de dominio con la opción `wrkgrp`. Sin esta opción, el servidor maneja localmente la autenticación.

### **Sistema de archivos de cliente SMB (Server Message Block)**

El sistema de archivos de cliente SMB se basa en el protocolo SMB versión 2.1 y versión 3.0.2. Puede utilizar el sistema de archivos de cliente SMB para acceder a los archivos de un servidor SMB.

El servidor SMB es un servidor que se ejecuta en el sistema operativo Windows Server 2012 o Windows Server 2016. En cada uno de estos tipos de sistema operativo de servidor puede exportarse un directorio como *recurso compartido*. A continuación, este recurso compartido se puede montar en una partición lógica de AIX utilizando el sistema de archivos de cliente SMB. Mediante el sistema de archivos de cliente SMB, puede acceder a los recursos compartidos de los servidores SMB como sistemas de archivos locales en la partición lógica de AIX. Puede utilizar el sistema de archivos de cliente SMB para crear, suprimir, leer y escribir archivos y directorios en el servidor SMB y también para modificar la duración del

acceso a estos archivos y directorios. Sin embargo, no puede cambiar el propietario ni el permiso de acceso de estos archivos y directorios.

➤ En el sistema de archivos de cliente SMB están disponibles las siguientes funciones de protocolo SMB 3.0.2:

### Negociación de dialecto seguro SMB 3.0.2

Puede montar un recurso compartido desde el servidor SMB en el sistema de archivos virtual de AIX (VFS) utilizando la versión 3.0.2 del protocolo SMB.

El servidor de dialecto SMB 3.0.2 proporciona una negociación de dialecto segura para estar protegido ante riesgos de seguridad. Cuando se negocia el dialecto SMB 3.0.2, el cliente SMB debe enviar una solicitud firmada obligatoria para validar la información de negociación.

### Firma de SMB 3.0.2

El protocolo SMB 3.0.2 utiliza un algoritmo de cifrado más reciente para la firma. Código de autenticación de mensajes basado en cifrado (CMAC) AES (Advanced Encryption Standard), AES-128-CMAC, para garantizar la integridad de los mensajes intercambiados entre el cliente SMB y el servidor SMB firmando los mensajes de salida y validando los mensajes de entrada.

### Cifrado de SMB 3.0.2

El cifrado SMB proporciona cifrado de extremo a extremo de los datos SMB y protege los datos ante sucesos de escucha en redes no fiables. El cifrado SMB se puede configurar individualmente para cada recurso compartido o para todo el servidor de archivos, y se puede habilitar para diversos escenarios en los que los datos circulen por redes no fiables.



- “[Instalación del sistema de archivos de cliente SMB](#)” en la página 654
- “[Montaje del sistema de archivos de cliente SMB como un punto de montaje local](#)” en la página 655
- “[Autenticación Kerberos para el sistema de archivos de cliente SMB](#)” en la página 656
- “[Contraseñas almacenadas](#)” en la página 657
- “[Soporte de archivos /etc/filesystems](#)” en la página 657

### Instalación del sistema de archivos de cliente SMB

El sistema de archivos de cliente SMB en el sistema operativo AIX requiere que la GSSAPI basada en Kerberos inicie la sesión autenticada por el usuario utilizando el protocolo SMB versión 2.1 o 3.0.2. En el sistema operativo AIX, la GSSAPI la proporciona una biblioteca de espacios de usuario en el conjunto de archivos de IBM Network Authentication Service (NAS) versión 1.16.1.0 o posterior. La versión 3.0.2 de SMB utiliza la biblioteca OpenSSL de AIX para generar claves para la firma y el cifrado. Por lo tanto, es necesario instalar la versión 1.0.2.2002 o una versión posterior del conjunto de archivos openssl.base. Estos conjuntos de archivos se incluyen en AIX Expansion Pack.

Para instalar el sistema de archivos de cliente SMB en una partición lógica de AIX, realice los pasos siguientes:

1. Vaya a la página web de [AIX Web Download Pack Programs](#) e inicie la sesión utilizando su ID y contraseña de IBM.
2. Seleccione la opción **SMB CLIENT Versión 3.0.2** y pulse **Descargar**.

Sus credenciales de IBM deben tener derecho a descargar el paquete del sistema de archivos de cliente SMB. De lo contrario, no puede descargar el paquete.

3. Instale el paquete smbc .rte utilizando el mandato **installp**.

Al instalar el paquete smbc .rte, se crea el dispositivo nsmbc0. Este dispositivo permite que el mandato **mount** establezca una conexión entre el servidor SMB y el sistema de archivos de cliente SMB utilizando el protocolo de cliente SMB versión 2.1 o 3.0.2.

## Montaje del sistema de archivos de cliente SMB como un punto de montaje local

Puede montar el sistema de archivos de cliente SMB utilizando el mandato siguiente:

```
mount -v smbc -n windows_server/Kerberos_username/password_for_Kerberos_user \
-o wrkgrp=workgroup,[[port=139|445],[signing=required|enabled],[pver=2.1|3.0.2|auto], \
[encryption=desired|required|disabled],[secure_negotiate=desired|required|disabled]] \
share_point_to_mount_created_on_windows local_mount_point
```

Por ejemplo,

```
mount -v smbc -n llm140.xyz.com/cec102usr1/Passw0rd \
-o "wrkgrp=SMB_302.test,port=445,signing=required,encryption=required, \
secure_negotiate=desired,pver=auto" /some_share /mnt
```

Puede especificar los parámetros siguientes con el distintivo **-o** del mandato **mount**. Los parámetros deben estar separados solo por una coma. No inserte un espacio antes ni después de una coma.

### fmode

Establece un archivo o directorio en modalidad octal para permisos de acceso. El valor predeterminado es 755.

### uid

Asigna un ID de usuario a los archivos durante la operación de montaje. El valor predeterminado es root.

### gid

Asigna un ID de grupo a los archivos durante la operación de montaje. El valor predeterminado es system.

### wrkgrp

Especifica el grupo de trabajo al que pertenece el servidor SMB. Este parámetro es obligatorio para montar el sistema de archivos de cliente SMB.

### port

Especifica el número de puerto. Los valores válidos son 445 y 139. El valor predeterminado es 445. El puerto 139 sólo está soportado cuando la dirección de servidor especificada está en el formato IPv4.

### pver

Especifica la versión de protocolo SMB que se utiliza para comunicarse con el servidor SMB. Los valores válidos son 2.1 o 3.0.2 y auto. Cuando se especifica el valor auto, se utiliza el protocolo SMB versión 2.1 o 3.0.2 en función del servidor SMB especificado.

### signing

Especifica si el sistema de archivos de cliente SMB requiere firma digital para la comunicación. Los valores válidos son enabled y required. Cuando el parámetro **signing** se establece en enabled, el sistema de archivos de cliente SMB no firma digitalmente los paquetes de datos a menos que el sistema de archivos del servidor SMB requiera firmas digitales para la comunicación. Cuando el parámetro **signing** se establece en required, el sistema de archivos de cliente SMB debe firmar digitalmente los paquetes de datos para la comunicación. Si no especifica el valor del parámetro **signing** utilizando el mandato **mount**, se utiliza un valor predeterminado a partir de los valores de parámetro ajustables del kernel que se establecen utilizando el mandato [smbctune](#).

### secure\_negotiate

Especifica si el sistema de archivos de cliente SMB requiere cifrado. Los valores válidos son desired, required y disabled. Si no especifica este parámetro en el mandato [mount](#), se utiliza un valor predeterminado a partir de los valores de parámetro ajustables del kernel que se establecen utilizando el mandato [smbctune](#).

### encryption

Especifica si el sistema de archivos de cliente SMB requiere cifrado. Los valores válidos son desired, required y disabled. Si no especifica este parámetro en el mandato [mount](#), se utiliza un valor predeterminado a partir de los valores de parámetro ajustables del kernel que se establecen utilizando el mandato [smbctune](#).

## Autenticación Kerberos para el sistema de archivos de cliente SMB

Para montar un sistema de archivos de cliente SMB, debe autenticarse en el servidor SMB proporcionando un nombre de usuario de Kerberos y una contraseña de Kerberos. Este nombre de usuario y contraseña se utilizan para realizar todas las operaciones de archivo necesarias en el servidor SMB. Si no proporciona ninguna contraseña, se le solicitará una contraseña mediante la solicitud de contraseña estándar de AIX.

**Nota:** La contraseña que se utiliza para montar el sistema de archivos de cliente SMB puede tener un máximo de 255 caracteres de longitud. La contraseña puede contener caracteres especiales.

Cuando se ejecuta un mandato de sistema de archivos, como por ejemplo un mandato read, en un archivo del punto de montaje del cliente SMB, se envía una solicitud al servidor SMB para que lea el archivo. El ID de sesión autenticado también se envía como parte de esta solicitud de lectura. El servidor SMB utiliza este ID de sesión para determinar si el usuario se autentica en el servidor y para realizar una operación de lectura en el archivo. Por lo tanto, el servidor SMB autoriza el acceso al archivo y controla si se puede realizar una operación en el archivo.

La opción **fmode** del mandato **mount** permite que el usuario root del sistema de archivos de cliente SMB controle el acceso a los archivos del servidor SMB antes de que se consulte el servidor SMB. Si no especifica ningún valor para la opción **fmode**, la opción **fmode** utiliza el valor predeterminado de 755. La tabla siguiente explica cómo funciona la opción **fmode** con varias operaciones:

Tabla 95. Casos en los que se permite o deniega el acceso a los usuarios en función de los permisos de acceso especificados de los archivos o directorios del servidor SMB					
Número de caso	Usuario autenticado en el servidor SMB	Usuario del sistema de cliente que solicita acceso de grabación	Propietario, grupo y modalidad de acceso del montaje	Propietario del archivo o directorio del servidor SMB, grupo y modalidad de acceso en el servidor SMB	Permiso de acceso
Caso 1	user1	user2	user1, staff, rwxr-xr-x	user1, staff, rwxrwxr-x	no
Caso 2	user1	root	user1, staff, rwxr-xr-x	user2, staff, rwxr-xr-x	no
Caso 3	user1	user1	user1, staff, rwxr-xr-x	user2, staff, rwxrwxr-x	sí
Caso 4	user1	user1	user1, staff, rwxr-xr-x	root, system, rwx-----	no
Caso 5	user1	user1	user1, staff, rwxr-xr-x	root, system, rwxrwxrwx	sí

En el Caso 1, se rechaza el acceso al archivo o directorio a user2 porque el propietario, el grupo y la modalidad en el punto de montaje en el cliente SMB no proporcionaba acceso de grabación a user2.

En el Caso 2, se rechaza el acceso al archivo o directorio al usuario root porque, aunque root tiene acceso a todos los elementos en el cliente SMB, el usuario autenticado por el servidor SMB, user1, no tiene acceso al archivo del servidor SMB.

En el Caso 3, se otorga el acceso a user1 al archivo o directorio porque user1 era el propietario del montaje durante la operación de montaje y user1, un miembro del grupo staff en el servidor SMB, tenía acceso al archivo en el servidor.

En el Caso 4, se rechaza el acceso al archivo o directorio a user1 porque, aunque user1 era el propietario durante la operación de montaje, el archivo es propiedad del usuario root en el servidor SMB, y los miembros del grupo y otros usuarios no tienen ningún permiso de acceso.

En el Caso 5, user1 tiene acceso al archivo o directorio porque la modalidad de acceso indicada especifica el permiso de acceso completo a todos los miembros del grupo y otros usuarios.

**Nota:** En el sistema de archivos montado, los caracteres siguientes no se pueden utilizar en el nombre del archivo: tecla de barra inclinada invertida (\), tecla de barra inclinada (/), dos puntos (:), asterisco (\*), signo de interrogación (?), tecla de menor de (<), tecla de mayor de (>) y tecla de barra vertical (|).

### Contraseñas almacenadas

El sistema de archivos de cliente SMB puede almacenar las credenciales de nombre de servidor, nombre de usuario y contraseña en el archivo /etc/smbc`red` para permitir la recuperación automática de contraseñas al realizar el montaje del sistema de archivos de cliente SMB. Puede ver, añadir, cambiar y eliminar las credenciales del archivo /etc/smbc`red` mediante los mandatos **lssmbc`red`**, **mksmbc`red`**, **chsmbc`red`** y **rmsmbc`red`** que se encuentran en el directorio /usr/sbin/. Las contraseñas que se añaden al archivo /etc/smbc`red` están cifradas. Cuando se realiza el montaje del sistema de archivos de cliente SMB sin especificar una contraseña, se busca en el archivo /etc/smbc`red` si hay credenciales coincidentes. Si se encuentra una coincidencia, se utiliza la contraseña almacenada del archivo /etc/smbc`red`. De lo contrario, se le solicitará una contraseña mediante la solicitud de contraseña estándar de AIX.

Tenga en cuenta las siguientes limitaciones sobre las contraseñas almacenadas:

- Para recuperar contraseñas almacenadas, el convenio de denominación de servidor debe ser coherente. Por ejemplo, si las credenciales se añaden con una dirección IP en lugar de un nombre de sistema principal o un nombre de dominio totalmente calificado (FQDN), las contraseñas sólo se recuperarán cuando se realice el montaje del sistema de archivos de cliente SMB por dirección IP.
- Debe eliminar la entrada de credencial del archivo /etc/filesystems antes de desinstalar el conjunto de archivos smbc.`rte`.

### Soporte de archivos /etc/filesystems

El sistema de archivos de cliente SMB da soporte al archivo /etc/filesystems para permitir la operación de montaje automatizada de sistemas de archivos durante la operación de arranque del sistema. El archivo /etc/filesystems también proporciona acceso a los datos de nombre de servidor, nombre de usuario, contraseña y configuración almacenados al montar un sistema de archivos. Cuando añada stanzas del sistema de archivos de cliente SMB manualmente al archivo /etc/filesystems, deberá almacenar las credenciales del sistema de archivos de cliente SMB en el archivo /etc/smbc`red`.

#### Por ejemplo:

```
$cat /etc/filesystems
.....
.....
.....
/mnt1:
dev = /fvt_share
vfs = smbc
mount = true
options = "wrkgrp=SMB_21.FVT"
nodename = <nombre_servidor>/<nombre_usuario>

/mnt:
dev = /fvt_share
vfs = smbc
mount = true
options = "wrkgrp=SMB_21.FVT,signing=required"
nodename = <nombre_servidor>/<nombre_usuario>
```

## Comunicaciones asíncronas

AIX proporciona las categorías siguientes de controladores de dispositivos asíncronos, también llamados controladores de dispositivos de tty:

- Controladores para los puertos serie de la placa del sistema
- Controladores para los puertos serie conectados al sistema a través de un adaptador
- Controladores pseudo tty

Los controladores de la primera categoría son los adaptadores PCI. Incluyen adaptadores de 2 puertos, de 8 puertos y de 128 puertos.

En la segunda categoría, los adaptadores PCI de 8 puertos y de 128 puertos se denominan adaptadores inteligentes, porque utilizan un procesador Intel 8086 para descargar la mayor parte del proceso de caracteres del CPU de host. Estos adaptadores están controlados mediante un sondeador de 20 ms en lugar de interrupciones de hardware y proporcionan características de rendimiento bien adecuadas a la mayoría de los dispositivos y aplicaciones serie. A medida que se añaden más dispositivos al sistema, la carga de trabajo del mismo aumenta muy poco, por lo que estos adaptadores pueden proporcionar soporte a un número muy grande de dispositivos serie, mucho mayor que el que sería posible utilizando interrupciones de hardware. Además, como estos adaptadores utilizan una mejora en rendimiento del software bajo patente, pueden enviar y recibir grandes cantidades de datos con mayor rapidez y eficacia que los puertos de sistemas nativos, siempre que los datos se mueven en grandes bloques. Para obtener más información, consulte la descripción wantio del archivo `/usr/include/sys/pse/README.pse`.

**Nota:** Los *puertos de sistema* integrados de POWER5 son parecidos a los puertos serie, con la salvedad de que los puertos del sistema solo están disponibles para funciones que reciben un soporte específico. Consulte el apartado “[Diferencias funcionales entre los puertos del sistema y los puertos serie](#)” en la [página 666](#) para obtener más información.

Sin embargo, algunos dispositivos y aplicaciones esperan o necesitan un período de latencia muy bajo durante el proceso de un único carácter, por lo que es posible que experimente problemas de temporización cuando se conecte a estos adaptadores inteligentes. La latencia por carácter, o el eco por carácter, puede definirse como el tiempo que se tarda en recibir un único carácter en un puerto serie, entregar este carácter a una aplicación y volver a realizar un eco del carácter desde el mismo puerto serie.

Como utilizan la prioridad de interrupción más alta del sistema(INTCLASS0), los puertos controlados por interrupciones proporciona valores de latencia comprendidos entre 0,10 y 0,20 ms en un sistema desocupado. Los adaptadores PCI de 8 puertos proporcionan valores de latencia que van de 10 a 12 ms, con tiempos individuales que varían en más o menos 10 ms debido al sondeador de 20 ms. Los adaptadores PCI de 128 puertos tienen el mismo sondeador de 20 ms, que se comunica a través de un enlace de comunicaciones sondeado con los RAN (nodos de acceso remoto). Los RAN permiten que un controlador de sondeo controle los puertos serie. Los valores de latencia de estos puertos están en 30 ms como media, pero pueden sobrepasar los 60 ms.

Los valores de latencia de los adaptadores PCI de 8 puertos y PCI de 128 puertos pueden ajustarse para aplicaciones especiales utilizando el parámetro EDELAY (retardo de sucesos). Para conseguir la máxima respuesta al recibir un solo carácter, reduzca el valor del parámetro EDELAY. Con ello se minimiza el tiempo necesario para pasar un único carácter desde el puerto serie a la aplicación, pero puede dar lugar a una reducción de la productividad y del rendimiento general del sistema cuando se reciben varios caracteres en una ráfaga.

El adaptador PCI EIA-32 de 2 puertos es un adaptador de comunicaciones serie asíncrono que se basa en Exar 17D152 Universal PC Dual UART. El adaptador de 2 puertos proporciona soporte a dos conectores DB-9 y proporciona conectividad con los dispositivos EIA-32 asíncronos como, por ejemplo, módems y terminales tty.

En la plataforma IBM eServer p5 no hay disponible ningún puerto del sistema nativo para AIX. Aunque la interfaz de terminal virtual se ha mejorado para proporcionar soporte a los puertos serie lógicos que se encuentran en el FSP a través del hipervisor, esta interfaz sólo proporciona soporte a un conjunto de dispositivos serie específicos y no resulta adecuada para sustituir un puerto serie físico de finalidad general. El adaptador de 2 puertos se comporta como un puerto del sistema nativo. El controlador de dispositivos del adaptador está controlado por interrupciones y proporciona soporte al tránsito programable y recibe niveles desencadenantes FIFO. Se trata de un adaptador PCI; por lo tanto, el controlador de dispositivos proporciona soporte a las consultas VPD, EEH y de "inserción en caliente". El adaptador de 2 puertos no proporciona soporte a las funciones del puerto del sistema nativo cuando se utiliza el terminal virtual como, por ejemplo, durante el arranque, la instalación y el soporte a KDB.

Los controladores pseudo tty se utilizan para acceder a un sistema a través de una red utilizando los mandatos **rlogin** o **telnet** o acceder a un sistema utilizando un sistema de ventanas de un supervisor de gráficos. El controlador pseudo tty proporciona una forma de ejecutar las aplicaciones existentes basadas en caracteres como, por ejemplo, el editor de textos **vi**, a través de soportes de comunicaciones que no son serie. Lo más importante que cabe observar sobre los controladores pseudo tty es que no son simétricos. El extremo esclavo proporciona una interfaz que cumple el estándar POSIX a las aplicaciones anteriores. El extremo maestro está controlado por una entidad como, por ejemplo, el daemon **rlogin** o **telnet** o X-windows, que debe proporcionar una emulación de un dispositivo de terminal serie con el controlador pseudo tty. AIX permite el soporte eficaz de un gran número de controladores pseudo tty.

## Velocidades de línea no POSIX

La interfaz con los dispositivos serie que POSIX y los estándares UNIX subsiguientes como, por ejemplo, X/Open especifican depende en la estructura de datos **termios**, definida en **/usr/include/termios.h**. Desgraciadamente, esta estructura de datos no puede utilizarse para especificar velocidades de línea superiores a los 38.400 bits por segundo. La mayor parte del hardware serie que se utiliza actualmente puede proporcionar soporte a velocidades de hasta 230.000 bps. Para utilizar estas velocidades de línea superiores en AIX, la velocidad deseada debe especificarse al configurar el puerto utilizando SMIT. Si el hardware del puerto serie (UART) puede proporcionar soporte a la velocidad de línea especificada, el puerto puede configurarse.

La opción **get attribute ioctl** utilizando la estructura **termio** o **termios** mostrará una velocidad de línea de 50 bps. El puerto utilizará la velocidad de la línea no POSIX hasta que se cambie, por lo que las aplicaciones que utilicen **set attribute ioctl** con la estructura **termio** y **termios** no deben modificar los distintivos CBAUD a menos que realmente intenten cambiar la velocidad de la línea. Si el hardware del puerto serie (UART) no puede proporcionar soporte a la velocidad de línea solicitada, el puerto no se configurará y se devolverá un error.

**Nota:** Los adaptadores PCI de 8 puertos y de 128 puertos sólo proporcionan soporte a velocidades de línea no POSIX de 115.200 y 230.000 bps. El adaptador PCI de 128 puertos tiene una restricción adicional de 2,5 Mbps de ancho de banda agregado (con un cable de 8 hilos), que los 11 dispositivos que estén transfiriendo deben consumir completamente a una velocidad sostenida de 230.000 bps cada uno. Esta restricción está en la línea que conecta el adaptador con los RAN, por lo que 22 dispositivos de este tipo pueden consumir un solo adaptador completamente.

## Adaptadores asíncronos

Los productos de comunicaciones asíncronas ofrecen la ventaja de comunicaciones con los terminales y los dispositivos de bajo coste, multiusuario, con un rendimiento entre medio y alto.

AIX permite que muchos usuarios accedan a los recursos y las aplicaciones del sistema. Cada usuario debe conectarse a través de una sesión del terminal. La conexión puede ser local o remota a través de un puerto serie.

Cada unidad del sistema tiene disponible por lo menos un puerto serie estándar (algunos sistemas tienen tres puertos serie). Estos puertos pueden proporcionar soporte a las conexiones de dispositivos y las comunicaciones asíncronas.

Los puertos asíncronos permiten la conexión de dispositivos periféricos asíncronos que cumplan con los estándares EIA 232, EIA 422 o RS-423 como, por ejemplo:

- Módems asíncronos
- Escáneres de códigos de barras
- Impresoras gráficas y de caracteres
- Terminales de teclado y de pantalla
- Sistemas personales
- Trazadores e impresoras
- Terminales de punto de venta
- Sensores y dispositivos de control
- Escáneres de texto
- Relojes

## Opciones de comunicaciones asíncronas

Es posible añadir a la unidad del sistema posibilidades ampliadas asíncronas mediante adaptadores que utilicen buses PCI (Peripheral Component Interconnect).

Varios factores pueden influir en el tipo de conexión asíncrona que se seleccione. La tabla siguiente resume estos productos.

Tabla 96. Productos de comunicación asíncrona						
Conexión asíncrona	Basado en el procesador POWER	Basado en Itanium	Tipo de bus	Código de característica o tipo de máquina (modelo)	Velocidad de datos máxima por puerto (kbps)	Características destacables
Puerto serie estándar	X	X	Placa del sistema	n/d	Seleznable en base a la velocidad del reloj del generador de la velocidad en baudios del receptor y el transmisor asíncrono universal (UART).	Característica estándar
RAN 232	X	X		8130	57,6	Posibilidad remota

Tabla 96. Productos de comunicación asíncrona (continuación)

Conexión asíncrona	Basado en el procesador POWER	Basado en Itanium	Tipo de bus	Código de característica o tipo de máquina (modelo)	Velocidad de datos máxima por puerto (kbps)	Características destacables
RAN 232 ampliado	X	X		8137	230	Posibilidad remota
RAN EIA 422 de 16 puertos	X	X		8138	230	Posibilidad remota
Controlador de 128 puertos	X			8128	230	Eficacia, número máximo de dispositivos más alto
Controlador de 128 puertos	X			2933	230	Eficacia, número máximo de dispositivos más alto
Controlador de 128 puertos	X	X	PCI	2944	230	Eficacia, número máximo de dispositivos más alto

**Nota:** RAN de montaje en bastidor es el 8136.

**Nota:** La velocidad de datos máxima por puerto está limitada por el ancho de banda (1,2 Mbps para el RAN estándar, o 2,4 Mbps para el RAN avanzado).

La primera característica de este tabla representa los puertos serie conectados a la placa estándares de cada unidad del sistema. Las siguientes características son los adaptadores. El subsistema asíncrono de 128 puertos incluye los nodos asíncronos remotos (RAN) que se conectan al mismo.

#### Puertos asíncronos conectados a la placa

La mayoría de los modelos de la unidad del sistema tienen dos puertos serie asíncronos integrados (estándares) EIA 232. Los dispositivos serie asíncronos EIA 232 pueden conectarse directamente a los puertos serie estándares utilizando cables serie estándares con conectores de shell D de 9 patillas.

Algunos sistemas de varios procesadores tienen un tercer puerto serie que se utiliza para la comunicación con el centro de servicio remoto.

**Nota:** Los sistemas basados en Itanium tienen uno o dos puertos serie integrados. Los modelos de estación de trabajo inicial tienen un puerto, mientras que los modelos de clase de servidor inicial tienen dos.

#### Puertos asíncronos conectados al adaptador

Cada uno de los adaptadores requiere una ranura de bus y sólo puede utilizarse en los sistemas que proporcionan soporte al tipo de bus necesario.

Los adaptadores ISA de 8 puertos y de 128 puertos y los adaptadores PCI de 8 puertos son adaptadores inteligentes que proporcionan una descarga significativa del procesador del sistema principal.

EIA 232 es el estándar de comunicaciones más común pero también se proporciona soporte a EIA 422A (utilizado cuando se necesita una distancia de cable superior). La implementación de EIA 422A no incluye la función de detección del estado del dispositivo ni las señales de control de módem RS 232.

**Nota:** La plataforma basada en Itanium sólo proporciona soporte a los adaptadores de PCI de 8 puertos y de 128 puertos.

### Puertos asíncronos conectados a nodos

El adaptador de 128 puertos, disponible para el bus Micro Channel, ISA o PCI, permite conectar entre uno y ocho nodos asíncronos remotos (RAN).

Cada RAN tiene 16 puertos asíncronos para conectar los dispositivos que son unidades con alimentación independiente. En las tarjetas de adaptadores de 128 posibles es posible conectar en margarita hasta cuatro RAN. Los RAN pueden proporcionar soporte a 16 dispositivos EIA 232 o a 16 dispositivos EIA 422. El controlador de 128 puertos es un adaptador inteligente que aumenta el número de sesiones asíncronas posibles a un determinado nivel de utilización de la CPU.

A continuación se muestran las características adicionales de la opción de 128 puertos:

- Para mantener el nivel de rendimiento máximo, los RAN pueden situarse hasta 300 metros del procesador del sistema y deben utilizar cableado apantallado de 8 hilos.
- La distancia puede ampliarse hasta los 1200 metros si se reduce la velocidad de los datos entre los RAN y el procesador del sistema.
- Los RAN pueden encontrarse remotamente al procesador del sistema utilizando un módem síncrono EIA 232 o EIA 422. En cada conexión en margarita de cuatro RAN sólo se permite un par de módems en cualquier punto de la cadena.
- El rendimiento del sistema experimentará una mejora si se descarga del procesador del sistema el proceso de caracteres de tty.

## Consideraciones para la selección de un producto

El producto asíncrono adecuado a menudo depende de una situación determinada.

Las preguntas siguientes lo ayudarán a seleccionar los productos que necesita instalar.

### Posibilidades de ampliación

- ¿Cuántos puertos asíncronos se necesitan?
- ¿Cuántos puertos se necesitarán en el futuro?

### Topología

- ¿Los dispositivos se hallarán en otros edificios o en ubicaciones remotas?
- ¿Dónde se realizará la administración del sistema/de la red?
- ¿Existe un clúster HACMP?
- ¿Qué tipo de cableado es necesario o ya existe?

### Rendimiento

- ¿La aplicación utiliza la CPU intensamente?
- ¿Qué tipos de dispositivos se conectarán?
- ¿Cuál es la demanda relativa de ancho de banda asíncrono para la suma agregada de los dispositivos?

Tabla 97. Demanda relativa de ancho de banda de los dispositivos

Demanda baja	Demanda moderada	Demanda elevada
Terminales ASCII, terminales de punto de venta, módems asíncronos	Impresoras, faxes/módems de baja velocidad, escáneres de códigos de barras	Terminales X serie, faxes/módems de alta velocidad, impresoras de alta velocidad, aplicaciones de transferencia de archivos

### Requisitos de la interfaz del dispositivo

- ¿Qué interfaz asíncrona se requiere, por ejemplo, EIA 232, EIA 422A, EIA 423?

¿Los dispositivos o las aplicaciones necesitan la interfaz EIA 232 en su totalidad?

## Seguridad

¿Se necesita el kernel de seguridad del sistema (SAK)? (sólo para los puertos conectados en placa)

La tabla siguiente muestra las características detalladas de los productos.

Tabla 98. Características de los productos de conexión asíncrona				
Características	Puertos serie nativos	PCI de 2 puertos	PCI de 8 puertos	PCI de 128 puertos con RAN
Número de puertos asíncronos por adaptador	n/d	2	8	128
Número máximo de adaptadores	n/d	sin límite	20	20
Número máximo de puertos asíncronos	2 o 3	2	160	2560
Número de puertos asíncronos por RAN	n/d	n/d	n/d	16
Número máximo de RAN	n/d	n/d	n/d	160
Velocidad máxima (Kbits/seg)	Seleznable en base a la velocidad del reloj del generador de la velocidad en baudios de UART.	230	230	230
Método de conexión	placa	directa	directa	nodo
Interfaces eléctricas asíncronas soportadas	EIA 232	EIA 232	EIA 232 EIA 422A	EIA 232 EIA 422
Conektor estándar	DB9	DB9	DB25M	RJ-45 (de 10 patillas o de 8 patillas)
Opciones del cable DB25	n/d	n/d	n/d	RJ-45-DB25
Opción de montaje en bastidor	n/d	n/d	n/d	sí
Fuente de alimentación	n/d	n/d	n/d	externa
Señales soportadas (EIA 232)	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI

## Aplicaciones de adaptadores asíncronos

Cada producto que se ofrece está caracterizado por un caso representativo donde comprobar sus puntos fuertes. Los adaptadores de este tema se listan junto con sus especificaciones para que puede seleccionar para cada caso concreto.

Item	Descripción
Bus PCI de 2 puertos EIA 232	<ul style="list-style-type: none"> <li>• Ranura de PCI disponible.</li> <li>• Hasta dos puertos por adaptador.</li> <li>• Necesita todos los puertos EIA 232.</li> <li>• Velocidades asíncronas de hasta 230 Kbps.</li> </ul>

Item	Descripción
Bus PCI de 8 puertos EIA 232/EIA 422	<ul style="list-style-type: none"> <li>Ranura de PCI disponible.</li> <li>Se necesitan menos de ocho puertos con escasa o ninguna ampliación.</li> <li>Requiere todos los puertos EIA 232, todos EIA 422 o una combinación de puertos EIA 232 y EIA 422.</li> <li>Interrupción de carácter de descarga y proceso de E/S de terminal de la CPU principal.</li> <li>Velocidades asíncronas de hasta 230 Kbps.</li> <li>Rendimiento máximo para los módems de alta velocidad (33,6 Kbps) con compresión de datos.</li> </ul>
Adaptador de 128 puertos (PCI)	<ul style="list-style-type: none"> <li>Disponible una ranura de bus Micro Channel, ISA o PCI. (Para obtener más información sobre Micro Channel o ISA, consulte el apartado <a href="#">“Adaptador de 128 puertos (Micro Channel, ISA)”</a> en la página 762).</li> <li>Dieciséis puertos que ahora pueden ampliarse a hasta 128 puertos sin ranuras adicionales.</li> <li>Terminal más distante situado a unos 90 metros (300 pies) del sistema a una velocidad de datos máxima de 230 Kbps.</li> <li>Terminales planificados: cercanos o en la instalación, distantes en la instalación o remotos.</li> <li>Se necesita un elevado rendimiento asíncrono con baja demanda del procesador.</li> <li>Se necesita la posibilidad de una impresora conectada al terminal.</li> <li>Se necesita conectar a las instalaciones remotas a través de módems síncronos o de fibra óptima.</li> </ul>

### Ejemplos de soluciones asíncronas

Los ejemplos de clientes indicados a continuación se solucionaron con un controlador PCI de 8 puertos y un controlador asíncrono de 128 puertos.

Item	Descripción
Oficina inmobiliaria	<ul style="list-style-type: none"> <li>La simplicidad y los costes son la máxima prioridad.</li> <li>Sistema operativo y servidor.</li> <li>Entre seis y diez dispositivos conectados al servidor con acceso a la base de datos.</li> <li>Una ranura está disponible para la comunicación asíncrona.</li> <li>Los dispositivos se encuentran a menos de 61 metros (200 pies) del servidor.</li> </ul> <p><b>Solución:</b></p> <p>PCI de 8 puertos.</p>

Item	Descripción
Punto de venta al por menor	<ul style="list-style-type: none"> <li>El coste por asiento es la máxima prioridad.</li> <li>Sistema operativo y servidor.</li> <li>20 o más terminales ASCII: por ejemplo, registros de caja.</li> <li>Una ranura está disponible para la comunicación asíncrona.</li> <li>Está prevista la futura ampliación de terminales adicionales.</li> </ul> <p><b>Solución:</b> Controlador asíncrono de 128 puertos con dos RAN. Futura ampliación con RAN adicionales.</p>

## Consideraciones topológicas

La familia de adaptadores asíncronos ofrece una amplia gama de opciones en lo que respecta a la topología a distancia.

La longitud máxima de los cables de los adaptadores de placa y de conexión directa suele ser la distancia entre el puerto y el dispositivo asíncrono para que funcionen a la velocidad de datos máxima que se haya especificado. El adaptador del puerto 128 se mide desde la tarjeta del adaptador al RAN conectado en margarita al mismo. Con el puerto 128, es posible conseguir efectivamente distancias ilimitadas utilizando los módems asíncronos EIA 422 que conectan los RAN al adaptador.

El cableado correcto es extremadamente importante y es exclusivo para cada entorno.

## Comunicación serie

A continuación se describen los estándares, el hardware, la terminología y los conceptos de la comunicación asíncrona.

Los puertos serie se utilizan para conectar físicamente los dispositivos asíncronos con un sistema. Se encuentran en la parte de atrás de la unidad del sistema, integrados o utilizando un adaptador de varios puertos como, por ejemplo, los adaptadores asíncronos de 2 puertos, 8 puertos, 16 puertos y 128 puertos.

**Nota:** Los puertos del sistema integrados POWER5 no son puertos serie con finalidad general y funciones completas. Consulte el apartado [“Diferencias funcionales entre los puertos del sistema y los puertos serie”](#) en la página 666 para obtener más información.

Para comprender el funcionamiento de un puerto serie, es necesario examinar primero las comunicaciones paralelo. Un puerto paralelo estándar utilizar ocho conectores o cables para transmitir los bits de datos de forma simultánea, formando un solo carácter. La ilustración siguiente muestra la transmisión en paralelo de la letra a.

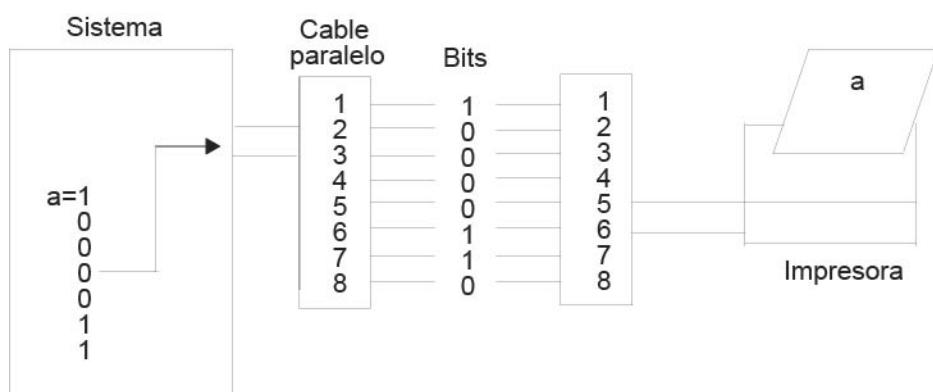


Figura 29. Puerto de comunicaciones paralelo

Los puertos serie requieren un solo conector, o cable, para enviar el mismo carácter de datos al dispositivo. Para conseguirlo, los datos se convierten del formato paralelo (enviado por el sistema), a formato secuencial, en el que los bits se organizan uno tras otro en una serie. Los datos se transmiten entonces al dispositivo, enviando el bit menos significativo (o el bit cero) en primer lugar. Una vez que el dispositivo remoto recibe los datos, éstos se vuelven a convertir al formato paralelo. La ilustración siguiente muestra la transmisión serie de la letra a.

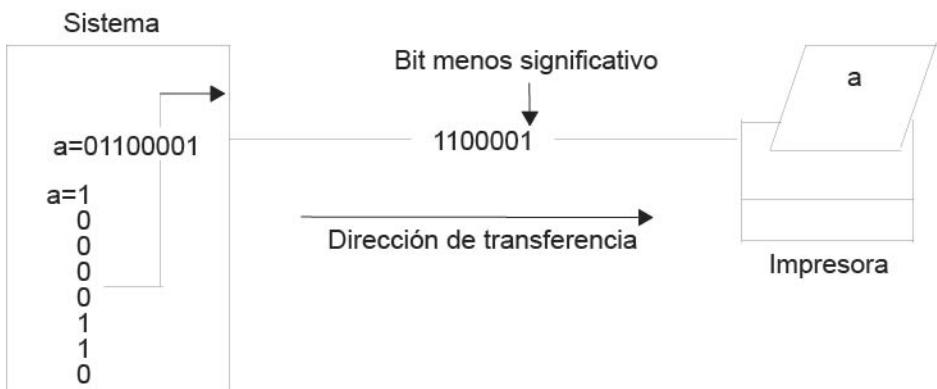


Figura 30. Puerto de comunicaciones serie

Las transmisiones serie de un solo carácter son simples y directas; sin embargo, surgen complicaciones cuando se transmiten en series un gran número de caracteres tal como se muestra en la ilustración siguiente. El sistema receptor no sabe cuándo finaliza un carácter y empieza el otro. Para solucionar este problema, ambos extremos del enlace de comunicación deben estar sincronizados o temporizados.



Figura 31. Transmisión serie

### Diferencias funcionales entre los puertos del sistema y los puertos serie

Los *puertos de sistema* integrados de POWER5 son parecidos a los puertos serie, con la salvedad de que los puertos del sistema solo están disponibles para funciones que reciben un soporte específico.

Los puertos del sistema se inhabilitan cuando un puerto de la Consola de gestión de hardware (HMC) se conecta a una HMC. Pueden utilizarse los puertos HMC o los puertos del sistema, pero no ambos.

Aunque no haya conectada ninguna HMC, los puertos del sistema integrados están limitados al funcionamiento de la consola TTY conectada en serie. Sólo funcionan correctamente con los módems de llamada al centro de soporte, los terminales asíncronos y ciertos UPS. La conexión de cualquier otro dispositivo serie (incluidas las conexiones de sistema a sistema para HACMP) requiere un adaptador de puerto serie en una ranura de PCI.

### Sincronización

La sincronización es el proceso de temporización de la transmisión serie para identificar los datos que se envían correctamente.

Las dos modalidades más frecuentes son la síncrona y la asíncrona.

### Transmisión síncrona

El término *síncrona* se utiliza para describir una transferencia de bloques de datos con una temporización continua y coherente.

Estos tipos de conexiones se utilizan cuando deben transferirse grandes cantidades de datos con gran rapidez desde una ubicación a la otra. La velocidad de la conexión síncrona se consigue transfiriendo datos en grandes bloques en lugar de caracteres individuales.

Los bloques de datos se agrupan y espacian a intervalos regulares y van precedidos por caracteres especiales denominados caracteres desocupados síncronos o syn. Vea la ilustración siguiente.



Figura 32. Transmisión síncrona

Una vez el dispositivo remoto ha recibido los caracteres syn, éstos se decodifican y utilizan para sincronizar la conexión. Cuando la conexión se ha sincronizado correctamente, la transmisión de datos puede empezar.

Este tipo de datos se sería análoga a la transmisión de un documento de texto grande. Antes de transferir el documento a través de la línea síncrona, éste se divide primero en bloques de frases y párrafos. Los bloques se envían entonces al sitio remoto a través del enlace de comunicaciones. Con otras modalidades de transmisión, el texto se organiza en largas series de letras (o caracteres) que forman las palabras de las frases y párrafos. Estos caracteres se envían a la vez a través del enlace de comunicaciones y vuelven a recopilarse en la ubicación remota.

La temporización necesaria para las conexiones síncronas se obtiene de los dispositivos que se encuentran en el enlace de comunicaciones. Todos los dispositivos del enlace síncrono deben establecerse siguiendo la misma temporización.

A continuación se muestra una lista de las características específicas de la comunicación síncrona:

- No hay espacios entre los caracteres que se transmiten.
- La temporización la proporcionan los módems u otros dispositivos en cada extremo de la conexión.
- Los datos transmitidos van precedidos por caracteres syn especiales.
- Los caracteres syn se utilizan entre bloques de datos con fines de temporización.

### Transmisión asíncrona

El término *asíncrona* se utiliza para describir el proceso en el que los datos transmitidos se codifican con bits de inicio y de detención, que especifican el principio y el final de cada carácter.

En la figura siguiente se muestra un ejemplo de transmisión asíncrona.

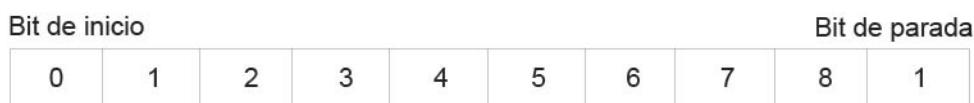


Figura 33. Transmisión asíncrona

Estos bits adicionales proporcionan la temporización o sincronización para la conexión e indican cuándo se ha enviado o recibido un carácter completo; así pues, la temporización de cada carácter empieza con el bit de inicio y finaliza con el bit de parada.

Cuando aparecen huecos entre las transmisiones de los caracteres, se dice que la línea asíncrona se encuentra en un estado de marca. Una marca es un 1 binario (o un voltaje negativo) que se envía durante los períodos de inactividad de la línea, tal como se muestra en la figura siguiente.

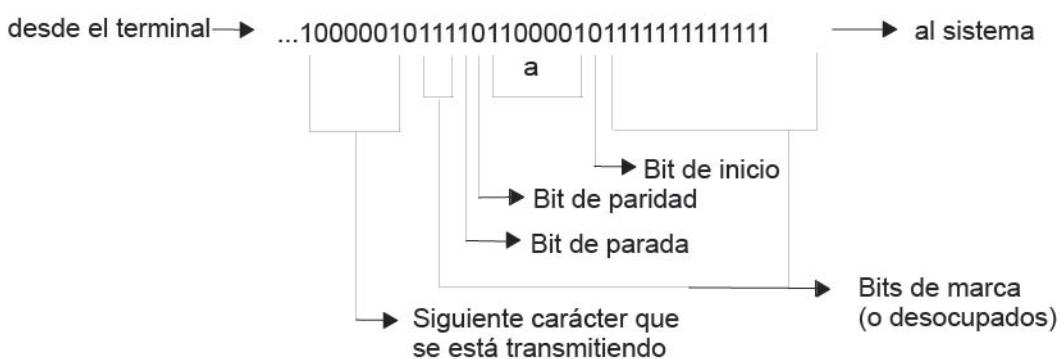


Figura 34. Bits de marca (desocupados) de la corriente de datos

Cuando el estado de marca se ve interrumpido por un voltaje positivo (un 0 binario), el sistema destinatario sabe que van a llegar caracteres de datos. Por este motivo, el bit de inicio, que precede el carácter de datos, siempre es un bit de espacio (un 0 binario) y el bit de parada, que señala el final de un carácter, siempre es un bit de marca (un 1 binario).

A continuación se muestra una lista de las características específicas de la comunicación asíncrona:

- Cada carácter va precedido por un bit de inicio y seguido por uno o más bits de parada.
- Puede haber huecos o espacios entre los caracteres.

### Parámetros de comunicación serie

Entre los parámetros utilizados durante la comunicación serie se encuentran bits por carácter, bits por segundo (bps), velocidad en baudios, paridad y bits de inicio, detención y marca.

#### **Bits por carácter**

El número de bits por carácter (bpc) indica el número de bits utilizado para representar un solo carácter de datos durante la comunicación serie.

Este número no refleja la cantidad total de bits de paridad, parada o inicio que se incluyen con el carácter. Los valores posibles para bpc son 7 y 8.

Cuando se utiliza el valor de siete bits por carácter, es posible enviar solamente los 128 primeros caracteres (0-127) del juego de caracteres ASCII estándar. Cada uno de estos caracteres está representado por siete bits de datos. El valor de ocho bits por carácter debe utilizarse para enviar el juego de caracteres ASCII ampliado (128-255). Cada uno de estos caracteres sólo puede representarse utilizando ocho bits de datos.

#### **Bits por segundo (bps)**

Proporciona una descripción de las estadísticas de bits por segundo.

Bits por segundo (bps) es el número de bits de datos (unos y ceros binarios) que se transmiten por segundo a través de la línea de comunicaciones.

#### **Velocidad en baudios**

La velocidad en baudios es el número de veces por segundo que una señal de comunicaciones serie cambia de estado; el estado puede ser un nivel de voltaje, una frecuencia o un ángulo de fase de frecuencia.

Si la señal cambia una vez para cada bit de datos, entonces un bps equivale a un baudio. Por ejemplo, un módem a 300 baudios cambia de estado 300 veces por segundo.

#### **Bits de paridad**

El bit de paridad, a diferencia de los bits de inicio y de parada, es un parámetro opcional que se utiliza en las comunicaciones serie para determinar si el dispositivo remoto está recibiendo correctamente el carácter de datos que se transmite.

Bit de inicio									Bit de parada
0	1	2	3	4	5	6	7	8 o paridad	1

Figura 35. Paridad

El bit de paridad puede tener una de las cinco especificaciones siguientes:

Item	Descripción
ninguna	Especifica que el sistema local no debe crear un bit de paridad para los caracteres de datos que se están transmitiendo. También indica que el sistema local no comprueba el bit de paridad de los datos recibidos de un sistema principal remoto.

Item	Descripción
par	Especifica la suma del número total de unos binarios de un solo carácter es un valor par. En caso negativo, el bit de paridad debe ser un 1 para asegurarse de que el número total de unos binarios sea par.  Por ejemplo, si la letra a (1100001 binario) se transmite bajo la paridad par, el sistema de envío suma el número de unos binarios que, en este caso, es tres y deja el bit de paridad en un 1 para mantener un número par de unos binarios. Si la letra A (1000001 binario) se transmite bajo las mismas circunstancias, el bit de paridad sería un 0, por lo que el número total de unos binarios se mantendría como un número par.
impar	Funciona bajo las mismas directrices que la paridad par, con la excepción de que el número total de unos binarios debe ser un número impar.
espacio	Especifica que el bit de paridad siempre será un cero binario. Otro término utilizado para la paridad de espacio es relleno de bits, que se deriva de su utilización como rellenador de los datos de siete bits que se transmiten a un dispositivo que sólo acepte datos de ocho bits. Estos dispositivos interpretan el bit de paridad de espacio como un bit de datos adicional para el carácter transmitido.
marca	Funciona bajo las mismas directrices que la paridad de espacio, con la excepción de que el bit de paridad siempre es un 1 binario. El bit de paridad de marca sólo actúa como rellenador.

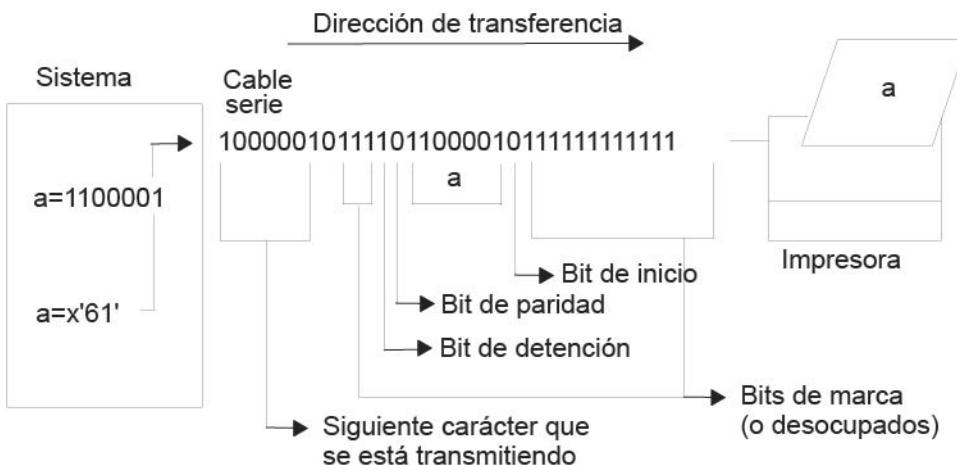
## *Bits de inicio, parada y marca*

Los bits de inicio y de parada se utilizan en la comunicación asíncrona con el fin de temporizar la sincronización de los caracteres de datos que se transmiten.

Sin la utilización de estos bits, los sistemas emisores y receptores no sabrán dónde termina un carácter y empieza el siguiente.

Otro bit que se utiliza para separar caracteres de datos durante la transmisión es el bit RS de marca (o desocupado). Este bit, un 1 binario, se transmite cuando la línea de comunicaciones está desocupada y no se está enviando o recibiendo ningún carácter.

Cuando el sistema recibe un bit de inicio (binario 0), se entiende que un número fijo del bit de carácter (determinado por el parámetro **bits per character**), e incluso un bit de paridad (determinado por el parámetro **parity**), sigue al bit de inicio. A continuación, el sistema recibe un bit de parada (binario 1). En el ejemplo siguiente está presente el bit de **parity** y el **bits per character** es 7.



*Figura 36. Bits de inicio, parada y marca*

## **El estándar EIA 232D**

El estándar EIA 232D se desarrolló en 1.969 para especificar las conexiones entre un sistema y un módem.

El propio término es un acrónimo que puede leerse de la forma siguiente:

Electronics Industry Association (EIA) accepted standard, ID number 232 revision D (Estándar aceptado de la asociación de la industria electrónica, número de ID 232 revisión D)

EIA 232D especifica las características de las conexiones físicas y eléctricas entre dos dispositivos. Es necesario asignar nombres y abreviaturas a cada patilla o cable para la comunicación serie como, por ejemplo:

Tabla 99. Conexiones EIA 232D			
Señal	Tipo de equipo	Símbolo	Patilla
Transmitir datos	DCE	TxD	2
Recibir datos	DTE	RxD	3
Petición a enviar	DCE	RTS	4
Borrar para enviar	DTE	CTS	5
Conjunto de datos preparado	DTE	DSR	6
Señal de toma de tierra		SG	7
Detección de portadora	DTE	CD	8
Terminal de datos preparado	DCE	DTR	20
Indicador de llamada	DTE	RI	22

En EIA 232D, a los dispositivos que utilizan la patilla 2 (TxD) para la salida (por ejemplo, los sistemas y las terminales) se les proporciona el equipo de terminal de datos (DTE) de nombre. A los dispositivos que utilizan la patilla 2 (TxD) para la entrada (por ejemplo, los módems) se les proporciona el equipo de comunicación de datos (DCE) de nombre.

EIA 232D también especifica los conectores. Un dispositivo DTE suele tener conectores macho mientras que los dispositivos DCE tienen conectores hembra. Los fabricantes no siempre cumplen este estándar; por lo tanto, los usuarios siempre deben revisar la documentación del dispositivo antes de conectar los cables.

### Métodos de comunicación asíncrona

Describe las dos formas de comunicación asíncrona, de una vía o de dos vías (donde se incluye la modalidad dúplex y semi-dúplex).

Simplex, o comunicación de una vía, es la forma de conexión más sencilla entre los dos dispositivos. Esta modalidad de comunicación permite la transmisión de datos en una dirección solamente y sólo requiere la conexión de dos líneas como, por ejemplo, TxD (o RxD) y SG.

Existen dos formas de comunicación de dos vías: semi-dúplex y dúplex. Una conexión en modalidad semi-dúplex permite que los datos se transmitan en dos direcciones, pero no de forma simultánea. La modalidad semi-dúplex sería similar a la utilización de una radio CB donde la comunicación de dos vías es posible pero sólo una persona puede hablar cada vez.

En modalidad dúplex, la comunicación de datos puede realizarse en dos direcciones de forma simultánea. La modalidad dúplex sería similar a una conversación telefónica en la que ambas personas hablan al mismo tiempo.

### Control de flujo

El dispositivo serie necesita cierto tipo de control de flujo de datos para limitar la cantidad de datos que el sistema transmite.

Los dispositivos serie como, por ejemplo, las impresoras y los módems, no procesan los datos con la misma rapidez y eficacia que los sistemas a los que están conectados.

El término *control de flujo* se utiliza para describir el método en el que un dispositivo serie controla la cantidad de datos que se transmiten al mismo.

### **Flujo de hardware RTS/CTS**

La petición de enviar/borrar para enviar (RTS/CTS) a veces se llama reconocimiento de hardware o ritmo en lugar de control de flujo.

El término reconocimiento de hardware viene de la utilización de cables y voltajes como un método para el control de transmisión de datos. A diferencia de XON/XOFF, que envía caracteres de control en la serie de datos, RTS/CTS utilice voltajes positivos y negativos junto con patillas o hilos dedicados en el cableado del dispositivo.

Un voltaje positivo significa que se permite la transmisión de datos y un voltaje negativo significa que la transmisión de datos debe suspenderse.

### **Flujo de hardware DTR/DSR**

Terminal de datos preparado (DTR), otra forma de control de flujo de hardware, suelen generarla los dispositivos como, por ejemplo, las impresoras, para indicar que están preparados para comunicarse con el sistema. Esta señal se utiliza junto con Conjunto de datos preparado (DSR) que el sistema genera para controlar el flujo de datos.

Un voltaje positivo significa que se permite la transmisión de datos y un voltaje negativo significa que la transmisión de datos debe suspenderse.

### **Flujo de software XON/XOFF**

Los controles de flujo transmisor activado/transmisor desactivado (XON/XOFF) implican el envío de caracteres de control de transmisión de datos junto con la serie de datos (Tx y Rx). Por este motivo, se denomina control de flujo de software.

Cuando se envían datos a un módem, éstos se colocan en un almacenamiento intermedio. Justo antes de que el almacenamiento intermedio alcance la capacidad máxima, el módem enviará un carácter XOFF al sistema y el sistema dejará de transmitir los datos. Cuando el almacenamiento intermedio del módem esté casi vacío y listo para recibir más datos, volverá a enviar un carácter XON al sistema, lo que provocará que se envíen más datos.

### **Configuración de un puerto para el reconocimiento del hardware RTS/CTS**

Se recomienda que los módems conectados al servidor que funcionen a una velocidad de 9600 o superior utilicen el reconocimiento de hardware RTS/CTS en lugar del control de flujo XON/XOFF.

Con ello se evitará el desbordamiento del almacenamiento intermedio de un sistema con recursos limitados. RTS no es un valor predeterminado en ningún puerto tty y el administrador del sistema debe establecerlo correspondientemente.

#### **Prerrequisitos**

Para RTS/CTS debe utilizarse un cable de por lo menos cinco hilos.

Para habilitar RTS/CTS para un puerto, siga los pasos siguientes:

1. Utilice la vía rápida smit tty.
2. Seleccione **Cambiar/Mostrar características de un TTY**.
3. Seleccione el tty en el que RTS/CTS debe habilitarse.
4. Establezca el campo CONTROL DE FLUJO a utilizar en **rts**.
5. Seleccione **Do**.
6. Salga de SMIT.

### **Dispositivo de terminal TTY**

Un dispositivo de terminal tty es un dispositivo de caracteres que realiza la entrada y la salida de carácter en carácter.

La comunicación entre los dispositivos de terminal y los programas que los leen y escriben está controlada por la interfaz tty. Entre los ejemplos de dispositivos tty se encuentran:

- Módems
- Terminales ASCII
- Consola del sistema (LFT)
- **aixterm** bajo AIXwindows

Los dispositivos tty pueden añadirse, suprimirse, listarse y modificarse como cualquier otro dispositivo en el sistema utilizando la herramienta SMIT o los mandatos específicos del dispositivo.

#### **Valores de TERM para distintos terminales y pantallas**

La información acerca de las posibilidades de los terminales se almacena en la base de datos **terminfo**.

El valor de la variable de entorno TERM identifica la descripción de un terminal en concreto de la base de datos **terminfo**. Proporciona toda la información que un programa necesita para comunicarse de forma eficaz con el dispositivo de tty actual.

<i>Tabla 100. Valores de TERM para distintos terminales</i>	
<b>Terminal/pantalla</b>	<b>Valor</b>
Terminal ASCII 3161	ibm3161
Terminal ASCII 3163	ibm3161
DEC VT100 (terminal)	vt100
DECVT220	vt220
Estación de pantalla ASCII 3151 con cartucho o Estación de pantalla ASCII 3161 con cartucho	ibm3161-C
Estación de pantalla ASCII 3162	ibm3161
Estación de pantalla ASCII 3162 con cartucho	ibm3162
Pantalla 6091	lft
AIXwindows	aixterm

Para obtener información sobre las entradas en la base de datos **terminfo**, consulte el formato de archivo **terminfo**. Para convertir las entradas **termcap** en **terminfo**, consulte el mandato **captioninfo**. (El archivo **termcap** contiene las descripciones de los terminales para los sistemas Berkeley anteriores.)

#### **Características del TTY**

La *disciplina de línea* proporciona la interfaz de usuario independiente del hardware para la comunicación entre el sistema y un dispositivo asíncrono.

Por ejemplo, un usuario puede borrar una sola línea o interrumpir un proceso que esté en ejecución actualmente escribiendo una secuencia de caracteres determinada. Puede definir el significado de estas secuencias de caracteres así como establecer otras características de los terminales como, por ejemplo, la velocidad de la comunicación, utilizando el mandato **chdev**, la herramienta System Management Interface Tool (SMIT) o el mandato **stty**.

#### **Requisitos del dispositivo TTY conectado**

Una comunicación correcta entre el sistema principal y un dispositivo tty conectado debe cumplir los requisitos siguientes:

- Una cable de conexiones conectado correctamente
- Valores de comunicaciones que coincidan (velocidad de la línea, tamaño de los caracteres, paridad, bit de parada e interfaz) entre el sistema principal y el dispositivo tty conectado.

#### **Gestión de dispositivos de TTY**

Aquí pueden consultarse las tareas de gestión de dispositivos y los mandatos y las vías rápidas de SMIT asociados a las mismas.

Tabla 101. Gestión de las tareas de dispositivos de TTY

Tarea	Vía rápida de SMIT	Mandato o archivo
Lista de los dispositivos de TTY definidos	smit lsdtty	<b>lsdev -C -c tty -H</b>
Añadir un TTY	smit mktty	<b>mkdev -t tty</b> <sup>1,2</sup>
Mover un TTY a otro puerto <sup>3</sup>	smit movtty	<b>chdev -l Nombre -p NombrePadre -w UbicaciónConexión</b> <sup>2,4</sup>
Cambiar/Mostrar las características de un TTY	smit chtty	<b>lsattr -l Nombre -E</b> (para mostrar); <b>chdev -l Nombre</b> (para cambiar) <sup>4,5</sup>
Eliminar un TTY <sup>3</sup>	smit rmtty	<b>rmdev -l Nombre</b>
Configurar un TTY definido (Dejar disponible para su utilización)	smit mktty	<b>mkdev -l Nombre</b>

**Nota:**

1. Pueden especificarse otros distintivos para especificar el dispositivo de tty nuevo con mayor detalle. Por ejemplo, para definir y configurar un dispositivo de tty RS-232 conectado al puerto 0 del adaptador asíncrono de 8 puertos sa3 con el atributo speed (velocidad) establecido en 19200 y otros atributos establecidos en los valores recuperados desde el archivo foo:
 

```
mkdev -t tty -s rs232 -p sa3 -w 0 -a speed=19200 -f foo
```
2. Los mandatos **mkdev** y **chdev** proporcionan soporte a opciones no permitidas con SMIT.
3. Inhabilite el tty antes de realizar esta tarea. Consulte el mandato **pdisable**.
4. Utilice los distintivos para cambiar características sobre un tty desde la línea de mandatos.
5. Puede seleccionar una velocidad en baudios Posix en la función de lista o escribirla directamente en el campo como velocidad en baudios no Posix. Si el hardware del módem no puede proporcionar soporte a la velocidad en baudios seleccionada, el sistema visualiza un mensaje de error.

Si añade o modifica un tty desde la línea de mandatos, consulte la lista siguiente para averiguar el nombre de *atributo* que debe especificarse en el distintivo **-a atributo=valor** para la característica que desee establecer. Por ejemplo, especifique **-a speed=valor** para establecer la velocidad en baudios de un dispositivo de tty.

Tabla 102. Atributos TTY

Características	Nombre del atributo
Habilitar INICIO DE SESIÓN	login
Velocidad en BAUDIOS	speed
PARIDAD	paridad
BITS por carácter	bpc
Número de BITS de PARADA	stops
TIEMPO antes de avanzar a la siguiente definición de puerto	timeout
Reconocimiento XON-XOFF	xon
Tipo de TERMINAL	term
CONTROL DE FLUJO a utilizar	flow_disp

Tabla 102. Atributos TTY (continuación)

Características	Nombre del atributo
DISCIPLINA DE APERTURA a utilizar	open_disp
Atributos STTY para EJECUCIÓN	runmodes
Atributos STTY para INICIO DE SESIÓN	logmodes
EJECUTAR gestor de actividad de shell	shell
Nombre INICIADOR DE SESIÓN	logger
ESTADO de dispositivo en el ARRANQUE	autoconfig
Número total de almac. intermedios de TRANSMISIÓN	tbc
Nivel desencadenante de RECEPCIÓN	rtrig
Módulos STREAMS a activar al ABRIR	modules
Archivo de correlaciones de ENTRADA	imap
Archivo de correlaciones de SALIDA	omap
Archivo correlaciones CODESET	csmap
Carácter de INTERRUPCIÓN	intr
Carácter de ABANDONAR	quit
Carácter de BORRAR	erase
Carácter KILL	kill
Carácter de FIN DE ARCHIVO	eof
Carácter de FIN DE LÍNEA	eol
Carácter de 2º FIN DE LÍNEA	eol2
Carácter de RETARDO DE SUSPENDER EL PROCESO	dsusp
Carácter de SUSPENDER EL PROCESO	susp
Carácter de LITERAL SIGUIENTE	lnext
Carácter de ARRANCAR	inicio
Carácter de DETENER	parada
Carácter de BORRAR PALABRA	werase
Carácter de VOLVER A IMPRIMIR LÍNEA	reprint
Carácter de ELIMINAR	discard

### Resolución de problemas en TTY

Existen varias situaciones frecuentes para la resolución de problemas en TTY.

Entre las situaciones frecuentes de resolución de problemas en TTY se incluyen los errores de Reejecución con demasiada rapidez, puertos de TTY colgados y archivos de registro cronológico de errores, mandatos y mensajes de comunicación de errores comunes.

## **Errores de reejecución con demasiada rapidez**

El sistema registra el número de procesos **getty** creados para un tty en concreto durante un breve período de tiempo. Si el número de procesos **getty** creados en este período de tiempo es superior a 5, en la consola se visualiza el error **Reejecución con demasiada rapidez** y el sistema inhabilita el puerto.

El tty permanece inhabilitado durante 19 minutos aproximadamente o hasta que el administrador del sistema vuelva a habilitarlo. Una vez transcurridos los 19 minutos, el sistema habilita el puerto automáticamente, lo que provoca la creación de un nuevo proceso **getty**.

Entre las causas posibles se encuentran las siguientes:

- Una configuración incorrecta del módem
- Un puerto está definido y habilitado pero no tiene conectado ningún cable o dispositivo
- Cables defectuosos o conexiones sueltas
- Ruidos en la línea de comunicaciones
- Corrupción o manipulación de los archivos `/etc/environment` o `/etc/inittab`
- La configuración del tty está dañada
- El hardware es defectuoso

De los procedimientos de recuperación siguientes, utilice el que sea aplicable a su situación.

- Configuración incorrecta del módem:

Asegúrese de que la detección de la portadora del módem *no* se haya forzado como alta.

**Nota:** Lo siguiente es aplicable a los módems compatibles con Hayes

1. Conecte el módem y examine el perfil activo.
2. Establezca la detección de la portadora del módem en **&C1** en vez de en **&C0** (forzada alta). Utilice los mandatos de módem AT siguientes para establecer y modificar el atributo de la portadora:

```
AT&C1  
AT&W
```

### **Nota:**

- a. Consulte el apartado “Envío de mandatos AT con el mandato cu” en la página 689
- b. Consulte la documentación del módem si desea información adicional.

- Inhabilite el tty, elimine la definición del tty o conecte un dispositivo al puerto:

- Para inhabilitar la definición del tty utilice el mandato **chdev** de la forma siguiente:

```
chdev -l nombretty -a Login=disable
```

Después de ejecutar este mandato, el tty *no* se habilita cuando se reinicia el sistema.

- Para eliminar la definición del tty:

1. Inhabilite el puerto del tty, utilice el mandato **pdisable** y escriba:

```
pdisable nombretty
```

2. Elimine la definición del tty del sistema. Consulte el apartado “Gestión de dispositivos de TTY” en la página 672 si desea información adicional.

- Compruebe si hay cables defectuosos o conexiones sueltas:

1. Compruebe el cableado. Apriete las conexiones sueltas y sustituya los conectores dañados o inadecuados.
  2. Verifique que el cableado sospechoso sea cable serie de IBM N/P 6323741 o que el cable cumpla el mismo estándar. Sustituya los cables dañados o inadecuados.
- Elimine los ruidos de la línea de comunicaciones:

1. Verifique que el cableado tenga la longitud y la impedancia correctas.
2. Asegúrese de que en los cables más largos haya colocadas arandelas de toroide en los lugares necesarios.
3. Compruebe el direccionamiento de los cables; no deberían pasar cerca de luces fluorescentes ni de motores.
- Compruebe si los archivos /etc/environment o /etc/inittab están dañados o se han manipulado:
  1. Si es posible, compare estos archivos con copias en buen estado.
  2. Copie los archivos como copias de seguridad y realice las modificaciones necesarias.
  3. En el archivo /etc/environment elimine las líneas que *no* sean:
    - líneas en blanco
    - líneas de comentarios
    - *variable=valor*
4. En el archivo /etc/inittab examine las líneas del dispositivo tty. Si el tty está establecido en desactivado, es probable que el puerto del tty no se utilice. Si no se utiliza, elimine la definición del tty o conecte un dispositivo al puerto.
- Elimine la configuración dañada del tty:
  1. Elimine la definición del tty. Consulte el apartado “[Gestión de dispositivos de TTY](#)” en la página 672 si desea información adicional.
  2. Si desea un registro en copia impresa de la definición del tty antes de eliminarlo, pulse la tecla de Imagen (F8 o Esc+8). Se capturará la imagen actual de la pantalla y se copiará en el archivo smit.log del directorio \$HOME.
  3. Lea la definición del tty. Consulte el apartado “[Gestión de dispositivos de TTY](#)” en la página 672 para ver las instrucciones para añadir un TTY.
- Localice el hardware defectuoso:
  1. Ejecute diagnósticos utilizando el mandato **diag**.
  2. Si se detecta algún problema de hardware, siga los procedimientos locales para la resolución de problemas.

#### **Información del registro de errores y los identificadores de registro de TTY**

Los mandatos y archivos de registro siguientes hacen referencia a los TTY.

##### Mandato: **errclear**

Este mandato suprime entradas del registro de errores. Es posible borrar la totalidad del registro con **errclear 0** o eliminar las entradas con números de ID, clases o tipos determinados.

##### Mandato: **errpt**

Este mandato genera un informe de los errores de las entradas en el registro de errores del sistema. El formato más utilizado para este mandato es **errpt -a | pg**, que genera un informe detallado que empieza por los errores más recientes.

##### Archivo: /var/adm/ras/errlog

Este archivo almacena las instancias de los errores y las anomalías que el sistema detecta. El archivo **errlog** tiende a hacerse bastante largo. Si no se borra con regularidad, puede ocupar bastante espacio del disco duro. Utilice el mandato **errclear** mencionado anteriormente para limpiar este archivo.

##### Archivo: /usr/include/sys/errids.h

El archivo de cabecera **errids.h** correlaciona los ID de los errores con las etiquetas de los errores.

Los siguientes mensajes del informe de errores comunes están relacionados con TTY:

Tabla 103. Mensajes de error de TTY

Mensaje	Descripción	Comentarios
Core Dump	Programa de software terminado anormalmente	Este error se registra cuando un programa de software finaliza anormalmente y provoca un vuelco de la imagen de memoria. Es posible que los usuarios no salgan de las aplicaciones correctamente, que el sistema se haya apagado mientras los usuarios estaban trabajando en una aplicación o que la terminal del usuario se haya bloqueado y la aplicación se haya detenido.
Errlog On	Errdaemon activado	El daemon <b>error</b> registra este error cuando se inicia el registro de errores. El sistema desactiva el registro de errores de forma automática durante el apagado.
Lion Box Died	Se ha perdido la comunicación con el concentrador de 64 puertos	El controlador del concentrador de 64 puertos registra este error si se pierden las comunicaciones con el concentrador. Si recibe este error, compruebe la indicación de la fecha y hora para ver si es posible que el usuario haya provocado este mensaje. Una serie de estos errores puede indicar un problema con el adaptador de 64 puertos o el hardware asociado con el mismo.
Lion Buffero	Desbordamiento del almacenamiento intermedio: concentrador de 64 puertos	Este error se produce cuando se desborda el almacenamiento intermedio del hardware en un concentrador de 64 puertos. Si el dispositivo y el cableado lo permiten, intente añadir el reconocimiento RTS (petición de envío) al puerto y al dispositivo. Intente también disminuir la velocidad en baudios.
Lion Chunknumc	Cuenta de fragmentos errónea: controlador de 64 puertos	Este error se produce cuando el valor del número de caracteres de un fragmento no coincide con los valores reales del almacenamiento intermedio. Este error puede indicar un problema de hardware; intente ejecutar los diagnósticos en los dispositivos.

Tabla 103. Mensajes de error de TTY (continuación)

Mensaje	Descripción	Comentarios
Lion Hrdwre	No se puede acceder a la memoria en un controlador de 64 puertos	El controlador del concentrador de 64 puertos registra este error si no puede acceder a la memoria en el controlador de 64 puertos.
Lion Mem ADAP	No se puede asignar memoria: estructura ADAP	El controlador del concentrador de 64 puertos registra este error si se produce una anomalía en la rutina malloc para la estructura ADAP.
Lion Mem List	No se puede asignar memoria: lista TTYP_T	El controlador del concentrador de 64 puertos registra este error si se produce una anomalía en la rutina malloc para la estructura de la lista <i>ttyp_t</i> .
Lion Pin ADAP	No se puede fijar memoria: estructura ADAP	El controlador del concentrador de 64 puertos registra este error si se produce una anomalía en la rutina pin para la estructura ADAP.
SRC	Error del programa de software	El daemon del Controlador de recursos del sistema (SRC) registra este error en caso de que se produzca una condición anormal. Las condiciones anormales se dividen en tres áreas: subsistemas anómalos, anomalías de comunicación y otras anomalías.
Lion Unkchunk	Código de error desconocido del concentrador de 64 puertos	Código de error: Número de caracteres del fragmento recibido.
TTY Badinput	Cable o conexión defectuosos	El puerto genera entrada con más rapidez que el sistema puede consumirla y parte de esta entrada se rechaza. Normalmente, la entrada errónea se debe a que una o más señales RS-232 cambian de estado con rapidez o de forma repetitiva durante un breve período de tiempo, lo que provoca que el sistema pase mucho tiempo en el manejador de interrupciones. Los errores de las señales suelen deberse a un conector suelto o roto, a un cable defectuoso, sin toma de tierra o sin apantallar o a un enlace de comunicaciones "ruidoso".

Tabla 103. Mensajes de error de TTY (continuación)

Mensaje	Descripción	Comentarios
TTY Overrun	Desbordamiento del receptor durante la entrada	<p>La mayoría de puertos TTY tienen una entrada FIFO de 16 caracteres y el valor predeterminado determina en envío de una interrupción después de recibir 14 caracteres. Este error se comunica cuando el manejador de interrupciones del controlador borra la entrada FIFO y se pierden los datos. Las soluciones posibles dependen del hardware que se utilice:</p> <ul style="list-style-type: none"> <li>• Adaptadores de 8 puertos y 128 puertos Verifique que el control de flujo esté configurado correctamente. Si es así, ejecute los diagnósticos y sustituya el hardware necesario.</li> <li>• Puertos nativos Si el problema se produce en un sistema desocupado, mueva la carga de trabajo a un puerto distinto. Si con ello se corrige el problema, actualice el firmware del sistema.</li> <li>• Soluciones generales <ul style="list-style-type: none"> <li>– Reduzca el parámetro "nivel de desencadenante de RECEPCIÓN" para este puerto de 3 a 2 o 1.</li> <li>– Reduzca la velocidad de la línea en este puerto.</li> <li>– Examine otros dispositivos y procesos para intentar reducir el tiempo que el sistema pasa con las interrupciones inhabilitadas.</li> </ul> </li> </ul>

Tabla 103. Mensajes de error de TTY (continuación)

Mensaje	Descripción	Comentarios
TTY TTYHOG	Desbordamiento de TTYHOG	Este error suele deberse a una discrepancia en el método de control de flujo que utiliza el transmisor y el receptor. El controlador de TTY ha intentado solicitar una pausa al transmisor varias veces pero la entrada no se ha detenido y los datos se han rechazado. Compruebe el método de control de flujo configurado en cada extremo para asegurarse de que se utilice el mismo método en los dos.
TTY Parerr	Error de paridad/trama en la salida	Este error indica errores de paridad en los datos de entrada a puertos asíncronos que se transmitan de carácter en carácter. Suele deberse a una discrepancia en los parámetros de control de la línea (paridad, velocidad de la línea, tamaño de los caracteres o número de bits de parada) entre el transmisor y el receptor. Los parámetros de control de la línea deben estar establecidos del mismo modo en ambos extremos para poder comunicarse.
TTY Prog PTR	Error interno del controlador	El controlador de tty registra este error si el puntero <i>t_hptr</i> es nulo.

#### Eliminación de puerto de TTY colgado

En este ejemplo de eliminación de un puerto colgado, se supone que el puerto de tty colgado es *tty0*. Debe tener autorización root para poder realizar este procedimiento.

- Determine si el tty actualmente gestiona algún proceso escribiendo lo siguiente:

```
ps -lt tty0
```

Debería devolver unos resultados similares a los siguientes:

```
F S UID PID PPID C PRI NI ADDR SZ WCHAN TTY TIME CMD
240001 S 202 22566 3608 0 60 20 781a 444 70201e44 tty0 0:00 ksh
```

El ID del proceso (PID) aquí es 22566. Para eliminar este proceso, escriba lo siguiente:

```
kill 22566
```

Asegúrese de que el proceso se haya eliminado satisfactoriamente escribiendo el mandato `ps -lt tty0`. Si el proceso todavía existe, añada el distintivo `-9` al mandato `kill` tal como se indica en el ejemplo a continuación.

**Nota:** No utilice la opción -9 para eliminar un proceso slattach. Al eliminar un proceso slattach con el distintivo -9 un bloqueo de SLIP podría permanecer en el archivo /etc/locks. Suprima este archivo de bloqueo para hacer limpieza después de slattach.

```
kill -9 22566
```

2. Determine si algún proceso intenta utilizar el tty escribiendo lo siguiente:

```
ps -ef | grep tty0
```

**Nota:** Si el mandato **ps -ef | grep tty** devuelve una salida similar a la siguiente:

```
root 19050 1 0 Mar 06 - 0:00 /usr/sbin/getty /dev/tty
```

donde se visualiza "-" entre la fecha (Mar 06) y la hora (0:00), este tty no tiene el cable correcto. Este estado indica que el proceso de inicio de sesión del sistema (getty) intenta abrir este tty y el proceso abierto se cuelga porque no se declara la señal de detección de portadora de datos (DCD) RS-232. Puede arreglarlo utilizando el adaptador de módem nulo correcto en el cableado. Cuando getty puede abrir el puerto de tty, "-" se sustituye por el número de tty. Para obtener más información sobre los cables, consulte el apartado "[Conexión del módem con los cables adecuados](#)" en la página 688.

**Nota:** El mandato siguiente puede utilizarse para inhabilitar el proceso de inicio de sesión en **tty0**.

```
pdisable tty0
```

Si el proceso de ha eliminado satisfactoriamente pero el tty sigue sin contestar, continúe con el paso siguiente.

3. Escriba el mandato siguiente:

```
fuser -k /dev/tty0
```

Se eliminarán los procesos que se encuentren en ejecución en el puerto y se visualizará el PID. Si el tty sigue sin poder utilizarse, continúe con el paso siguiente.

4. Utilice el mandato **strreset** para desechar los datos de salida del puerto que está colgado debido a que los datos no pueden entregarse porque se ha perdido la conexión con el extremo remoto.

**Nota:** Si el mandato **strreset** arregla el puerto colgado, el puerto tiene un problema de cableado o de configuración, porque la pérdida de la conexión con el extremo remoto debería haber provocado la eliminación de los datos del almacenamiento intermedio de forma automática.

Necesita determinar en primer lugar el número mayor y menor de dispositivo para el tty escribiendo lo siguiente:

```
ls -al /dev/tty0
```

Los resultados deberían ser similares a los siguientes:

```
crw-rw-rw- 1 root system 18, 0 Nov 7 06:19 /dev/tty0
```

Esto indica que **tty0** tiene un número de dispositivo mayor de 18 y un número de dispositivo menor de 0. Especifique estos números cuando utilice el mandato **strreset** de la forma siguiente:

```
/usr/sbin/strreset -M 18 -m 0
```

Si el tty sigue sin poder utilizarse, continúe con el paso siguiente.

5. Desconecte el cable del puerto de tty colgado y vuelva a conectarlo. AIX utiliza la señal Detección de portadora de datos (DCD) para determinar la presencia de un dispositivo conectado al puerto.

Al descartar DCD, si se desconecta el cable y vuelve a conectarse, en la mayoría de casos se eliminarán los procesos colgados.

Para determinar la ubicación del puerto en el que el tty está configurado, escriba el mandato siguiente:

```
lsdev -Cl tty0
```

Los resultados deberían ser similares a los siguientes:

```
tty0 Available 00-00-S1-00 Asynchronous Terminal
```

La tercera columna de la salida anterior indica el código de ubicación del tty. En este ejemplo, S1 indica que se ha configurado el puerto serie para el puerto serie nativo 1. Para obtener más información sobre cómo interpretar los códigos de ubicación, consulte el apartado [../devicemanagement/devloccodes.html](#) en *Sistema operativo y gestión de dispositivos*.

Si el tty sigue sin poder utilizarse, continúe con el paso siguiente.

6. Elimine el puerto utilizando **stty-cxma**. Escriba lo siguiente:

```
/usr/lbin/tty/stty-cxma flush tty0
```

Este mandato está pensado para los tty configurados en puertos de los adaptadores de 8 puertos y 128 puertos. Sin embargo, en algunos casos, puede resultar útil para eliminar otros puertos de tty.

Si el tty sigue sin poder utilizarse, continúe con el paso siguiente.

7. En el teclado del terminal colgado, mantenga pulsada la tecla Control y pulse Q. Se reanudará la salida suspendida mediante el envío de un carácter **Xon**.

Si el tty sigue sin poder utilizarse, continúe con el paso siguiente.

8. En ocasiones, un programa abre un puerto de tty, modifica algunos atributos y cierra el puerto si restablecer los atributos en su estado original. Para corregir esto, deje el tty en estado DEFINIDO y, a continuación, haga que esté disponible escribiendo lo siguiente:

```
rmdev -l tty0
```

Este mandato deja la información sobre el tty en la base de datos pero hace que el tty no esté disponible en el sistema.

El mandato siguiente vuelve a activar el tty:

```
mkdev -l tty0
```

Si el tty sigue sin poder utilizarse, plantéese mover el dispositivo a otro puerto y configurar un tty en esta ubicación hasta que sea posible volver a arrancar el sistema. Si el arranque del sistema no elimina el puerto, probablemente se trata de un problema de hardware. Compruebe los problemas de hardware del puerto en el informe de errores escribiendo lo siguiente:

```
errpt -a | pg
```

Algunos de mandatos anteriores no funcionarán y mostrarán un error de método que indicará que el dispositivo está ocupado. Esto es debido al proceso que se ejecuta en el tty. Si ninguno de los pasos detallados más arriba libera el tty colgado, como último recurso, vuelva a arrancar el sistema AIX y elimine el kernel para que el proceso desaparezca.

## Módems

Los módems proporcionan comunicaciones serie a través de líneas telefónicas convencionales. Entre los conceptos de los módems se incluyen los estándares, la configuración general de los módems y consejos de configuración específica para los módems corrientes.

Un *módem* es un dispositivo que permite conectar un sistema a otro a través de líneas telefónicas convencionales. El sistema telefónico actual no es capaz de transportar los cambios de voltaje necesarios para una conexión digital directa. Un módem soluciona esta limitación modulando la información digital en tonos de audio para la transmisión a través de la línea telefónica y volviendo a desmodular estos tonos en información digital durante la recepción. Los módems se utilizan con frecuencia con los Programas de utilidad básicos de red (BNU) u otra implementación del UNIX-to-UNIX Copy Program (UUCP). Puede

utilizarse un módem de alta velocidad (14.400 bps o superior) con SLIP (Serial Line Interface Protocol) para proporcionar conectividad TCP/IP (Transmission Control Protocol/Internet Protocol) también.

A menudo, para hacer referencia al módem, se utiliza el término *baudios* en lugar de bps. De hecho, el baudio es una medida de la velocidad de modulación. En los módems más antiguos, sólo se codificaba 1 bit en cada cambio de señal, por lo que la velocidad en baudios del módem era igual que la velocidad del módem. Sin embargo, los módems que funcionan a velocidades superiores todavía suelen seguir funcionando a 2.400 (o incluso a 1.200) baudios mientras que codifican dos o más bits por cambio de señal. La velocidad en bps de un módem se calcula multiplicando el número de bits de datos por señal por los baudios (por ejemplo, 2.400 baudios x 6 bits por cambio de señal = 14.400 bits por segundo). La mayoría de los módems modernos pueden comunicarse a distintas velocidades (por ejemplo, 28.800, 14.400, 9.600, 7.800, 4.800 y 2.400 bps).

### **Estándares para las telecomunicaciones**

Anteriormente, las velocidades de 300, 1.200 y 2.400 bps estaban bien definidas. Sin embargo, a medida que los fabricantes de módems empezaron a diseñar métodos para conseguir velocidades superiores, cada fabricante de módems empezó a utilizar un método en propiedad incompatible con los módems de los otros fabricantes. Actualmente, ITU-TSS (anteriormente el Comité consultivo de las Naciones Unidas para la telefonía y la telegrafía internacional, abreviado CCITT) define los estándares para las comunicaciones más rápidas.

Incluso los módems más rápidos resultan mucho más lentos que otros métodos de comunicaciones informáticas. Un módem de alta velocidad puede funcionar a 28.800 bps pero una conexión Ethernet funciona a 10.000.000 bps. Para mejorar el rendimiento de los datos, los módems de alta velocidad suelen ofrecer uno o más algoritmos de compresión de datos. Estos algoritmos pueden mejorar el rendimiento de los módems de alta velocidad a velocidades de 57.600 bps (si la velocidad de los datos es de 14.400 bps) o 115.200 bps (si la velocidad de los datos es de 28.800 bps). Observe que estos algoritmos de compresión son sensibles a los datos que se transmiten. Si los datos ya se han comprimido (por ejemplo, con el mandato **compress**), los métodos de compresión de datos de los módems de alta velocidad ofrece una mejora limitada o nula y pueden incluso reducir el rendimiento de los datos. Cuando se utiliza un módem con tecnología de compresión de datos, la velocidad de la conexión del equipo terminal de datos/equipo de terminación del circuito de datos (DTE/DCE) entre el sistema y el módem es igual o superior a la velocidad nominal de los datos de la conexión entre los módems. Por ejemplo, con un módem V.32bis con compresión de datos V.42bis, la velocidad de los datos del módem (la velocidad a la que el módem se comunica a través de las líneas telefónicas) es de 14.400 bps. Cuando la compresión V.42bis está activada, el rendimiento real de los datos puede llegar a los 57.600 bps. Para dar cabida al mayor rendimiento que la compresión de datos ofrece, la velocidad del enlace entre el sistema y el módem debe establecerse en 57.600 bps.

ITU-TSS define los estándares para las comunicaciones de alta velocidad, incluidos los algoritmos de compresión de datos. Los estándares de ITU-TSS suelen denominarse V.*nn*, donde *nn* es un número. Otro estándar, ligeramente menos frecuente, es el protocolo MNP (Microcom Networking Protocol). Disponible en las versiones (denominadas clases) 1-9, MNP es un protocolo de alto rendimiento y alta velocidad que estuvo disponible relativamente pronto y se convirtió en un estándar de facto antes de la llegada de los estándares de ITU-TSS.

### **Transmisiones dúplex y semi dúplex**

Al estudiar los estándares de telecomunicaciones, es importante comprender las diferencias entre las transmisiones dúplex y semi dúplex.

En una transmisión *semi dúplex* (HDX), un paquete de datos es enviado por un sistema y recibido por el otro. No es posible enviar otro paquete de datos hasta que el sistema receptor envíe un reconocimiento al emisor.

En una transmisión *dúplex* (FDX), el sistema emisor y el receptor se comunican entre sí de forma simultánea; en otras palabras, ambos módems pueden enviar y recibir datos al mismo tiempo. Esto significa que un módem puede estar recibiendo un paquete de datos mientras reconoce la recepción de otro.

### **Estándares de comunicaciones ITU-TSS**

A continuación se describen algunos de los estándares de comunicaciones que define ITU-TSS.

Observe que se trata de una lista parcial solamente. Para ver la lista completa, consulte el sitio web de Internet de la Unión de telecomunicaciones internacional.

Item	Descripción
V.29	Estándar ITU-TSS para las comunicaciones semi dúplex a 9600 bps.
V.32	Estándar ITU-TSS para las comunicaciones dúplex a 9600 bps.
V.32bis	Estándar ITU-TSS para las comunicaciones a 14.400 bps. V.32bis es una revisión del estándar V.32.
V.34	Estándar ITU-TSS para las comunicaciones a 33.600 bps. Observe que este estándar logra velocidades de datos de 33.600 bps si se utiliza la codificación de varios bits en lugar del esquema de compresión de datos que MNP Clase 9 utiliza. Con anterioridad, este estándar se denominaba <i>V.fast</i> .
V.42	Procedimientos de corrección de errores de ITU-TSS para los DCE utilizando la conversión asíncrona a síncrona.
V.42bis	Estándar de compresión de datos ITU-TSS revisado.

#### **Microcom Networking Protocol (MNP)**

Otro estándar de facto es el protocolo **MNP (Microcom Networking Protocol)** desarrollado originariamente por Microcom, Inc.

Disponible en las versiones (denominadas clases) 1-9, **MNP** es un protocolo de alto rendimiento y alta velocidad que estuvo disponible antes de la llegada de los estándares ITU-TSS. Con **MNP**, el módem remoto detecta los errores de los paquetes de datos transmitidos y solicita una retransmisión del paquete de datos erróneo. La posibilidad de reconocer y corregir con rapidez los errores de datos, convierte a **MNP** en uno de los protocolos más comunes en la actualidad.

La tabla siguiente especifica los estándares de comunicaciones de **MNP**.

Item	Descripción
<b>MNP Clase 1</b>	Un método de transferencia de datos asíncrono, semi dúplex basado en bytes con el que se consigue un 70% de eficacia aproximadamente. Este estándar es poco frecuente en los módems modernos.
<b>MNP Clase 2</b>	Un homólogo dúplex a <b>MNP Clase 1</b> que también es poco frecuente en los módems modernos.
<b>MNP Clase 3</b>	Un método de transferencia de datos síncrono, dúplex y basado en bits con el que se consigue una eficacia del 108% aproximadamente. Se consigue una eficacia superior al 100% porque se eliminan los bits de inicio/parada para una conexión asíncrona. El DTE/DCE entre el módem y el sistema siguen siendo asíncronos.
<b>MNP Clase 4</b>	Una mejora de <b>MNP Clase 3</b> que incluye un mecanismo para variar el tamaño de los paquetes (conjunto de paquetes adaptable) y una forma de eliminar la sobrecarga administrativa redundante (optimización de la fase de datos). Un módem <b>MNP Clase 4</b> ofrece una eficacia del 120% aproximadamente.
<b>MNP Clase 5</b>	Incluye la compresión de datos además de las funciones de la Clase 4. Un módem <b>MNP Clase 5</b> ofrece una eficacia del 200%.
<b>MNP Clase 6</b>	Permite la incorporación en un módem de múltiples técnicas de modulación incompatibles (negociación universal de enlaces). Esto permite a los módems <b>MNP Clase 6</b> empezar la comunicación a una velocidad inferior y negociar una transición a una velocidad superior. La <b>Clase 6</b> también incluye un esquema de dúplex estadístico que asigna la utilización de la modulación semi dúplex dinámicamente, para simular un servicio dúplex. Se proporciona soporte a todas las funciones de <b>MNP Clase 5</b> .

<b>Item</b>	<b>Descripción</b>
<b>MNP Clase 7</b>	Incorpora la compresión de datos mejorada. En combinación con la Clase 4, es posible lograr una eficacia del 300%.
<b>MNP Clase 8</b>	No aplicable.
<b>MNP Clase 9</b>	Combina la compresión de datos ampliada con la tecnología V.32 para permitir una velocidad de los datos de hasta 28.800 bps.

#### **Consideraciones sobre el módem**

Los requisitos de la interfaz del módem para el usuario general pueden variar.

La configuración de un módem conectado a este sistema operativo es distinta a la de un sistema personal (PC) o una estación de trabajo.

#### **Módems soportados**

Cualquier módem compatible con EIA 232 que sea capaz de devolver resultados en respuesta a un mandato puede conectarse a este sistema operativo.

#### **Gestión de la detección de la portadora de datos**

El servidor utiliza la señal Detección de portadora de datos (DCD) para supervisar el estado real de un módem.

Si la señal DCD del puerto del módem es "alta", el servidor cree que el módem se está utilizando. Por lo tanto, es importante saber qué circunstancias hacen que esta señal se fuerce a un estado "alto". La señal DCD puede activarse alta por los motivos siguientes:

- La utilización de `clocal` en los atributos de `stty` para el campo de tiempo de ejecución en el panel **Configuración de TTY** de SMIT.
- Si el campo Ignorar detección de portadora está establecido en habilitar en el panel **Configuración de TTY** de SMIT para los ttys conectados a un adaptador de 128 puertos.
- El módem fuerza una DCD alta con los conmutadores o los mandatos AT.
- Una aplicación ya está utilizando el puerto del tty.

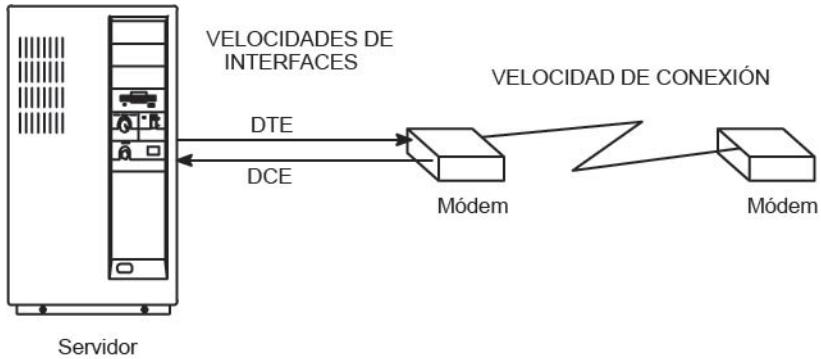
**Nota:** Cuando los módems establecen una conexión con otro módem, el módem activa la CD. Los valores predeterminados de la mayoría de los módems establece esta señal "alta" en todo momento, aunque el módem esté desocupado. La CD no debería forzarse "alta."

#### **Velocidades del Equipo terminal de datos (DTE) o del Equipo de terminación de circuito de datos (DCE)**

El Equipo de terminación de datos (DTE) y el Equipo de comunicación de datos (DCE) se utilizan para describir dos grupos de hardware distintos.

El término DTE se utiliza principalmente para aquellos dispositivos que visualizan información del usuario. También incluye los dispositivos que almacenan o generan datos para el usuario. Las unidades del sistema, los terminales y las impresoras todos se encuentran en la categoría DTE.

DCE incluye los dispositivos que pueden utilizarse para ganar acceso a un sistema a través de las líneas de telecomunicaciones. Las formas más comunes de DCE son los módems y los multiplexores.



*Figura 37. Consideraciones sobre la velocidad del módem*

Con la comunicación serie de este sistema operativo que implica a los módems, tal como se mostraba en la ilustración anterior, existen tres consideraciones principales:

- La velocidad de la interfaz DTE (del servidor al módem). Se trata de la velocidad con la que el servidor se comunica con el módem.
- La velocidad de la interfaz DCE (del módem al servidor), a veces denominada "velocidad de la interfaz del puerto serie". Se trata de la velocidad a la que el módem se comunica con el servidor.
- La velocidad de la conexión (de módem a módem). Se trata de la velocidad a la que un módem se comunica (o conversa) con otro módem.

>La mayoría de módems modernos de alta velocidad permiten que la velocidad de la interfaz DCE sea distinta a la velocidad de la conexión. Esto permite que la velocidad de DTE se bloquee a una sola velocidad en baudios pero que la velocidad de la conexión pueda fluctuar, aumentando o reduciéndose, según sea necesario, para la comunicación correcta entre los módems.

Los módems modernos de alta velocidad retienen los datos que deben transmitirse al servidor en un almacenamiento intermedio y los envían cuando el sistema puede aceptarlos. También retienen los datos que deben transmitirse al otro módem en un almacenamiento intermedio y los envían cuando el sistema remoto puede aceptarlos. Este tipo de transmisión de datos requiere que el módem y el servidor participen en el *control de flujo*.

#### **Señales de control del módem**

Los módems suelen utilizarse para iniciar y recibir llamadas. Por tanto, es importante programar el módem para que negocie una conexión a la velocidad más alta posible y se restablezca en un estado conocido una vez ha finalizado la conexión.

El servidor comutará la señal Terminal de datos preparado (DTR) de activada a desactivada para indicar al módem que debe terminar la conexión. La mayoría de los módems puede configurarse para que se restablezcan cuando se produce esta transición de activada a desactivada de la señal DTR.

**Nota:** Es posible configurar el tty para que no descarte DTR inhabilitando el distintivo `hupcl` en los atributos de tiempo de ejecución de tty.

Para que la conexión entre el servidor y el módem sea completamente funcional, el cableado debe tener las calificaciones siguientes:

- Debe cumplir las especificaciones.
- Debe estar correctamente apantallado.
- Deben proporcionarse las señales siguientes: RxD, TxD, RTS, CTS, SG, DCD y DTR.

**Nota:** El adaptador asíncrono de 16 puertos no proporciona soporte a las señales RTS y CTS. Por lo tanto, es imposible utilizar el control de flujo de hardware RTS/CTS con este adaptador.

Si deben transmitirse datos binarios utilizando un módem en este adaptador, debe utilizarse un protocolo de transferencia de archivos que detecte los datos incorrectos y vuelva a enviar los datos que falten (por ejemplo, Xmodem, zmodem, Kermit y UUCP).

A continuación se describen las señales que el servidor utiliza:

<b>Señal</b>	<b>Descripción</b>
<b>FG</b>	Toma de tierra del bastidor. Patilla 1 de la especificación EIA 232D que proporciona una protección para el cable. Si se utiliza correctamente, la señal sólo se conecta a la patilla 1 en un extremo del cable y a una funda de metal alrededor del cable.
<b>TxD</b>	Transmitir datos. La patilla 2 de la especificación EIA 232D. Los datos se transmiten con esta señal. Controlada por el servidor.
<b>RxD</b>	Recibir datos. La patilla 3 de la especificación EIA 232D. Los datos se reciben con esta señal, controlada por el módem, que el módem envía.
<b>RTS</b>	Petición a enviar. La patilla 4 de la especificación EIA 232D. Se utiliza cuando el control de flujo RTS/CTS está habilitado. Esta señal está alta cuando el sistema está preparado para enviar datos y se elimina cuando el sistema desea que el módem deje de enviar datos.
<b>CTS</b>	Borrar para enviar. La patilla 5 de la especificación EIA 232D. Se utiliza cuando el control de flujo RTS/CTS está habilitado. Esta señal está alta cuando el módem está preparado para enviar o recibir datos. Se elimina cuando el módem desea que el servidor deje de enviar datos. Controlada por el módem.
<b>DSR</b>	Conjunto de datos preparado. La patilla 6 de la especificación EIA 232D. Indica al servidor que el módem se encuentra en un estado en el que está preparado para su utilización. Controlada por el módem.
<b>SG</b>	Señal de toma de tierra. La patilla 7 de la especificación EIA 232D. Esta señal proporciona un voltaje de referencia para las otras señales.
<b>DCD</b>	Detección de portadora de datos. La patilla 8 de la especificación EIA 232D. Proporciona una señal al servidor que indica que el módem está conectado a otro módem. Cuando esta señal está alta, los programas que se ejecutan en el servidor pueden abrir el puerto. Controlada por el módem.
<b>DTR</b>	Terminal de datos preparado. La patilla 20 de la especificación EIA 232D. Proporciona una señal al módem que indica que el módem está activado y preparado para aceptar una conexión. Esta señal de elimina cuando el servidor desea eliminar una conexión con otro módem. Está alta cuando el puerto está abierto. Controlada por el servidor.
<b>RI</b>	Indicación de llamada. La patilla 22 de la especificación EIA 232D. Proporciona una señal al servidor que indica que el módem está recibiendo una llamada. Casi nunca se utiliza y no es necesaria para las operaciones frecuentes. Controlada por el módem.

### Cableado del módem

Estas tablas muestran un resumen de la información sobre los cables necesaria para conectar correctamente un módem a cualquiera de los controladores serie.

<b>Adaptador/Controlador</b>	<b>Números de pieza de IBM</b>
Serie nativa (S1 o S2)	00G0943*, 6326741
Controlador de 2 puertos	00G0943*, 6326741
Controlador de 8 puertos	6323741
Controlador de 128 puertos	43G0935, 6323741

<b>Número de pieza de IBM</b>	<b>Descripción</b>	<b>Longitud en pies</b>
00G0943*	Puente de puerto serie (trenzado)	0,33
6323741	Asíncrono	10
43G0935	Cable conversor de RJ-45 a DB25	2

\*Este número de pieza no es necesario para algunos tipos de máquinas.

#### Configuración del dispositivo de TTY en el sistema operativo

Utilice la herramienta SMIT (System Management Interface Tool) para definir un puerto de tty para la conexión del dispositivo.

La mayoría de los campos son para el tipo de dispositivo general. El único campo que puede afectar el módem es el campo Habilitar INICIO DE SESIÓN con los valores siguientes:

Item	Descripción
<b>INHABILI TAR</b>	No se ejecuta ningún proceso getty en el puerto. Utilice este valor para los puertos del módem de marcación de salida exclusivamente.
<b>HABILITA R</b>	Se ejecuta un proceso getty en el puerto. Utilice este valor para los módems de marcación de entrada exclusivamente.
<b>COMPART IR</b>	Se ejecuta un proceso getty en el puerto, pero el proceso getty permite a los programas realizar marcaciones de entrada y de salida de este puerto sin cambiar manualmente a inhabilitar o a habilitar. Utilice este valor para el uso bidireccional del puerto.
<b>RETRASA R</b>	Se ejecuta un proceso getty en el puerto en modalidad bidireccional, pero no se envía ningún indicador hasta que el usuario pulse una tecla en el proceso getty.

Campos específicos del adaptador asíncrono de 128 puertos:

Item	Descripción
Forzar portadora o Ignorar la detección de portadora	inhabilitar*
Realizar proceso de preparación en adaptador	inhabilitar

**Nota:** Este valor, indicado mediante un asterisco (\*), se establece en inhabilitado si se utiliza el conector RJ-45 de 10 patillas. Este valor debería estar habilitado si se utiliza el conector RJ-45 de 8 patillas.

#### Conexión del módem con los cables adecuados

El primer paso al configurar un módem consiste en conectar el módem con los cables adecuados.

A continuación se muestran los números de pieza y la descripción de los mismos.

##### 6323741

Cable asíncrono EIA-232; utilizado para conectar todos los dispositivos asíncronos; a veces se utiliza con otros montajes de cables.

##### 59F3740

Conector de shell D de 10 a 25 patillas utilizado para conectar el cable asíncrono 6323741 con puertos serie nativos S1 y S2, tal como se muestra en la figura siguiente.



Figura 38. Conector de 10 a 25 patillas

Esta ilustración muestra un conector de 10 a 25 patillas.

A continuación se muestran algunos ejemplos de conexiones de cables:

1. Para conectar un módem al puerto serie nativo S1, utilice los cables siguientes:



Figura 39. Conexión del módem con el cable de puerto serie nativo

Esta ilustración muestra un cable 59F3740 en el extremo del puerto serie y un cable 6323741 en el extremo del módem.

2. Para conectar un módem a una conexión de cable de interfaz del adaptador asíncrono de 8 puertos (EIA-232), utilice los cables siguientes:



Figura 40. Conexión de la interfaz de 8 puertos con el cable del módem

Esta ilustración muestra una interfaz de 8 puertos conectada a un módem con un cable 6323741.

#### Adición de un TTY para el módem

Utilice esta información al añadir un tty para un módem.

En primer lugar, asegúrese de que el sistema esté encendido y el módem apagado. Utilice la vía rápida de SMIT smit mkttty.

#### Configuración del módem

Utilice sólo uno de los métodos presentados aquí para configurar el módem.

Si los Programas de utilidad básicos de red (Basic Networking Utilities - BNU) están instalados, consulte el apartado “Envío de mandatos AT con el mandato cu” en la página 689. Si BNU no está instalado, consulte el apartado “Envío de mandatos AT utilizando un programa C” en la página 690. Para obtener información sobre cómo instalar BNU, consulte el apartado “Programas de utilidad básicos de red (Basic Networking Utilities)” en la página 513.

#### Envío de mandatos AT con el mandato cu

Si los Programas de utilidad básicos de red (Basic Network Utilities - BNU) están instalados, utilice el mandato **cu** para configurar un módem de la forma siguiente.

Los mandatos y los valores que se tratan en este apartado configuran un módem compatible con Hayes con los parámetros básicos necesarios para el funcionamiento en los puertos serie del servidor.

1. Añada la línea siguiente al archivo **/usr/lib/uucp/Devices**. No añada la línea si ya aparece en el archivo. (Sustituya # por el número de su puerto.)

```
Direct tty# - Any direct
```

2. Verifique que tty esté inhabilitado escribiendo lo siguiente:

```
pdisable tty#
```

3. Escriba el mandato siguiente:

```
cu -ml tty#
```

Debería ver un mensaje que diga Conectado.

4. Verifique que tiene la atención del módem escribiendo lo siguiente:

```
AT
```

El módem debería responder OK. En caso contrario, consulte el apartado “Resolución de problemas con el módem” en la página 692.

Para ver mandatos AT adicionales y la descripción de los mismos, consulte el apartado “Mandatos AT” en la página 694.

5. Dependiendo de la opción getty que haya seleccionado, escriba uno de los mandatos siguientes. Sustituya el dispositivo de tty por *n*.

- penable ttyn
- pshare ttyn
- pdelay ttyn
- pdisplay ttyn

El módem está configurado ahora con los mandatos básicos necesarios para realizar la mayoría de las necesidades de comunicaciones serie del sistema operativo. Si tiene problemas, invoque el mandato **cu -dl** para iniciar un rastreo de diagnóstico sobre la conexión.

### **Envío de mandatos AT utilizando un programa C**

Si no ha podido configurar el módem utilizando el mandato **cu** o si no tiene instalado BNU, intente ejecutar el programa C siguiente.

Cree un archivo denominado **motalk.c** que contenga el código siguiente. Guarde el archivo. Compílelo y ejecútelo según las instrucciones de los comentarios del programa.

```
/*********************************************
/* MoTalk - Un programa "C" para configurar el módem. */
/*          Este programa está pensado como ayuda exclusivamente */
/*          e IBM no proporciona soporte.                      */
/*          compile: cc -o motalk motalk.c                  */
/*          Usage: motalk /dev/tty? [speed]                 */
/********************************************

#include <errno.h>
#include <stdio.h>
#include <signal.h>
#include <fcntl.h>
#include <termio.h>
FILE *fdr, *fdw;
int fd;
struct termio term_save, stdin_save;
void Exit(int sig)
{
    if (fdr) fclose(fdr);
    if (fdw) fclose(fdw);
    ioctl(fd, TCSETA, &term_save);
    close(fd);
    ioctl(fileno(stdin), TCSETA, &stdin_save);
    exit(sig);
}
main(int argc, char *argv[])
{
    char *b, buffer[80];
    int baud=0, num;
    struct termio term, tstdin;
    if (argc < 2 || !strcmp(argv[1], "-?"))
    {
        fprintf(stderr, "Usage: motalk /dev/tty? [speed]\n");
        exit(1);
    }
    if ((fd = open(argv[1], O_RDWR | O_NDELAY)) < 0)
    {
        perror(argv[1]);
        exit(errno);
    }
    if (argc > 2)
    {
        switch(atoi(argv[2]))
        {
            case 300: baud = B300;
                        break;
            case 1200: baud = B1200;
                        break;
            case 2400: baud = B2400;
                        break;
            case 4800: baud = B4800;
                        break;
            case 9600: baud = B9600;
                        break;
            case 19200: baud = B19200;
                        break;
            case 38400: baud = B38400;
                        break;
            default:   baud = 0;
                        fprintf(stderr, "%s: %s is an unsupported baud\n", argv[0], argv[2]);
                        exit(1);
        }
    }
    /* Guarde el estado de stdin y tty y atrape algunas señales */
    ioctl(fd, TCGETA, &term_save);
    ioctl(fileno(stdin), TCGETA, &stdin_save);
    signal(SIGHUP, Exit);
    signal(SIGINT, Exit);
}
```

```

signal(SIGQUIT, Exit);
signal(SIGTERM, Exit);
/* Establezca stdin en modalidad bruta, sin eco */
ioctl(fileno(stdin), TCGETA, &tstdin);
tstdin.c_iflag = 0;
tstdin.c_lflag &= ~(ICANON | ECHO);
tstdin.c_cc[VMIN] = 0;
tstdin.c_cc[VTIME] = 0;
ioctl(fileno(stdin), TCSETA, &tstdin);
/* Establezca el estado de tty */
ioctl(fd, TCGETA, &term);
term.c_cflag |= CLOCAL|HUPCL;
if (baud > 0)
{
    term.c_cflag &= ~CBAUD;
    term.c_cflag |= baud;
}
term.c_lflag &= ~(ICANON | ECHO); /* para forzar la modalidad bruta */
term.c_iflag &= ~ICRNL; /* para evitar líneas en blanco innecesarias */
term.c_cc[VMIN] = 0;
term.c_cc[VTIME] = 10;
ioctl(fd, TCSETA, &term);
fcntl(fd, F_SETFL, fcntl(fd, F_GETFL, 0) & ~O_NDELAY);
/* Abra tty para lectura y escritura */
if ((fdw = fopen(argv[1], "r")) == NULL )
{
    perror(argv[1]);
    exit(errno);
}
if ((fdw = fopen(argv[1], "w")) == NULL )
{
    perror(argv[1]);
    exit(errno);
}
/* Hable con el módem */
puts("Ready... ^C to exit");
while (1)
{
    if ((num = read(fileno(stdin), buffer, 80)) > 0)
        write(fileno(fdw), buffer, num);
    if ((num = read(fileno(fdw), buffer, 80)) > 0)
        write(fileno(stdout), buffer, num);
    Exit (0);
}
}
}

```

## Utilización de módems Hayes y compatibles con Hayes

Utilice este procedimiento para los módems Hayes y compatibles con Hayes.

1. Cambie los valores de tty, si es necesario, utilizando la vía de acceso rápida de SMIT, smit chtty. Por ejemplo, es posible que desee cambiar el campo Habilitar INICIO DE SESIÓN a **compartir o habilitar**.
2. Añada la línea siguiente al archivo /usr/lib/uucp/Systems:

```
hayes Nvr HAYESPROG 2400
```

3. Añada esto al archivo /usr/lib/uucp/Devices:

```
# Para programar el módem hayes exclusivamente:
HAYESPROG tty0 - 2400 HayesProgram2400
#entrada ACU habitual:
ACU tty0 - Any hayes
```

4. Añada esto al archivo /usr/lib/uucp/Dialers:

```
# Esta Entrada se utiliza para PROGRAMAR el módem EXCLUSIVAMENTE:
# Las 3 líneas siguientes deberían formar una sola:
HayesProgram2400      =,-      "" \d\DAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OK AT&K3&C1\r\c OK ATL0E0Q2\r\c OK ATS0=1\r\c OK AT&W\r\c
OK
hayes      =,-,      "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
```

5. Para programar el módem, entre el mandato cu -d hayes.

Este mandato utiliza el mandato **cu** para programar el módem. Como no se efectúa ninguna conexión con otro sistema, el mandato no será satisfactorio. El módem está programado si en la salida se visualiza sendthem AT&W y, a continuación, OK got it.

Si no está realizando transferencias de archivos binarios o utilizando BNU, omita el mandato **&K3** y establezca XON como el flujo de control que debe utilizarse. Sin embargo, resulta más eficaz utilizar el control de flujo de hardware (frente al reconocimiento XON-XOFF). Para hacerlo, utilice los valores y las entradas Dialers del paso siguiente.

6. Una vez el módem esté programado, es posible configurar el controlador de dispositivos del sistema para que utilice el control de flujo de hardware. Utilizanado SMIT (smitty chtty vía de acceso rápida), cambie el control de flujo a RTS. Compruebe los manuales del módem para averiguar si el módem proporciona soporte al control de flujo de hardware.

### Resolución de problemas con el módem

Cuando encuentre problemas al utilizar un módem con su sistema, tenga en cuenta los puntos siguientes.

- Algunos módems son sensibles a las mayúsculas y las minúsculas. Utilice letras todas en mayúsculas para los mandatos AT.
- En funcionamiento normal, es preferible restablecer el módem cuando se descarta el DTR (valor &D3). Sin embargo, cuando se configura el módem por primera vez, es aconsejable no restablecer el módem si se descarta el DTR (valor &D2). Si el módem se restablece, se perderán todos los valores programados que no estén guardados en la memoria del módem.

Si no se restablece el módem también se protegen los cambios cuando se establece &C1. El cambio del estado de Detección de portadora puede provocar que la línea de detección de portadora se commute en algunos módems, lo que hace que el mandato **cu** descarte la línea. Es posible que desee configurar el módem en &D3 una vez realizada la configuración final.

- Aunque los mandatos indicados en esta recopilación de temas son estándares para la mayoría de los módems compatibles con Hayes, no existe ninguna garantía de que sean estándares para su módem. Compare los mandatos con la documentación del módem antes de continuar.

Una forma cómoda de depurar posibles problemas con el módem consiste en extraer el módem y conectar un terminal ASCII (con un intermediario o un módem nulo) en el mismo puerto y con el mismo cableado del módem. Configure el terminal con una velocidad de línea, bits por carácter y paridad igual que para el módem. Si el puerto está habilitado para el inicio de sesión, debe visualizar un aviso de inicio de sesión en la pantalla. Si el aviso se visualiza en la pantalla del terminal, el problema puede aislar con rapidez a la configuración del módem.

Los consejos siguientes ayudarán a aislar problemas asociados con las conexiones del módem:

Tabla 104. Problemas y soluciones de módem	
Problema	Solución
<b>Reejecución con demasiada rapidez</b>	<b>init</b> reejecuta el programa getty.

Tabla 104. Problemas y soluciones de módem (continuación)

Problema	Solución
<b>Mensajes en la consola o errpt</b>	<p>Si <b>init</b> ve que debe reejecutar algún programa más de cinco veces en 225 segundos, visualizará el mensaje en la consola y no lo reejutará durante un período de tiempo. La solución consiste en averiguar por qué no responde <b>getty</b>. Puede haber varias causas:</p> <ul style="list-style-type: none"> <li>• Valores del módem incorrectos, normalmente debido a que la CD está establecida alta en el módem o el cableado o a que está activado el "eco" o la "respuesta de mandatos". (También puede presuponerse que la CD está conectada alta si se añade clocal en las modalidades de ejecución y/o en las modalidades de registro de la configuración del puerto o si se fuerza en el puerto 128).</li> <li>• Conmutación de la señal de CD. El proceso <b>getty</b> no responderá cada vez que la CD se commute de estado activado a desactivado. (Esta acción podría deberse a bastante motivos. Asegúrese de verificar que el cable esté apantallado correctamente. Iniciar y finalizar la sesión varias veces en una sucesión rápida puede causar este problema).</li> </ul>
<b>No se visualiza ninguna solicitud de inicio de sesión después de una conexión con el módem</b>	Asegúrese de que <b>getty</b> se esté ejecutando en el puerto. Si lo está, verifique que emerja la señal de conexión con módem de detección de portadora una vez que el extremo remoto haya conectado con el módem. Si la CD está declarada correctamente, verifique que el módem esté conectado al puerto correcto. Si sigue sin ver el inicio de sesión, conecte un terminal con un intermediario al cable en lugar del módem y verifique que aparezca una solicitud de inicio de sesión. Si continúa sin ver una solicitud, intente realizar un eco de los caracteres en la pantalla del terminal para verificar que el cable y el hardware funcionen correctamente.
<b>Cuando un módem remoto se conecta, éste se desconecta inmediatamente</b>	Verifique que el módem converse con el servidor a la misma velocidad a la que el servidor escucha al módem. Intente distintas velocidades en baudios para el <b>tty</b> o programe el módem para que bloquee la velocidad de DTE para que ésta coincida con la del puerto del <b>tty</b> . Verifique que el módem o el puerto no mantenga alta la señal de detección de portadora o que otro proceso ya esté utilizando el puerto.
<b>Aparecen caracteres basura en lugar de una solicitud de inicio de sesión</b>	Esto es debido a una diferencia en los protocolos. Asegúrese de verificar que el módem y el puerto del <b>tty</b> hayan acordado la misma paridad, velocidad en baudios, control de flujo y tamaño de caracteres.
<b>En ocasiones, tras un inicio de sesión satisfactorio, nadie puede iniciar la sesión</b>	Puede deberse a que el módem no se restablece después de la desconexión. Consulte el manual del módem para ver cómo puede restablecerse el módem tras una transición de DTR de activado a desactivado.
<b>El almacenamiento intermedio del receptor se desborda en errpt</b>	El almacenamiento intermedio del chip UART se está desbordando. Reduzca el valor del desencadenante de recepción para el <b>tty</b> en SMIT. Esta solución sólo es válida para los adaptadores asíncronos de 8 o 16 puertos nativos. Verifique que el módem y el puerto del <b>tty</b> utilicen el mismo flujo de control.
<b>Errores ttyhog en errpt</b>	El módem y el <b>tty</b> no se ponen de acuerdo sobre el control de flujo o no se está llevando a cabo ningún control de flujo.

#### Cuestionario sobre el módem para los servicios de software

Antes de llamar solicitando ayuda con problemas con el módem, recopile cierta información básica para agilizar el servicio.

Entre la información disponible debe incluirse la siguiente:

- El nivel del sistema operativo. ¿Cuánto tiempo ha estado trabajando con este nivel sistema operativo?
- ¿El módem funcionaba anteriormente?
- ¿Qué tipo de módem utiliza? ¿Qué tipo de módem se encuentra en el otro extremo de la conexión telefónica?
- ¿A qué tipo de adaptador está conectado el módem?
- ¿A qué número de puerto está conectado el módem?
- ¿A qué número de tty está conectado el módem?
- ¿Qué tipo de cableado está utilizando?
- ¿Cuál es el valor de inicio de sesión (compartir, retardo, habilitar)?
- ¿El módem puede conectarse a otros módems?
- ¿Otros módems pueden conectarse a su módem?
- ¿Cuáles son los valores siguientes en SMIT, el módem, o el puerto?
  - XON/XOFF
  - RTS/CTS
  - Velocidad en BPS
- Incluya los puntos siguientes en la descripción del problema:
  - ¿El puerto se bloque intermitentemente?
  - ¿Puede realizar marcaciones de salida? ¿Los otros puede realizar marcaciones de entrada?
  - Cualquier otra condición de error específica y descriptiva.
- ¿Aparecen errores en la consola? ¿Cuáles?
- ¿Aparece errores en el informe de errores? (**errpt** o **errpt -a**)
- ¿Qué mandato está utilizando para las marcaciones de salida?
- ¿Qué software está implicado en el sistema?

### **Mandatos AT**

El conjunto de mandatos Smartmodem de Hayes incluye el conjunto de mandatos AT que muchos módems populares utilizan.

Esta información procede de Hayes Smartmodem 2400 *Quick Reference Card*, publicada por Hayes Microcomputer Products, Inc. Consulte la documentación del módem para ver la lista de los mandatos AT relevantes.

<b>Item</b>	<b>Descripción</b>
<b>AT</b>	Prefijo del mandato - precede la línea de mandatos.
<b>&lt;CR&gt;</b>	Carácter de retorno de carro (línea nueva) - finaliza la línea de mandatos.
<b>A</b>	Descolgar, permanecer en modalidad de mandato.
<b>A/</b>	Repetir la línea de mandatos anterior. Este mandato no va precedido por <b>AT</b> ni seguido por <b>&lt;CR&gt;/</b> .
<b>B0</b>	Seleccionar el estándar CCITT V.22 para las comunicaciones a 1200 bps.
<b>B1</b>	Seleccionar el estándar Bell 212A para las comunicaciones a 1200 bps.
<b>D</b>	Entrar la modalidad de origen, marcar el número que sigue e intentar entrar en línea. D suele ir seguido por T (por tonos) pero también puede utilizarse P (por impulsos).
<b>DS=n</b>	Marcar el número almacenado en la ubicación <i>n</i>
<b>E0</b>	Inhabilitar el echo de los caracteres en el estado del mandato.
<b>E1</b>	Habilitar el eco de los caracteres en el estado del mandato.

<b>Item</b>	<b>Descripción</b>
<b>H0</b>	Colgar (colgar el teléfono).
<b>H1</b>	Utilizar enganche de conmutación y relé auxiliar.
<b>I0</b>	Devolver código de identificación del producto.
<b>I1</b>	Realizar suma de comprobación en ROM de firmware; devuelve suma de comprobación.
<b>I2</b>	Realizar suma de comprobación en ROM de firmware; devuelve OK o ERROR como resultado.
<b>L0</b>	Altavoz desactivado.
<b>L1</b>	Volumen del altavoz bajo.
<b>L2</b>	Volumen del altavoz medio.
<b>L3</b>	Volumen del altavoz alto.
<b>M0</b>	Altavoz desactivado.
<b>M1</b>	Altavoz activado hasta que se detecte la portadora.
<b>M2</b>	Altavoz siempre activado.
<b>M3</b>	Altavoz activado hasta que se detecte la portadora, excepto durante la marcación.
<b>00</b>	Entrar a estado en línea.
<b>01</b>	Entrar a estado en línea e iniciar reentrenamiento del ecualizador.
<b>Q0</b>	El módem devuelve los códigos de resultados.
<b>Q1</b>	El módem no devuelve los códigos de resultados.
<b>Sr</b>	Establecer puntero en el registro r.
<b>Sr=n</b>	Establecer registro r en valor n.
<b>V0</b>	Visualizar códigos de resultados en formato numérico.
<b>V1</b>	Visualizar códigos de resultados en formato detallado (como palabras).
<b>X0</b>	Habilitar las funciones representadas mediante los códigos de resultados 0-4.
<b>X1</b>	Habilitar las funciones representadas mediante los códigos de resultados 0-5,10.
<b>X2</b>	Habilitar las funciones representadas mediante los códigos de resultados 0-6, 10.
<b>X3</b>	Habilitar las funciones representadas mediante los códigos de resultados 0-5, 7, 10.
<b>X4</b>	Habilitar las funciones representadas mediante los códigos de resultados 0-7, 10.
<b>Y0</b>	Inhabilitar la desconexión de espacios largos.
<b>Y1</b>	Habilitar la desconexión de espacios largos.
<b>Z</b>	Restablecer el módem
<b>&amp;C0</b>	Asumir que la portadora de datos siempre está presente.
<b>&amp;C1</b>	Rastrear la presencia de la portadora de datos.
<b>&amp;D0</b>	Ignorar la señal de DTR.
<b>&amp;D1</b>	Asumir el estado del mandato cuando se produce una transición de activado a desactivado del DTR.
<b>&amp;D2</b>	Colgar y asumir el estado del mandato cuando se produce una transición de activado a desactivado del DTR.
<b>&amp;D3</b>	Restaurar cuando se produce una transición de activado a desactivado del DTR.

<b>Item</b>	<b>Descripción</b>
<b>&amp;F</b>	Volver a llamar a los valores de fábrica para la configuración activa.
<b>&amp;G0</b>	Ningún tono de protección.
<b>&amp;G1</b>	Tono de protección de 500 Hz.
<b>&amp;G2</b>	Tono de protección de 1800 Hz.
<b>&amp;J0</b>	Conector de telecomunicaciones RJ-11/RJ41/RJ45S.
<b>&amp;J1</b>	Conector de telecomunicaciones RJ-11/RJ-13.
<b>&amp;P0</b>	Marcación por impulsos con ratio de realizaciones/interrupciones de 39/61.
<b>&amp;P1</b>	Marcación por impulsos con ratio de realizaciones/interrupciones de 33/67.
<b>&amp;Q0</b>	Funcionar en modalidad asíncrona.
<b>&amp;Qn</b>	Funcionar en modalidad asíncrona <i>n</i>
<b>&amp;R0</b>	Rastrear CTS según RTS.
<b>&amp;R1</b>	Ignorar RTS; asumir siempre la presencia de CTS.
<b>&amp;S0</b>	Asumir la presencia de una señal DSR.
<b>&amp;S1</b>	Rastrear la presencia de una señal DSR.
<b>&amp;T0</b>	Finalizar la prueba en curso.
<b>&amp;T1</b>	Iniciar bucle de retorno análogo local.
<b>&amp;T3</b>	Iniciar bucle de retorno digital.
<b>&amp;T4</b>	Otorgar petición de enlace de datos remoto (RDL) desde módem remoto.
<b>&amp;T5</b>	Denegar petición de RDL desde módem remoto.
<b>&amp;T6</b>	Iniciar bucle de retorno digital remoto.
<b>&amp;T7</b>	Iniciar bucle de retorno digital remoto con autoprueba.
<b>&amp;T8</b>	Iniciar bucle de retorno análogo local con autoprueba.
<b>&amp;V</b>	Visualizar configuración activa, perfiles de usuario y números almacenados.
<b>&amp;Wn</b>	Guardar parámetros almacenables de la configuración activa como perfil de usuario <i>n</i> .
<b>&amp;X0</b>	El módem proporciona la señal de reloj de transmisión.
<b>&amp;X1</b>	El terminal de datos proporciona la señal de reloj de transmisión.
<b>&amp;X2</b>	La recepción de portadora proporciona la señal de reloj de transmisión.
<b>&amp;Yn</b>	Volver a llamar al perfil de usuario <i>n</i> .
<b>&amp;Zn=x</b>	Almacenar el número de teléfono <i>x</i> en la ubicación <i>n</i> .

#### *Resumen de los registros S*

En la tabla siguiente se muestran los registros S, sus rangos y la descripción de los mismos.

<i>Tabla 105. Descripciones de los registros S</i>		
<b>Registro</b>	<b>Rango</b>	<b>Descripción</b>
S0	0-255	Selecciona el número de llamadas antes de contestar.
S1	0-255	Cuenta de llamadas (incrementada con cada llamada).

Tabla 105. Descripciones de los registros S (continuación)

Registro	Rango	Descripción
S2	0-127	Define el carácter de la secuencia de escape (ASCII).
S3	0-127	Define el carácter de retorno de carro (ASCII).
S4	0-127	Define el carácter de salto de línea (ASCII).
S5	0-32, 127	Define el carácter de retroceso (ASCII).
S6	2-255	Selecciona el tiempo de espera en segundos antes de una marcación a ciegas.
S7	1-55	Selecciona el tiempo de espera en segundos para el tono de marcación/portadora.
S8	0-255	Selecciona la duración en segundo de coma.
S9	1-255	Tiempo de respuesta de la detección de la portadora a intervalos de 0,1 segundos (10 = 1 segundo).
S10	1-255	Retardo entre que se pierde la portadora y se cuelga en intervalos de 0,1 segundos.
S11	50-255	Duración/espaciado de los tonos en milisegundos.
S12	50-255	Tiempo de guarda de la secuencia de escape a intervalos de 0,02 segundos.
S13	—	Reservado.
S14	—	Reservado.
S15	—	Reservado.
S16	—	Reservado - las funciones de este registro están bajo el control de los mandatos <b>&amp;T</b> ).
S17	—	Reservado.
S18	0-255	Duración del temporizador de prueba en segundos.
S19	—	Reservado.
S20	—	Reservado.
S21	—	Reservado.
S22	—	Reservado.
S23	—	Reservado.

*Tabla 105. Descripciones de los registros S (continuación)*

<b>Registro</b>	<b>Rango</b>	<b>Descripción</b>
S24	—	Reservado.
S25	0-255	Seleccionar el tiempo de detección de cambio de DTR a intervalos de 0,01 segundos.
S26	0-255	Retardo de RTS a CTS a intervalos de 0,01 segundos.
S27	—	Reservado.

*Códigos de resultado para los adaptadores asíncronos*

En la tabla siguiente se identifican los códigos de resultado que los adaptadores asíncronos devuelven, incluidos los números, palabras y descripciones de los mismos.

*Tabla 106. Códigos de resultado de adaptadores asíncronos*

<b>Número</b>	<b>Palabra</b>	<b>Descripción</b>
0	OK	Mandato ejecutado.
1	CONNECT	Conexión establecida a 0-300 bps.
2	RING	Señal de llamada detectada.
3	NO CARRIER	Señal de portadora perdida o no detectada.
4	ERROR	Mandato o suma de comprobación no válido, error de la línea de mandatos o línea de mandatos demasiado larga.
5	CONNECT 1200	Conexión establecida a 1200 bps.
6	NO DIALTONE	Tono de marcación no detectado.
7	BUSY	Señal de que comunican detectada.
8	NO ANSWER	Sin respuesta al marcar un sistema.
9	CONNECT 2400	Conexión establecida a 2400 bps.

*Modificadores de marcación*

En la tabla siguiente pueden consultarse los modificadores de marcación y la descripción de los mismos.

<b>Item</b>	<b>Descripción</b>
<b>0-9 # * A-D</b>	Dígitos y caracteres para la marcación.
<b>P</b>	Marcación por impulsos.
<b>T</b>	Marcación por tonos.
<b>,</b>	Retrasar proceso del carácter siguiente.
<b>!</b>	Multiconferencia.

<b>Item</b>	<b>Descripción</b>
@	Esperar silencio.
W	Esperar tono de marcación.
;	Volver al estado del mandato después de marcar.
R	Invertir modalidad.
S=n	Marcar el número almacenado en la ubicación <i>n</i> .

### Ayuda para el módem

Cuando encuentre problemas con el módem, podrá disponer de ayuda en los sitios siguientes.

- El representante local de su zona puede ayudarle en la configuración del módem.
- Hay muchas opciones de soporte técnico distintas, disponibles para los clientes en los Servicios de soporte técnico ofrecidos, incluida la asistencia in situ o el soporte técnico por teléfono. Póngase en contacto con el representante de servicio técnico más cercano para obtener ayuda.
- Quizás una fuente de ayuda a menudo no tenida en cuenta es el propio fabricante del módem. La mayoría de fabricantes tiene algún tipo de ayuda en línea para sus productos.

### Entradas del archivo /usr/lib/uucp/Dialers.samples

Estas entradas del archivo de ejemplo se proporcionan sin ninguna garantía y funcionarán tal cual para los modelos mencionados pero es posible que no satisfagan sus necesidades específicas.

Serán necesarias algunas modificaciones para satisfacer sus necesidades individuales. Consulte el manual del módem para obtener una explicación más detallada de los valores.

Para utilizar los valores para programar el módem, necesita una entrada en el archivo /usr/lib/uucp/Systems parecida a esta:

```
hayes Nvr HayesPRGM Any
```

El archivo /usr/lib/uucp/Devices debe tener una entrada similar a la siguiente:

```
HayesPRGM tty0 - 2400 HayesProgram2400
```

Una vez realizadas las dos entradas anteriores, utilice el mandato **cu** siguiente para programar el módem:

```
cu -d hayes
#
# COMPONENT_NAME: cmduucp
#
# (C) COPYRIGHT International Business Machines Corp. 1994
# Materiales bajo licencia - Propiedad de IBM
# Derechos restringidos para los usuarios de EE.UU. - El uso, duplicación o
# divulgación están sujetos a las restricciones del GSA ADP Schedule Contract
# con IBM Corp.
#####
# Módem UDS de Motorola
#
# Utilice udsmodemPROGRAM para programar el módem.
# Es necesario establecer rts/cts en el puerto.
# Utilice un dialer uds o hayes.
#
# La línea "udsmodemPROGRAM" debe ser una sola linea continua
#
#####
udsmodemPROGRAM =,-,""\dAT&FQ2\r\c OK
ATE0Y0&C1&D2&S1%B5%E0*LC\r\c OKAT&K3&W\r\c OK

uds =,-,""\dAT\r\c OK\r ATDT\T\d\r\c CONNECT
#####
#
# IBM 7855 Modelo 10
# Utilice IBMProgram para programar el módem.
# Éste establece el control de flujo rts/cts, desactiva
```

```

# xon/xoff y establece la velocidad de DTE en 19.200 bps.
# El módem se conectará con el servidor a la velocidad y
# el control de flujo adecuados.
# Es necesario establecer rts/cts en el puerto.
#
# La línea "IBMPrgm" debe ser una sola linea continua
#
#####
IBMPrgm =,-, "" \dATQ0\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OK AT&C1\R2\Q2\14\r\c OK AT&B8N1L0E0\A0\r\c OK
ATS0=1\r\c OK ATQ1&W0&Y0\r\c ""
#####

# Lo siguiente se utiliza para la marcación de salida
# en un dispositivo ACU 7855 regular. Hemos de activar
# los códigos de resultados (Q0) porque se desactivaron
# cuando lo programamos. (No permite que el inicio de
# sesión todo en mayúsculas suceda en los intentos de
# marcación de entrada.) Necesitamos una "\" adicional
# delante de "\N" porque los programas BNU lo
# eliminarán si está delante de una "N".
#####
ibm =,-, "" \dATQ0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECL (Sin compresión)
ibmec1 =,-, "" \dAT\N3%C0Q0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECLC (Compresión)
ibmec1c =,-, "" \dAT\N3%C1Q0\r\c OK ATDT\T\d\r\c CONNECT

# IBM_7855 ECLC Compresión con tamaño de bloques de 256 bytes
ibmec1c256 =,-, "" \dAT\N3%C1Q0\A3\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 1200 bps
ibm_ne12 =,-, "" \dATQ0\N0&A2%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 2400 bps
ibm_ne24 =,-, "" \dATQ0\N0&A3%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 9600 bps
ibm_ne96 =,-, "" \dATQ0\N0&A6%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 19200 bps
ibm_ne192 =,-, "" \dATQ0\N0%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 12000 bps
ibm_ne120 =,-, "" \dATQ0\N3%C0&AL8\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 1200 bps (marcación silenciosa)
ibmq12 =,-, "" \dATQ0\r\c OK AT&A2M0DT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 2400 bps (Marcación silenciosa)
ibmq24 =,-, "" \dATQ0\r\c OK AT&A3M0DT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 9600 bps (Marcación silenciosa)
ibmq96 =,-, "" \dATQ0\r\c OK AT&A6M0DT\T\d\r\c CONNECT

# IBM 7855 Sin compresión 19200 bps (marcación silenciosa)
ibmq192 =,-, "" \dATQ0\r\c OK ATM0DT\T\d\r\c CONNECT

#####
#
# Módem Intel 9600EX
# Utilice IntelProgram para programar el módem.
# Éste establece el control de flujo rts/cts y desactiva
# xon/xoff.
# Es necesario establecer rts/cts en el puerto. (Utilice el
# dialer hayes).
#
# La línea "IntelProgram" debe ser una sola linea continua
#
#####
#IntelProgram =,-, "" \dAT\r\c OK AT&F\r\c OK AT&S1M1\r\c OK
AT&D3\r\c OK AT&C1\R1\r\c OK AT&L0E0Y0&Y0\X1\r\c OK ATS0=1\r\c OK
AT&W\r\c OK

#####
# Módem Practical Peripherals 1440FXMT
# Utilice PracPerProgram144 para programar el módem.
# Éste establece el control de flujo rts/cts y desactiva
# xon/xoff. (Utilice el
# dialer hayes).

```

```

# La velocidad de DTE se bloqueará a la velocidad de conexión
# cuando se programe el módem. (Recomendación: 38400 baudios)
#
# La línea "PracPerProgram144" debe ser una sola línea continua
#
#####
PracPerProgram144 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1&K3\r\c OK ATQ2E1&Q9\r\c OK ATS0=1S9=20\r\c OK
AT&W\r\c OK

#####
# Módem Practical Peripherals 9600 bps
# Utilice PracPerProgram9600 para programar el módem.
# Éste establece el control de flujo rts/cts y desactiva
# xon/xoff. (Utilice el
# dialer hayes).
#
# La línea "PracPerProgram144" debe ser una sola línea continua
#
#####
PracPerProgram9600 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1&K3\r\c OK ATL0E0\r\c OK ATS0=1S9=20\r\c OK
AT&W\r\c OK

#####
# Módem Practical Peripherals 2400 bps
# Utilice PracPerProgram para programar el módem.
#
# La línea "PracPerProgram2400" debe ser una sola línea continua
#
#####
PracPerProgram2400 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1\r\c OK ATL0E0\r\c OK ATS0=1S9=20\r\c OK AT&W\r\c OK

#####
# Módem Hayes 2400 bps
# Utilice HayesProgram2400 para programar el módem.
# (Utilice el dialer hayes para marcar)
#
# La línea "HayesProgram2400" debe ser una sola línea continua
#
#####
HayesProgram2400 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1\r\c OK ATL0E0\r\c OK AT S0=1\r\c OK AT&W\r\c OK

#####
# Telebit t2000 Trailblazer Plus
# Utilice TelebitProgram para programar el módem.
# Éste establece el control de flujo rts/cts y desactiva
# xon/xoff y establece la velocidad de DTE por omisión
# en 19.200 bps.
# Es necesario establecer rts/cts en el puerto.
# Esto establece el módem para que envíe tonos PEP al final,
# ya que éstos pueden confundir a los otros módems.
#
# La línea "TelebitProgram" debe ser una sola línea continua
#
#####
TelebitProgram =,-, "" \dAT&F\r\c OK
ats2=255s7=60s11=50s41=2s45=255s51=254s52=2s54=3s58=2s64=1s66=1\r\c OK
ATS69=1s92=1s96=0s105=0s110=1s111=30s130=3s131=1F1M0Q6TV1W0X3Y0\r\c OK
ATE0&W\r\c OK
# Entradas de los dialers Telebit T2000:
# Impone una conexión PEP:
tbfast =,-, "" \dATs50=255s7=60\r\c OK\r ATDT\T\r\c
CONNECT-\d\c-CONNECT

# Conexión a 2400 bps:
#tb2400 =,-, "" \dATs50=3\r\c OK\r ATDT\T\r\c CONNECT

# 2400 MNP:
tb24mnp =,-, "" \dAT\r\c OK ATS0=0S95=2S50=3S41=0\r\c OK
ATDT\T\r\c CONNECT

# Conexión a 1200 bps:#tb1200 =,-, "" \dATs50=2\r\c OK\r
ATDT\T\r\c CONNECT

# 1200 MNP:
tb12mnp =,-, "" \dAT\r\c OK ATS0=0S95=2S50=2S41=0\r\c OK
ATDT\T\r\c CONNECT

```

```

#####
# Telebit WorldBlazer
# WORLDBLAZERProgram establece la velocidad de DTE en 38400,
# pero es posible establecer por encima si la conexión DTE
# puede gestionarlo. Contestamos con tonos PEP al final para
# no confundir a los otros módems. Esto desactiva xon/xoff y
# activa el control de flujo RTS/CTS. El puerto debe
# bloquearse en 38400 con estos valores y necesita tener
# activado RTS/CTS.
#
# La línea "WORLDBLAZERProgram" debe ser una sola linea continua
#
#####
WORLDBLAZERProgram =,-, "" \dAT\r\c AT AT&F3M0\r\c AT
ATs51=253s92=1\r\c ATAT&W\r\c AT

#####
# Dialers ACU para distintas velocidades en BAUDIOS
# para WorldBlazer - Cada uno establece que el módem
# intente conectarse a la velocidad especificada y por # debajo.
WBBlazer aceptará cualquier cosa que el módem
# remoto pueda hacer. Deseará utilizar PEP para otros
# Telebits, así que utilice WBBlazer38400 o WBBlazer19200
# para los mismos.
#####
# WBBlazer =,-, "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
WBBlazer38400 =,-, "" \dATs50=255\r\c OK ATDT\T\d\r\c CONNECT
WBBlazer19200 =,-, "" \dATs50=255\r\c OK ATDT\T\d\r\c CONNECT
# WBBlazer14400 intenta negociar una conexión V.42bis.
WBBlazer14400 =,-, "" \dATs50=7\r\c OK ATDT\T\d\r\c CONNECT

# Para una conexión V.32:
WBBlazer9600 =,-, "" \dATs50=6\r\c OK ATDT\T\d\r\c CONNECT

# Para una conexión V.22:
WBBlazer2400 =,-, "" \dATs50=3\r\c OK ATDT\T\d\r\c CONNECT

# Para una conexión a 1200 bps:
WBBlazer1200 =,-, "" \dATs50=2\r\c OK ATDT\T\d\r\c CONNECT

```

#### *Consideraciones sobre el cableado del módem de 128 puertos*

Este sistema operativo no requiere DSR en las aplicaciones de control de módem y como casi todos los módems actuales tiene la función de contestación automática, la señal del indicador de llamada normalmente no es necesaria.

El conector RJ-45 de 10 patillas no es el subsistema de cableado predominante y su obtención en el mercado al por menor puede resultar difícil. El subsistema de TTY de este sistema operativo proporciona una función opcional llamada ALTPIN que intercambia las funciones lógicas de DSR (Conjunto de datos preparado) con DCD (Detección de portadora de datos) para un puerto. Cuando ALTPIN está habilitado, DCD está disponible en la patilla 1 de un conector RJ-45 de 8 patillas (equivalente a la patilla 2 de un conector de 10 patillas).

Si desea crear un cable de módem de 8 hilos para el RAN de 128 puertos, utilice el conector RJ-45 de 8 patillas, como en la tabla siguiente:

Tabla 107. Cableado del módem de 128 puertos		
Item	Descripción	Módem
<b>SYSTEM END CONNECTOR</b>	<b>DISPOSITIVO FINRI</b>	22
RJ-45 de 8 patillas		
1	DSR	6
2	RTS	4
3 (Chasis)	GND	SHELL
4	TxD	2
5	TxD	3

Tabla 107. Cableado del módem de 128 puertos (continuación)		
Item	Descripción	Módem
6 (Señal)	GND	7
7	CTS	5
8	DTR	20
	CD	8

**Nota:** La ubicación física de DSR y CD puede intercambiarse con el parámetro ALTPIN cuando se habilita utilizando el mandato tty-cmxa.

La tabla siguiente muestra la comunicación asíncrona mediante señales entre la unidad del sistema y un módem conectado. Aquí, los datos se envían desde la unidad del sistema a un sistema remoto.

Tabla 108. Comunicación asíncrona mediante señales

DISPOSITIVO	SEÑAL	ACTIVADO/ DESACTIVADO	SIGNIFICADO
Sistema	DTR	+	Eh, módem, ¿estás listo para conectarte a otro sistema?
Módem	DSR	+	Sí, lo estoy. Puedes marcar.
Módem	DCD	+	Tengo otro sistema en el teléfono.
Sistema	RTS	+	De acuerdo. ¿Puedo enviar los datos ahora?
Módem	CTS	+	Desde luego. Adelante.
Sistema	TxD		Enviando los datos al módem.
Módem	RxD		He recibido los datos.
Módem	CTS	-	No me envíes más datos. Estoy enviándolos...
Módem	CTS	+	De acuerdo. Estoy listo para recibir más datos. Envíamelos.
Los datos de transmisión de datos pueden repetirse hasta...Computer	DTR	-	TERMINADO. Puedes colgar.
Módem	DCD	-	De acuerdo.
Ésta es la comunicación mediante señales entre RS/6000 y un módem que está a punto de recibir una llamada de entrada desde otro sistema.Sistema	DTR	+	Estoy listo y he "habilitado" el puerto para la marcación de entrada.
Módem	DSR	+	Estoy listo pero estoy esperando una llamada.

Tabla 108. Comunicación asíncrona mediante señales (continuación)

DISPOSI-TIVO	SEÑAL	ACTIVADO/DESACTIVA-DO	SIGNIFICADO
Alguien está llamando. Módem	DCD	+	Alguien ha llamado y está en línea.
Módem	CTS	+	Tengo datos de otro teléfono. ¿Puedo enviarte los datos ahora?
Sistema	RTS	+	Estoy listo para recibir. Puedes enviar.
Módem	RxD		Ahí va.
El módem continúa enviando los datos hasta... Computer	RTS	-	ESPERA. El almacenamiento intermedio está lleno. No me envíes más datos.
Sistema	RTS	+	Ahora estoy bien. Envíame más datos.
Módem	DCD	-	La llamada ha finalizado.
Sistema	DTR	-	De acuerdo. Cuelga, por favor.

## Opciones de terminal **stty-cxma**

**stty-cxma** es un programa de utilidad que establece y visualiza las opciones del terminal para los adaptadores PCI de 2, 8 y 128 puertos que se encuentra en el directorio /usr/lbin/tty.

El formato es el siguiente:

```
stty-cxma [-a] [opciones] [ttynname]
```

Si no se especifica ninguna opción, **stty-cxma** visualiza todos los valores especiales del controlador, las señales del módem y todos los parámetros estándares que **stty(1)** muestra para el dispositivo de tty al que la entrada estándar hace referencia. Se proporcionan opciones de mandatos para cambiar los valores de control de flujo, establecer opciones de impresión transparente, forzar líneas de control del módem y visualizar todos los valores de tty. Las opciones que no se reconocen se pasan a **stty(1)** para que las interprete. Las opciones son las siguientes:

### **-a**

Visualiza todos los valores de las opciones exclusivas del adaptador, así como todos los valores de tty estándares que el mandato **stty -a** comunica.

### **ttynname**

Establece y visualiza las opciones de un dispositivo tty determinado, en lugar de la entrada estándar. Este formato puede utilizarse con un nombre de vía de acceso de tty con el prefijo **/dev/** o simplemente con un nombre de tty que empiece por tty. Esta opción puede utilizarse en una línea de control del módem cuando no hay ninguna portadora.

Las opciones siguientes especifican acciones transitorias que pueden realizarse inmediatamente:

### **break**

Envía una señal de interrupción de 250 ms desde la línea de tty.

### **flush**

Indica la entrada y la salida del tty debe desecharse(descartarse) inmediatamente.

### **flushin**

Sólo se desecha la entrada del tty.

**flushout**

Sólo se desecha la salida del tty.

Las opciones siguientes especifican acciones que se restablecen cuando se cierra el dispositivo. El dispositivo utilizará los valores predeterminados cuando vuelva a abrirse.

**stopout**

Detiene la salida exactamente como si se hubiera recibido un carácter XOFF.

**startout**

Reinicia la salida detenida exactamente como si se hubiera recibido un carácter XON.

**stopin**

Activa el control de flujo para detener la entrada.

**startin**

Libera el control de flujo para reanudar la entrada detenida.

**[–]dtr [drop]**

Activa la línea de control del módem DTR, a menos que se seleccione el control de flujo del hardware DTR.

**[–]rts [drop]**

Activa la línea de control del módem RTS, a menos que se seleccione el control de flujo del hardware DTR.

Las opciones siguientes estarán en vigor hasta que se rearranje el sistema o se modifiquen las opciones.

**[–]fastcook**

Realiza el proceso de preparación de la salida en la tarjeta inteligente para reducir el uso de la CPU del sistema principal y aumentar el rendimiento de la entrada en la modalidad bruta.

**[–]fastbaud**

Modifica las tablas de la velocidad en baudios, así que 50 baudios se convierten en 57.600 baudios, 75 baudios se convierten en 76.800 baudios, 110 baudios se convierten en 115.200 baudios y 200 baudios se convierten en 230.000 baudios para los dispositivos soportados.

**[–]rtospace**

Habilita/inhabilita el control de flujo de entrada de hardware RTS por lo que la transmisión remota queda en pausa cuando se descarta el RTS.

**[–]ctspace**

Habilita/inhabilita el control de flujo de salida del hardware CTS, por lo que la transmisión local queda en pausa cuando se descarta el CTS.

**[–]dsrpace**

Habilita/inhabilita el control de flujo de salida del hardware DSR, por lo que la transmisión local queda en pausa cuando se descarta el DSR.

**[–]dcdpase**

Habilita/inhabilita el control de flujo de salida del hardware DCD, por lo que la transmisión local queda en pausa cuando se descarta la DCD.

**[–]dtrpace**

Habilita/inhabilita el control de flujo de entrada de hardware DTR por lo que la transmisión remota queda en pausa cuando se descarta el DTR.

**[–]forcedcd**

Inhabilita [vuelva a habilitar] el sentido de la portadora, con lo que el tty puede abrirse y utilizarse aunque no exista ninguna portadora.

**[–]altpin**

Correlaciona los conectores de salida RJ-45 con los valores del conector predeterminado de 10 patillas o con los valores del conector de 8 patillas. Cuando este parámetro está **habilitado**, se conmuta la ubicación de DSR y de DCD, de forma que DCD está disponible cuando se utiliza el conector RJ-45 de 8 patillas en lugar del conector RJ-45 de 10 patillas. (Valor predeterminado=**inhabilitar**).

Valores posibles:

**habilitar** (especifica valores del conector de 8 patillas)

**inhabilitar** (especifica valores del conector de 10 patillas)

**startc c**

Establece el carácter de control de flujo XON. El carácter puede proporcionarse como un número decimal, octal o hexadecimal. Los números octales se reconocen por la presencia de un cero inicial y los números hexadecimales se indican mediante un 0x inicial. Por ejemplo, el carácter XON estándar Control-Q, puede entrarse como 17 (decimal), 021 (octal) o 0x11 (hexadecimal).

**stopcc**

Establece el carácter de control de flujo XOFF. El carácter puede proporcionarse como un número decimal, octal o hexadecimal (consulte **startc** para ver el formato de los números octales y hexadecimales).

**astartcc**

Establece el carácter de control de flujo XON auxiliar. El carácter puede proporcionarse como un número decimal, octal o hexadecimal (consulte **startc** para ver el formato de los números octales y hexadecimales).

**astopcc**

Establece el carácter de control de flujo XOFF auxiliar. El carácter puede proporcionarse como un número decimal, octal o hexadecimal (consulte **startc** para ver el formato de los números octales y hexadecimales).

**[-]aixon**

Habilita el control de flujo auxiliar, de forma que se utilicen dos caracteres exclusivos para XON y XOFF. Si se reciben los dos caracteres XOFF, la transmisión no se reanudará hasta que se reciban los dos caracteres XON.

**[-]2200flow**

Utiliza el control de flujo de estilo 2200 en el puerto. Los terminales 2200 proporcionan soporte a una impresora conectada y utilizan cuatro caracteres de control de flujo: XON del terminal (0xF8), XON de la impresora (0xF9), XOFF del terminal (0xFA) y XOFF de la impresora (0xFB).

**[-]2200print**

Determina cómo se interpretan estos caracteres de control de flujo. Si 2200print está establecido, ejecute un control de flujo independiente para el terminal y los dispositivos de impresión transparente. En caso contrario, el control de flujo del terminal y de la impresora se une lógicamente. Si se recibe alguno de los caracteres XOFF, toda la salida se deja en pausa hasta que se reciba el carácter XON correspondiente.

**maxcpsn**

Establece la velocidad máxima en caracteres por segundo (cps) a la que los caracteres se envían como salida al dispositivo de impresión transparente. La velocidad seleccionada debe encontrarse justo por debajo de la velocidad de impresión media. Si el número es demasiado bajo, la velocidad de la impresora se reducirá. Si el número es demasiado alto, la impresora utiliza el control de flujo y el tiempo de la entrada del usuario se reduce. El valor predeterminado es 100 cps.

**maxcharn**

Establecer el número máximo de caracteres de impresión transparente que el controlador coloca en la cola de salida. Una reducción de este número aumenta la actividad general del sistema; un aumento de este número retrasa el tiempo de eco de las pulsaciones del operador cuando la impresora transparente se está utilizando. El valor predeterminado es 50 caracteres.

**bufsizer**

Establece el tamaño estimado por el controlador del almacenamiento intermedio de entrada de la impresora transparente. Tras un período de inactividad, el controlador envía en una ráfaga todos estos caracteres a la impresora transparente antes de reducir de la velocidad de maxcps. El valor predeterminado es 100 caracteres.

**onstrs**

Establece la secuencia de escape del terminal para activar la impresión transparente. Las series pueden estar formadas por caracteres ASCII imprimibles y no imprimibles estándares. Los caracteres

de control (no imprimibles) deben entrarse con sus valores octales y deben estar formados por tres dígitos precedidos por un carácter de barra inclinada invertida. Por ejemplo, el carácter de Escape, 33 octal, debe entrarse como \033. Si la serie <Esc>[5i (estándar ANSI) activa la impresión transparente, ésta se entraría como: \033[5i.

#### **offstrs**

Establece la secuencia de escape del terminal para desactivar la impresión transparente. Consulte **onstrs** para ver el formato de las series.

#### **termf**

Establece las series de activación/desactivación de la impresora transparente en los valores encontrados en la tabla predeterminada interna. Los valores predeterminados internos se utilizan para los terminales siguientes: adm31, ansi, dg200, dg210, hz1500, mc5, microterm, multiterm, pcterm, tvi, vp-a2, vp-60, vt52, vt100, vt220, wyse30, wyse50, wyse60 o wyse75. Si el tipo de terminal no se encuentra en la tabla predeterminada interna, ditty lee la entrada terminfo para el tipo de terminal y establece las series de activación/desactivación de la impresión transparente en los valores proporcionados por los atributos mc5/mc4 que se encuentran en las entradas terminfo.

## **Subsistema del protocolo PPP (Point-to-Point Protocol) asíncrono**

El subsistema del **protocolo PPP (Point-to-Point Protocol) asíncrono** proporciona una alternativa a SLIP.

**PPP** proporciona un método estándar para transportar diagramas de datos de distintos protocolos a través de un soporte de almacenamiento punto a punto. **PPP** incluye tres niveles principales:

1. Un método para encapsular los diagramas de datos de distintos protocolos. **PPP** proporciona soporte a los protocolos a nivel de red TCP/IP.
2. Un **protocolo de control de enlace (LCP)** para establecer, configurar y probar la conexión de enlace de datos. **PPP** lo implementa mediante extensiones del kernel de corrientes de datos.
3. Una familia de **Protocolos de control de red (NCP)** para establecer y configurar distintos protocolos a nivel de red. **PPP** proporciona soporte al **Protocolo Internet Protocol de control (IPCP/IPv6CP)** para negociar una conexión TCP/IP.

Esta implementación de **PPP** proporciona soporte a las siguientes RFC (solicitudes de comentarios):

- RFC 1661, *Protocolo LCP de PPP (Point-to-Point Protocol)*
- RFC 1332, *Protocolo Internet Protocol de control (IPCP) de PPP*
- RFC 1662, *PPP en una trama similar a HDLC*
- RFC 1334, *Protocolos de autenticación de PPP*
- RFC 1990, *Multienlace de PPP*
- RFC 2472, *IP Versión 6 a través de PPP*

**PPP** distingue entre cliente y servidor. Este sistema operativo puede actuar como cliente y como servidor. La distinción se realiza para simplificar la configuración. Los servidores **PPP** tienden a asignar una agrupación de direcciones IP/IPv6CP entre las conexiones que se están realizando. Existe una cierta correlación entre los dispositivos de soportes de almacenamiento. Esta implementación de **PPP** interrumpe esta correlación. Todas las conexiones **PPP** del servidor se asignan en función de la primera disponibilidad. Esto facilita la separación de **PPP** de los soportes de almacenamiento. El proceso de conexión debe solicitar su enlace al tipo de enlace adecuado.

### **Procesos PPP a nivel de usuario**

El protocolo **Point-to-point protocol asíncrono** de este sistema operativo utiliza tres procesos a nivel de usuario.

1. Daemon de control (**pppcontrold**) que root ejecuta bajo el Controlador de recursos del sistema (**startsrc -s pppcontrold**). La función del daemon de control comprende la carga y la configuración de todas las extensiones del kernel asociadas con el subsistema. Continúa en ejecución mientras el sistema operativo necesite la función **PPP**.
2. Un proceso de conexión (**pppattachd**) que vincula una serie de TTY a una instancia del **protocolo de control de enlace**, el **protocolo de control de red** y un protocolo de diagrama de datos. Existe una

instancia de **pppattachd** para conexión activa de **PPP** del sistema. Los usuarios del proceso de conexión deben pertenecer al grupo uucp y contener /usr/sbin en la variable de entorno PATH.

3. Un proceso de dialer (**pppdial**) que establece una conexión de salida. El dialer está pensado para que **pppattachd** lo ejecute como el programa conector. Su finalidad consiste en interactuar a través del dispositivo asíncrono antes de la negociación de **PPP**. Esta interacción se define de forma similar al formato de diálogo del chat UUCP. El dialer permite ayudar en el establecimiento de una conexión con un sistema remoto. El establecimiento de sesión propiamente dicho está fuera del alcance de **PPP**.

### Configuración del protocolo PPP (Point-to-Point Protocol) asíncrono

Puede utilizar SMIT para configurar el protocolo **PPP** asíncrono.

La tabla siguiente muestra todas las tareas que pueden ser necesarias para configurar el sistema. Debe tener privilegios root para realizar las tareas de esta tabla.

Al configurar el sistema inicialmente deben seleccionarse, como mínimo, las tareas siguientes de la tabla:

- Añadir una configuración de enlace
- Añadir una interfaz de servidor (si la máquina se configura como un servidor PPP)
- Añadir una interfaz de Demanda (si desea que la máquina proporcione soporte a las conexiones de demanda)
- Manipular usuarios/contraseñas PAP o CHAP (si desea que la máquina proporcione soporte a la autenticación **PPP**)
- Iniciar **PPP** para efectuar los cambios (o Detener **PPP** y, a continuación, volver a iniciarlos, si **PPP** se está ejecutando actualmente)

Tabla 109. Configuración de las tareas de PPP asíncrono

Tarea	Vía rápida de SMIT
Crear una configuración de control de enlace	smit ppplcp
Añadir una configuración de enlace	smit addlcp
Modificar/Mostrar una configuración de enlace	smit chglcp
Eliminar una configuración de enlace <sup>1</sup>	smit rmlcp
Crear interfaces PPP IP	smit pppip
Añadir una interfaz de servidor	smit addpppserver
Modificar/Mostrar una interfaz de servidor	smit listserver
Eliminar una interfaz de servidor <sup>1</sup>	smit rmlistserver
Añadir una interfaz de Demanda	smit addpppdemand
Modificar/Mostrar una interfaz de Demanda	smit listdemand
Eliminar una interfaz de Demanda <sup>1</sup>	smit rmlistdemand
Manipular usuarios/contraseñas PAP	smit pppap
Añadir un usuario PAP	smit addpapuser
Modificar/Mostrar un usuario PAP	smit listpapuser
Eliminar un usuario PAP	smit rmpapuser
Manipular usuarios/contraseñas CHAP	smit pppchap
Añadir un usuario CHAP	smit addchapuser
Modificar/Mostrar un usuario CHAP	smit listchapuser
Eliminar un usuario CHAP	smit rmchapuser

Tabla 109. Configuración de las tareas de PPP asíncrono (continuación)

Tarea	Vía rápida de SMIT
Iniciar <b>PPP</b> <sup>2</sup>	smit startppp
Detener <b>PPP</b> <sup>3</sup>	smit stopppp
Interfaces <b>PPP IPv6</b>	smit pppipv6
Añadir una interfaz de servidor <b>PPP IPv6</b>	smit addpppv6server
Mostrar o modificar una interfaz <b>PPP IPv6</b> .	smit listv6server
Eliminar una interfaz <b>PPP IPv6</b> .	smit rmlistv6server
Añadir una interfaz de cliente <b>PPP IPv6</b> .	smit addpppv6client
Mostrar o modificar una interfaz de cliente <b>PPP IPv6.</b>	smit listpppv6client
Eliminar una interfaz de cliente <b>PPP IPv6.</b>	smit rmlistpppv6client
Añadir una interfaz de Demanda <b>PPP IPv6</b>	smit addpppv6demand
Mostrar o modificar una interfaz de Demanda <b>PPP IPv6.</b>	smit listpppv6demand
Eliminar una interfaz de Demanda <b>PPP IPv6.</b>	smit rmlistpppv6demand
Interfaces <b>PPP IP e IPv6</b>	smit pppipv4_6
Añadir una interfaz de servidor <b>PPP IP/IPv6</b>	smit addpppv4_6server
Mostrar o modificar una interfaz <b>PPP IP/IPv6.</b>	smit listv4_6server
Eliminar una interfaz <b>PPP IP/IPv6.</b>	smit rmlistv4_6server
Añadir una interfaz de cliente <b>PPP IP/IPv6.</b>	smit addpppv4_6client
Mostrar o modificar una interfaz de cliente <b>PPP IP/IPv6.</b>	smit listpppv4_6client
Eliminar una interfaz de cliente <b>PPP IP/IPv6.</b>	smit rmlistpppv4_6client
Añadir una interfaz de Demanda <b>PPP IP/IPv6</b>	smit addpppv4_6demand
Mostrar o modificar una interfaz de Demanda <b>PPP IP/IPv6.</b>	smit listpppv4_6demand
Eliminar una interfaz de Demanda <b>PPP IP/IPv6.</b>	smit rmlistpppv4_6demand

**Nota:**

- Si se selecciona esta tarea, se destruye la información existente.
- Una forma alternativa para iniciar **PPP** consiste en emitir el mandato **startsrc -s pppcontrold**. Sin embargo, la interfaz SMIT también permite establecer el inicio de **PPP** durante el arranque.
- Una forma alternativa de detener **PPP** consiste en emitir el mandato **stopsrc -s pppcontrold**. Sin embargo, la interfaz SMIT también permite establecer que **PPP** no se inicie durante el arranque.

#### Habilitación de SNMP para PPP

**PPP** puede interactuar con el daemon SNMP de TCP/IP para ofrecer información sobre la configuración de la capa de enlace PPP así como información sobre las interfaces **Protocolo de control de enlaces (LCP)** activas.

Siempre que tanto el SNMP para TCP/IP como el software de gestión de SNMP estén configurados correctamente, SNMP para **PPP** permite:

- Recuperar información sobre la configuración de enlaces de **PPP** (por ejemplo, el tamaño de la unidad de recepción máxima y la correlación de caracteres asíncrona)
- Establecer información sobre la configuración de enlaces de **PPP**
- Recuperar información sobre las interfaces LCP para los enlaces LCP activos
- Modificar el estado de los enlaces de LCP activos, que pueden cambiarse a "desconectados" estableciendo el objeto de la Base de información de gestión (MIB) **ifAdminStatus** correspondiente

No se proporciona soporte a todos los objetos definidos por RFC1471 para la MIB de **PPP**. Sólo la tabla **pppLink** es aplicable al subsistema **PPP**, por lo que no se proporciona soporte a las secciones **pppLqr** y **pppTests**. Se proporciona soporte a la sección **pppLink** pero con las excepciones siguientes:

- El objeto **pppLinkConfigMagicNumber** es de sólo lectura. En **PPP**, la negociación del número mágico siempre se realiza y no puede inhabilitarse.
- El objeto **pppLinkConfigFcsSize** es de sólo lectura. Con este sistema operativo, **PPP** sólo proporciona soporte al tamaño 16 para FCS.

Por omisión, SNMP para **PPP** está inhabilitado. Para habilitar **PPP** SNMP, puede utilizar el procedimiento siguiente. Debe tener privilegios root para realizar este procedimiento.

**Nota:** En el procedimiento siguiente se asume que la configuración de enlaces de **PPP** ya se ha establecido. En caso contrario, realice el procedimiento que se describe en el apartado “Configuración del protocolo PPP (Point-to-Point Protocol) asíncrono” en la página 708 antes de habilitar SNMP para **PPP**.

1. Inicie la interfaz SMIT y muestre la pantalla Cambiar/Mostrar una configuración de enlace escribiendo:

```
smit chglcp
```

2. Commute a sí el campo del subagente Habilitar SNMP para **PPP**.
3. Acepte las modificaciones y salga de SMIT.

SNMP para **PPP** no se habilita hasta que se reinicia **PPP**.

- Si **PPP** se está en ejecución actualmente,
  1. Detenga **PPP** utilizando la vía rápida `smit stoppp` (consulte la tabla en el apartado “Configuración del protocolo PPP (Point-to-Point Protocol) asíncrono” en la página 708).
  2. De forma periódica, compruebe si el subsistema ha completado la conclusión escribiendo:

```
lssrc -s pppcontrold
```

El período de tiempo que se tarda en detener el subsistema completamente depende del número de enlaces definidos en la configuración de **PPP**. El subsistema está completamente apagado cuando la salida de este mandato muestra el estado no\_operativo.

3. Inicie **PPP** utilizando la vía rápida `smit startppp` (consulte la tabla en el apartado “Configuración del protocolo PPP (Point-to-Point Protocol) asíncrono” en la página 708).
- Si **PPP** no se está ejecutando actualmente, inicie **PPP** utilizando la vía rápida `smit startppp` (consulte la tabla en el apartado “Configuración del protocolo PPP (Point-to-Point Protocol) asíncrono” en la página 708).

## Serial Line Internet Protocol (SLIP)

**Serial Line Internet Protocol (SLIP)** es el protocolo que TCP/IP utiliza cuando funciona a través de una conexión serie.

Suele utilizarse en enlaces serie dedicados y en conexiones de marcación que funcionen a una velocidad entre 1200 bps y 19,2 Kbps o superior.

**Nota:** Para utilizar velocidades en baudios superiores a 38400, especifique una velocidad en baudios de 50 en el archivo /etc/uucp/Devices para el tty que desee y a continuación cambie la configuración de SMIT para que este tty refleje la velocidad en baudios real deseada.

Por ejemplo, para ejecutar el mandato **cu** en tty0 a una velocidad en baudios de 115200, siga el procedimiento siguiente:

1. Asegúrese de que el hardware proporcione soporte a la velocidad en baudios.
2. Edite /etc/uucp/Devices para incluir la línea siguiente:

```
Direct tty0 - 50 direct
```

3. Escriba la vía rápida smit chtty.
4. Seleccione tty0.
5. Cambie la velocidad en baudios a 115200.
6. Salga de SMIT.

## Configuración de SLIP

Se recomienda la realización de dos pasos durante la configuración de **SLIP**.

Este enfoque de dos pasos separa los requisitos de configuración dependientes de la máquina y del hardware de los problemas de sintaxis de los mandatos y el software de SLIP.

1. Utilice ATE o el programa de utilidad **cu** para conseguir un inicio de sesión satisfactorio en un sistema remoto.

Esto prueba la utilidad y adecuación del enlace físico.

Es importante verificar el funcionamiento de los módems implicados en un enlace **SLIP**, ya que suelen ser la causa más frecuente de problemas durante la fase de configuración.

2. Una vez que establezca un inicio de sesión sin errores en el sistema remoto, utilizando ATE o el mandato **cu**, puede empezar la configuración de **SLIP**.

## Consideraciones sobre los módems de SLIP

Al configurar los módems para **SLIP**, es importante que estos cambios se realicen en ambos extremos del enlace de comunicaciones.

El módem local y el remoto deben configurarse exactamente igual.

1. El módem debe reconocer la presencia de DTR.

Haciendo referencia al módem local, si DTR se presupone o se ignora, el módem nunca puede colgar. Sólo puede cerrar la línea o colgar cuando reconoce la pérdida de la portadora desde el otro extremo. Esto significa que las desconexiones sólo pueden producirse cuando el otro extremo las instiga. Los mandatos de AT &D2 o &D3 son valores adecuados para la mayoría de los módems compatibles con Hayes.

2. El módem nunca debe forzar, presuponer o ignorar la detección de la portadora de datos(DCD).

DCD debe seguir o rastrear la condición real. Esto significa que la portadora existirá después de una conexión de autenticidad con el otro extremo (módem) a través de la línea telefónica comutada. Esto también es aplicable a una línea dedicada. &C1 es el valor recomendado para la mayoría de los módems compatibles con Hayes.

3. El módem nunca debe forzar, presuponer o ignorar una señal de borrar para enviar (CTS).

CTS debe seguir o rastrear una petición para enviar (RTS). Si CTS se fuerza como verdadero, el puerto abierto fallará siempre que se coloque **getty** sobre el puerto o cuando el protocolo de control de flujo RTS se añada al puerto.

4. Los módems deben configurarse para desactivar los códigos de solicitud de repetición automática (ARQ) si surgen problemas durante los intentos de marcación de **slattach**.

Si los módems no consiguen repetidamente establecer una conexión durante los intentos de marcación de entrada de **slattach**, el usuario debe comprobar las configuraciones del módem y desactivar los códigos ARQ si actualmente están activados. En la mayoría de los módems compatibles con Hayes, se trata del valor &A0.

La inhabilitación de los códigos de resultados ARQ no afecta a las conexiones controladas mediante errores ni impide que el módem devuelva mensajes CONNECT estándares (si los códigos de resultados están habilitados) tal como es necesario para la serie de marcación **slattach**.

5. ECL (Comprobación de errores en el enlace) es crítico.

AMBOS módems o NINGUNO de los módem deben utilizarlo. Normalmente, ambos módems debe llegar a un acuerdo sobre su utilización durante la sesión de conexión. Si se selecciona ECL, la línea telefónica física debe ser lo suficientemente buena para permitir una recuperación de un error de datos antes de que caduquen los temporizadores de TCP/IP mientras se espera un paquete de reconocimiento para los últimos datos enviados a través del enlace de **SLIP**.

6. Compresión de datos a través del enlace.

Resulta aceptable la utilización de la compresión de datos a través del enlace siempre que los módems la gestionen totalmente. **SLIP** no realiza ningún tipo de compresión. Si se invoca la compresión de datos, es mucho mejor tener dos módems del mismo tipo exactamente; esto garantiza que cada uno realizará la compresión de la misma forma y el mismo período de tiempo.

### Programación manual de los módems utilizando el mandato cu

Utilice el procedimiento siguiente para programar manualmente los módems conectados a la unidad del sistema.

- El UNIX-to-UNIX Copy Program (UUCP) debe estar instalado en el sistema. Utilice el mandato **lslpp -f | grep bos.net.UUCP** para verificar la instalación.
- Debe haber un módem conectado al sistema y encendido.
- Se requiere autorización de usuario root para cambiar los archivos adecuados.

1. Añada la línea siguiente al archivo /etc/uucp/Devices si ésta todavía no existe (sustituya # por el número de su puerto).

```
Direct tty# - Any direct
```

**Nota:** Las líneas del archivo Devices que empiezan por un signo # en la columna situada más la izquierda son comentarios.

2. Guarde el archivo y salga.

3. Escriba el mandato siguiente en la línea de mandatos:

```
cu -m1 tty#
```

4. Debería aparecer un mensaje de conexión en pantalla indicando que el módem está conectado y listo para su programación.

5. Escriba AT y pulse Intro.

El módem debería responder OK. Si no se recibe ninguna respuesta del módem o si los caracteres escritos no aparecen en la pantalla, compruebe lo siguiente:

- Verifique las conexiones de cableado del módem.
- Verifique que el módem esté encendido.
- Observe las luces del panel frontal del módem cuando pulse Intro. Si las luces de Recibir datos (RD) y Enviar datos (SD) parpadea, el módem está comunicándose con el sistema y el problema puede encontrarse en los valores actuales del módem. Si las luces no parpadean, se trata de un problema con la conexión del módem.
- Escriba lo siguiente y vea si la cambia la condición:

```
ATE1 <Intro>
ATQ0 <Intro>
```

ATE1 activa la modalidad de eco, que visualiza en pantalla los caracteres que haya escrito. ATQ0 habilita la visualización de los códigos de resultado.

6. Programe el módem utilizando los valores que se muestran en el apartado anterior, "Consideraciones sobre el módem."

El ejemplo siguiente muestra cómo programar y guardar los valores básicos para un módem compatible con Hayes. Escriba:

```
AT&F      <Intro>
AT&D2    <Intro>
ATS0=1   <Intro>
ATS9=12  <Intro>
AT&C1    <Intro>
AT&W     <Intro>
~.       <Intro>
```

Donde &F se utiliza para restablecer el módem en los valores predeterminados de fábrica, &D2 establece DTR, S0 y S9 establecen los valores de registro, &C1 establece la portadora y &W graba los valores en el módem. Los caracteres de tilde-punto finalizan la conexión.

### Configuración automatizada de los módems

Los usuarios pueden personalizar los módems manualmente o utilizar el programa de utilidad **cu** y los archivos asociados al mismo para crear un script para la configuración automatizada de los módems.

- UUCP debe estar instalado en el sistema. Utilice el mandato **lslpp -f | grep bos.net.UUCP** para verificar la instalación.
- Debe haber un módem conectado al sistema y encendido.
- La serie de mandatos de módem AT ya debe existir (por ejemplo, at&f&c1&d3). Los usuarios no deben intentar la configuración automatizada de los módems hasta haber probado la serie de mandatos manualmente utilizando el mandato **cu**.
- Se requiere autorización de usuario root para cambiar los archivos adecuados.

El ejemplo siguiente muestra cómo configurar automáticamente un módem Telebit T3000 conectado a tty0.

1. Edite el archivo /etc/uucp/Systems.

2. Añada la línea siguiente al final del archivo. La entrada debería empezar por la columna situada más a la izquierda del archivo.

```
telebit Nvr TELEPROG 19200
```

3. Guarde el archivo y salga.

4. Edite el archivo /etc/uucp/Devices.

5. Añada la línea siguiente al final del archivo. La entrada debería empezar por la columna situada más a la izquierda del archivo.

```
TELEPROG tty0 - 19200 TelebitProgram
```

6. Guarde el archivo y salga.

7. Edite el archivo /etc/uucp/Dialers.

8. Añada las líneas siguientes al final del archivo.

Las entradas deberían empezar por la columna situada más a la izquierda del archivo.

**Nota:** Las cuatro líneas siguientes deberían formar una sola línea larga:

```
TelebitProgram =,-,    "" \dAT&F\r\c OK
ats0=1s2=255s7=60s11=50s41=2s45=255s51=252s63=1s58=2s64=1\r\c OK
ATs69=2s105=0s111=30s255=0M0&C1Q2&D3&Q0&R3&S1&T5\r\c OK
ATE0X12&W\r\c OK
```

9. Guarde el archivo y salga.

10. Para empezar la configuración automatizada, escriba el mandato siguiente:

```
cu -d telebit
```

El mandato fallará porque no está conectado a un sistema. Observe la salida de depuración del mandato para ver si se ha enviado al módem ATE0X12&W y si se ha recibido OK. En caso afirmativo, el módem se ha programado satisfactoriamente.

Es posible que surjan problemas debido a la colocación de valores incorrectos en el archivo Dialers o a una configuración existente del módem. En este caso, intente programar el módem manualmente y entre las series de los dialers (del paso 8) una a una.

### Configuración de SLIP a través de un módem

Para configurar **SLIP (Serial Line Interface Protocol)** entre dos sistemas que se comunican a través de un módem, puede utilizar este procedimiento, que alterna entre la System Management Interface Tool (SMIT) interfaz y la línea de mandatos para completar la configuración..

Para proporcionar mayor claridad, las instrucciones siguientes utilizan los nombres bronce y oro para los dos sistemas principales.

1. Conecte físicamente los módems a bronce y oro.
2. Para crear un tty en bronce utilizando SMIT, siga estos pasos:

- a) Escriba:

```
smit maktty
```

- b) Seleccione **rs232** como el tipo de tty que desea crear.
- c) Seleccione un puerto serie disponible como, por ejemplo, sa0 (puerto serie del sistema 1).
- d) Seleccione un número de puerto para este tty de la lista.
- e) Establezca la velocidad EN BAUDIOS en la velocidad en baudios de su módem.
- f) Establezca Habilitar INICIO DE SESIÓN en inhabilitar.
- g) Salga de SMIT.

3. Cree un tty en oro.

Siga el mismo procedimiento que para bronce (en el paso 2) pero establezca Habilitar INICIO DE SESIÓN en **habilitar**.

En el resto de estas instrucciones se asume que el número de tty tanto de bronce como de oro es tty1.

4. Pruebe la conexión física con ATE.

- a) En bronce, escriba:

```
ate
```

- b) En el Unconnected Main Menu, seleccione el submandato **Alter**. Establezca la velocidad en la velocidad en baudios de su módem y el dispositivo en tty1.
- c) En el Unconnected Main Menu, seleccione el submandato **Connect**. Cuando ATE le solicite un número de teléfono, entre el número de teléfono de oro y pulse Intro.
- d) En este momento, debería recibir una solicitud de inicio de sesión para oro. Inicie sesión.
- e) Vuelva a la pantalla de conexión, finalice la sesión de oro, pulse Control-V (para llegar al CONNECTED MAIN MENU de ATE), pulse la tecla T para terminar la conexión y pulse la tecla Q para salir de ATE.

**Nota:** Si no recibe la solicitud de inicio de sesión, vuelva al paso 1 y verifique que la configuración sea correcta. No prosiga hasta que consiga iniciar la sesión en oro.

5. Como la configuración de tty que debe utilizarse con ATE es ligeramente distinta de la configuración que debe utilizarse con SLIP, deberá realizar los cambios siguientes:

- a) En bronce, escriba:

```
smit chgtty
```

- b) En oro, escriba:

```
smmit chgtty-pdisable tty1
```

c) Seleccione **tty1** y seleccione **Cambiar/Mostrar programa de TTY**.

d) Establezca Habilitar INICIO DE SESIÓN en inhabilitar y salga de SMIT.

6. Añada la línea siguiente al archivo **/usr/lib/uucp/Devices** tanto en bronce como en oro:

```
Direct tty1 - 9600 direct
```

o sustituya 9600 por la velocidad real de su módem.

7. Cree una interfaz de red de **SLIP** en bronce.

a) Escriba:

```
smmit mkinet1sl
```

b) Para el PUERTO TTY para la interfaz de red de SLIP, seleccione **tty1**.

c) Especifique la DIRECCIÓN DE INTERNET como, por ejemplo, 130.130.130.1.

d) Especifique la dirección de DESTINO (de oro) como, por ejemplo, 130.130.130.2.

e) Especifique la VELOCIDAD EN BAUDIOS de su módem.

f) Especifique la SERIE DE MARCACIÓN como, por ejemplo:

- "" AT OK ATDT555-1234 CONNECT ""

- El significado de este mandato es: Utilizar **tty1** a 9600 baudios. Envíe AT al módem. El módem debería responder OK. Marque el número de teléfono 555-1234. El módem debería responder CONNECT. Los espacios antes y después de los caracteres " " son necesarios.

g) Salga de SMIT.

8. Cree una interfaz de red de **SLIP** en oro.

Siga el mismo procedimiento que para bronce (en el paso 5) pero intercambie la DIRECCIÓN DE INTERNET y la dirección de DESTINO.

9. Añada las dos entradas siguientes al archivo **/etc/hosts** tanto en bronce como en oro:

```
130.130.130.1    bronce  
130.130.130.2    oro
```

El nombre que asigne debe ser exclusivo. En otras palabras, si a la interfaz de red en anillo de bronce ya se le ha asignado el nombre **bronce**, asigne a la interfaz de **SLIP** un nombre como, por ejemplo **bronce\_slip**.

**Nota:** Para una interfaz simplificada con el mandato **slattach**, podría utilizar el script **/usr/sbin/slipcall**.

10. Pruebe la conexión de **SLIP**.

a) En bronce, escriba:

```
ping oro
```

b) En oro, escriba:

```
ping bronce
```

Si ambas pruebas son satisfactorias, la conexión de **SLIP** está lista para su utilización. En caso contrario, vuelva al paso 5 y verifique que la configuración sea correcta tanto en bronce como en oro.

### Configuración de **SLIP** a través de un cable de módem nulo

Para configurar **SLIP** entre dos sistemas que estén conectados utilizando un cable de módem nulo, puede utilizar este procedimiento, que alterna entre la interfaz System Management Interface Tool (SMIT) y la línea de mandatos para completar la configuración..

Para proporcionar mayor claridad, estas instrucciones utilizan los nombres bronce y oro para los dos sistemas principales.

1. Conecte bronce y oro físicamente mediante el cable de módem nulo.

Se necesitan los cables siguientes. (Los cables se listan en el orden en que se conectarán de bronce a oro.)

- a) Cable B (número de pieza 00G0943). Cable de puente de puerto serie; se proporcionan dos con cada sistema, a excepción de los modelos 220, 340 y 350, que no los requieren.
- b) Cable D (número de pieza 6323741, código de característica 2936). Cable asíncrono EIA-232/V.24.
- c) Cable E (número de pieza 59F2861, código de característica 2937). Intermediario impresora/terminal EIA-232 (cable de módem nulo).
- d) Adaptador del cambiador (los dos extremos del adaptador son zócalos).

2. Cree un tty en bronce.

- a) Escriba:

```
smit maktty
```

- b) Seleccione **rs232** como el tipo de tty que desea crear.
- c) Seleccione un puerto serie disponible como, por ejemplo, **sa0** (puerto serie del sistema 1).
- d) Seleccione un número de puerto para este tty de la lista.
- e) Establezca la velocidad EN BAUDIOS en 19200. (Más adelante, la cambiará a 38400. Pero ahora utilice 19200.)
- f) Establezca Habilitar INICIO DE SESIÓN en inhabilitar y salga de SMIT.

3. Cree un tty en oro. Siga los mismos pasos que para bronce (en el paso 2) pero establezca Habilitar INICIO DE SESIÓN en **habilitar**.

**Nota:** En el resto de estas instrucciones se asume que el número de tty tanto de bronce como de oro es tty1.

4. Pruebe la conexión física con ATE.

- a) En bronce, escriba:

```
ate
```

- b) En el Unconnected Main Menu, seleccione el submandato **Alter**. Establezca la velocidad en 19200 y el dispositivo en tty1.
- c) En el Unconnected Main Menu, seleccione el submandato **Connect**.

Cuando ATE le solicite un número de teléfono, pulse Intro. Debería recibir el mensaje siguiente:

```
ate: 0828-010 El mandato Connect ha efectuado una conexión a través del puerto tty1
```

- d) Pulse Intro.

Debería recibir una solicitud de inicio de sesión para oro. Inicie la sesión en oro.

- e) Finalmente, vuelva a la pantalla de conexión, finalice la sesión de oro, pulse Control-V (para llegar al CONNECTED MAIN MENU de ATE), pulse la tecla T para terminar (finalizar) la conexión y pulse la tecla Q para salir de ATE.

**Nota:** Si no recibe la solicitud de inicio de sesión, vuelva al paso 1 y verifique que la configuración sea correcta. No prosiga hasta que consiga iniciar la sesión en oro.

5. Como la configuración de tty que debe utilizarse con ATE es ligeramente distinta de la configuración que debe utilizarse con **SLIP**, deberá realizar los cambios siguientes:

- a) En bronce, escriba:

```
smit chgtty
```

b) Seleccione **tty1**. Establezca la velocidad EN BAUDIOS en 38400 y salga de SMIT.

c) En oro, escriba:

```
pdisable tty1
```

d) En oro, escriba:

```
smit chgtty
```

e) Seleccione **tty1**. Establezca Habilitar INICIO DE SESIÓN en inhabilitar, establezca la velocidad EN BAUDIOS en 38400 y salga de SMIT.

6. Añada la línea siguiente al archivo /usr/lib/uucp/Devices tanto en bronce como en oro:

```
Direct tty1 - 38400 direct
```

7. Cree una interfaz de red de **SLIP** en **bronce**.

a) Escriba:

```
smit mkinet1sl
```

b) Para el PUERTO TTY para la interfaz de red de SLIP, seleccione **tty1**.

c) Especifique la DIRECCIÓN DE INTERNET como, por ejemplo, 130.130.130.1.

d) Especifique la dirección de DESTINO (de oro) como, por ejemplo, 130.130.130.2 y seleccione Aceptar o Intro.

e)

8. Cree una interfaz de red de **SLIP** en oro. Siga el mismo procedimiento que para bronce (en el paso 5) pero intercambie la DIRECCIÓN DE INTERNET y la dirección de DESTINO.

9. Añada las dos entradas siguientes al archivo /etc/hosts tanto en bronce como en oro:

```
130.130.130.1    bronce  
130.130.130.2    oro
```

El nombre que asigne debe ser exclusivo. En otras palabras, si a la interfaz de red en anillo de bronce ya se le ha asignado el nombre bronce, asigne a la interfaz de **SLIP** un nombre como, por ejemplo bronce\_slip.

10. Inicie **SLIP** tanto en bronce como en oro. Escriba:

```
slattach tty1
```

11. Pruebe la conexión de **SLIP**.

a) En bronce, escriba:

```
ping oro
```

b) En oro, escriba:

```
ping bronce
```

Si ambas pruebas son satisfactorias, la conexión de **SLIP** está lista para su utilización. En caso contrario, vuelva al paso 5 y verifique que la configuración sea correcta tanto en bronce como en oro.

#### Desactivación de una conexión SLIP

Para desactivar una conexión **SLIP**, utilice el procedimiento siguiente.

1. Escriba:

```
ps -ef | grep slatt
```

Observe los números de los procesos asociados con el mandato **slattach**.

2. Para cada número de proceso, escriba:

```
kill número_proceso
```

No utilice el distintivo -9 del mandato **kill**.

Si **slattach** se ha eliminado accidentalmente con un distintivo -9, es posible que continúe un bloqueo latente en /etc/locks. Suprima este archivo de bloqueo para hacer limpieza después de **slattach**.

Para desactivar una conexión **SLIP** temporalmente, realice lo siguiente tanto en el sistema local como en el remoto:

1. Escriba:

```
ifconfig sl# down
```

2. Liste los procesos **slattach** que se estén ejecutando actualmente utilizando el mandato:

```
ps -ef | grep slat
```

La salida podría ser similar a la siguiente:

```
root 1269 1 0 Jun 25 ... slattach
```

3. Elimine el proceso **slattach** utilizando el ID del proceso. Por ejemplo, para eliminar el proceso **slattach** que se muestra en el ejemplo anterior, escriba:

```
kill 1269
```

donde 1269 es el ID del proceso **slattach**. No elimine el proceso **slattach** utilizando el distintivo -9 del mandato **kill**.

La conexión **SLIP** está ahora inhabilitada.

### Activación de una conexión SLIP

Siga las instrucciones siguientes para activar una conexión **SLIP** que esté inhabilitada temporalmente.

Ejecute estos mandatos tanto en el sistema local como en el sistema remoto.

1. Escriba:

```
ifconfig sl# up
```

2. Vuelva a emitir el mandato **slattach** utilizado inicialmente.

### Eliminación de una interfaz SLIP

Utilice estas instrucciones para eliminar completamente una interfaz **SLIP**.

Después de ejecutar estas instrucciones, se eliminan tanto la interfaz sl# como el proceso **slattach** asociado al mismo. Las entradas creadas en el archivo /etc/hosts permanecerán y deberán eliminarse manualmente.

1. Para eliminar la interfaz **SLIP** y el proceso **slattach** asociado a la misma, utilice la vía rápida smit rminet para acceder a la pantalla **Interfaces de red disponibles**.
2. Seleccione la entrada adecuada en la pantalla **Interfaces de red disponibles** y seleccione **Ejecutar**.

**Nota:** Las entradas creadas en el archivo /etc/hosts permanecerán y deberán eliminarse manualmente.

### Resolución de problemas en SLIP

Estos mandatos son necesarios para depurar problemas en **SLIP**.

Cada mandato viene con un ejemplo de cómo se utiliza el mandato para la resolución de problemas en **SLIP**.

Además, se proporciona una lista de los problemas y mensajes de error frecuentes para su consulta.

### Mandato netstat

El mandato **netstat** funciona en conjunto con el mandato **ifconfig** para proporcionar una condición de estado de la interfaz de red TCP/IP.

El mandato **netstat -in** utiliza por ejemplo el distintivo **-i** para presentar información sobre las interfaces de red, mientras que el distintivo **-n** imprime las direcciones IP en lugar del nombre de los sistemas principales. Utilice este mandato para verificar las interfaces SLIP, las direcciones y el nombre de los sistemas principales. El apartado siguiente describe la salida de **netstat -in**.

Programe el módem utilizando los valores que se muestran en el apartado “[Consideraciones sobre los módems de SLIP](#)” en la página 711. El ejemplo siguiente muestra cómo programar y guardar los valores básicos para un módem compatible con Hayes. Escriba:

Name	Mtu	Network	Address	Ipkts	Ierrrs	Opkts	Oerrrs	Col
lo0	1536	<Enlace>		2462	0	2462	0	0
lo0	1536	127	localhost.austi	2462	0	2462	0	0
tr0	1492	<Enlace>		1914560	0	21000	0	0
tr0	1492	129.35.16	glad.austin.ibm	1914560	0	21000	0	0
s10	552	1.1.1.0	1.1.1.1	48035	0	54963	0	0
sl1*	552	140.252.1	140.252.1.5	48035	0	54963	0	0

Fíjese en el \* junto a la interfaz sl1. Indica que la interfaz de red está desactivada o no está disponible para su utilización. El usuario puede corregir esto emitiendo el mandato **ifconfig sl1 up** si se trata de una interfaz **SLIP** válida.

**netstat** proporciona estadísticas respecto al número de paquetes de entrada y de salida, así como los errores de entrada y salida, que resultan útiles al solucionar problemas de conexión de **SLIP**.

Por ejemplo, un usuario emite una operación **ping** para un sistema principal remoto a través de un enlace **SLIP** y el mandato **ping** parece colgarse. El usuario ejecutó con rapidez un mandato **netstat -in** desde otro shell de mandatos y observó que el valor de Opkts aumentaba pero que no había ningún Ipkts desde el sistema principal remoto. Esto indica que el sistema remoto no devuelve (o no recibe) la información. El usuario debe ejecutar el mismo mandato **netstat** en el sistema remoto para verificar la recepción de los paquetes **ping** o aumentar la cuenta de errores.

La conversión del nombre de los sistemas principales en números de Internet depende de la resolución de nombres y, por lo tanto, resulta crucial para el funcionamiento correcto de una línea **SLIP**. Para depurar problemas de direccionamiento, de alias o de nombres del sistema principal, utilice el mandato **netstat -rn**. El nombre base del sistema principal o el nombre del sistema principal es el único nombre que debe devolverse desde el archivo **/etc/hosts**. Si un servidor de nombres presta servicio a la máquina (es decir, si existe **/etc/resolv.conf**), el servidor de nombres devolverá el nombre de dominio cualificado al completo en este mandato.

### Mandato ifconfig

El mandato **ifconfig** es la herramienta de configuración de la interfaz de red que permite la creación dinámica de la ESTRUCTURA de la interfaz de red y su supresión de la memoria del kernel.

Este mandato acepta datos de la línea de mandatos y, a continuación, crea una estructura de memoria que se ajusta a los parámetros. Con fines de depuración, el mandato **ifconfig** se utiliza para examinar el estado de la interfaz de comunicaciones.

**Nota:** Los cambios realizados en los atributos de una interfaz utilizando el mandato **ifconfig** se perderán cuando se rearanje el sistema.

Por ejemplo, para examinar el estado actual de la interfaz sl1:

1. Escriba el mandato **netstat -i** y examine la salida seleccionando la interfaz sl# adecuada. Por ejemplo, sl0, sl1, sl2 y así sucesivamente.
2. Escriba el mandato **ifconfig sl#** y examine la salida de ifconfig para los campos clave siguientes:

Item	Descripción
<b>El distintivo POINTTOPOINT (punto a punto)</b>	Este distintivo siempre debe estar presente en un enlace SLIP operativo. En caso contrario, el enlace podría encontrarse en estado desactivado o desconectado. Vuelva a intentar emitir los mandatos <b>ifconfig sl# up</b> y <b>ifconfig sl#</b> para ver si cambia la condición.
<b>El distintivo UP (activada)</b>	Indica que la interfaz de red sl# está activada y debería estar operativa.
<b>El distintivo RUNNING (en ejecución)</b>	Indica que el mandato <b>slattach</b> ha sido satisfactorio. Es decir, que se ha accedido al enlace, se ha realizado una marcación, el otro extremo ha contestado y el extremo remoto ha devuelto el estado DETECCIÓN DE PORTADORA. Cuando se produce el estado de CD, los distintivos se actualizan con el bit en ejecución.

#### **Mandatos pdisable y lsdev**

Los puertos tty que se utilicen para las conexiones **SLIP** deben estar en estado no disponible o inhabilitado.

Para verificar que el puerto para tty1 esté inhabilitado, obtenga autorización de usuario root y escriba uno de los mandatos siguientes:

- **lsattr -El tty1 -a login**

Este mandato visualiza el estado permanente del puerto tty tal como se registra en el Gestor de datos de objeto (ODM) del sistema. Si la salida es distinta de **login disable**, utilice SMIT para cambiar el valor del campo LOGIN de enable (habilitar) a **disabled** (inhabilitar).

- **pdisable | grep tty1**

Este mandato, cuando se utiliza sin parámetros, visualiza todos los puertos tty que se encuentran en estado inhabilitado. En este ejemplo, **pdisable** está interconectado con el mandato **grep** para eliminar la salida innecesaria. Si no se visualiza tty1 después de ejecutar este mandato, el puerto no está inhabilitado.

#### **Mando ps**

El mando **ps** visualiza información sobre los procesos activos en la salida estándar.

Utilice este mando para verificar la existencia (o la inexistencia) de procesos **slattach** que se utilicen para asignar una línea tty a interfaces de red.

Si **netstat -in** muestra que la interfaz está desactivada, el usuario debe ejecutar el mando **ps -ef | grep slat** para ver si actualmente se está ejecutando un proceso **slattach** en el puerto tty asociado. Observe que para una interfaz **SLIP** conectada directamente, las conexiones interrumpidas vuelven a intentarse de forma automática sin intervención manual. Para una interfaz **SLIP** conectada por módem, las conexiones interrumpidas deben volver a marcarse manualmente. Si un usuario proporciona una serie de marcación en la línea de mandatos **slattach**, el usuario debe volver a escribir el mando y la serie de marcación para restaurar una conexión interrumpida.

#### **El mando ping y las luces del módem**

El mando **ping** y las luces del módem se utilizan para depurar los problemas de comunicación **SLIP**.

Un mando ping consiste en un paquete de peticiones de eco que se envía desde la máquina y en un paquete de respuestas de eco que se devuelve. Esta secuencia de sucesos resulta útil si el administrador puede ver las luces del módem.

Por ejemplo, un sistema local construye el paquete de peticiones de eco y lo envía al sistema remoto. La luz de envío de datos (SD) del módem local se ilumina. Esto significa que el TCP/IP local, **slattach** y tty han podido agrupar la información y enviarla desde el módem al sistema remoto.

El módem remoto recibe el paquete y la luz de recepción de datos parpadea pero la luz de envío de datos (SD) no lo hace. Esto significa que el sistema remoto no ha podido enviar (o devolver) la petición de ping del sistema local. Como resultado, es posible que el usuario del sistema local vea que el mando **ping** se ha colgado y deba pulsar Control-C para salir de esta condición.

La causa más frecuente de este problema es la utilización del control de flujo XON/XOFF en uno o en ambos módems. Sin embargo, el usuario no debería descartar la posibilidad de conflictos de direccionamiento o de dirección en los sistemas.

#### **Problemas y mensajes de error frecuentes en SLIP**

Aquí pueden consultarse problemas y mensajes de error de **SLIP** frecuentes, las causas posibles de los mismos y las acciones del usuario sugeridas.

**Mensaje:** 0821-296 No se puede establecer la disciplina de línea para /dev/tty# en slip.ioctl(TXSETLD). Una llamada del sistema ha recibido un parámetro que no es válido.

**Causas posibles:** Este tipo de error normalmente se produce al iniciar el proceso **slattach** y se atribuye a una configuración incorrecta de SLIP. Es muy probable que el problema se deba a una discrepancia entre el número del dispositivo tty y el número de la interfaz sl. Esto también explica por qué el sistema ha indicado que ifconfig no se había ejecutado antes de **slattach**.

Este problema también puede producirse cuando los procesos **slattach** se descartan o eliminan incorrectamente o cuando el usuario intenta mover una conexión **SLIP** a otro puerto tty y olvida reconfigurar la interfaz sl# para que coincida con el tty. Compruebe si algún proceso **slattach** todavía está en ejecución (utilizando, por ejemplo, ps -ef | grep slat).

**Acción:** El dispositivo tty para SLIP es **/dev/tty24** y el usuario ha creado una interfaz sl0. Esto no es correcto. El usuario debe crear una interfaz sl24 que coincida con el número del tty (tty24 y sl24). Si el problema continúa, el usuario debe desactivar la interfaz sl (consulte "Desactivación de una interfaz SLIP") y volver a configurar la conexión utilizando los mandatos siguientes:

```
lsdev -Cc if -s SL
lsattr -El sl0
```

#### **Mensaje:**

La red no está disponible actualmente

El direccionamiento con el sistema principal remoto no está disponible

**Causa posible:** Estos errores se producen con mayor frecuencia cuando un usuario intenta realizar ping con un sistema principal a través del enlace **SLIP** y el enlace se ha establecido incorrectamente. El problema más probable es que los dos puertos asociados con la interfaz sl# se encuentren en estado habilitado. También es posible que exista un conflicto de direcciones o de rutas entre los sistemas principales.

#### **Acciones:**

- Elimine la interfaz sl# utilizando la vía de acceso smit rminet. Esto debe realizarse en el sistema principal local y remoto de SLIP.
- Realice lo siguiente para cada sistema principal de SLIP:
  1. Escriba pdisable | grep tty#.
  2. Si el dispositivo tty NO aparece en la salida del mandato anterior, el tty no está inhabilitado. Inhabilite el tty utilizando SMIT o la línea de mandatos. Con los puertos tty inhabilitados, utilice SMIT para volver a crear las interfaces de **SLIP** en ambos sistemas. Si el problema persiste, verifique las direcciones de la red y las rutas (si las hay). Utilice el mandato netstat -ir para ver la dirección, la ruta y la información de la interfaz con rapidez.

**Problema:** Cuando el sitio remoto llama al sistema principal local, el módem del sistema principal local se conecta pero no realiza el proceso de inicio de sesión.

**Causas posibles:** Si los dos módems se conectan y empiezan el reconocimiento o intercambian información sobre la conexión pero entonces se desconectan, el problema puede deberse a los códigos de resultado del módem. Este problema también puede provocarlos una serie de marcación **slattach** incorrecta. Si los dos módems marcan pero no llegan a empezar el proceso de reconocimiento, el problema puede ser que el módem no esté establecido para la contestación automática.

#### **Acciones:**

1. Pruebe la conexión del módem primero con el mandato **cu**. El módem del sistema principal remoto debe permitir que el usuario inicie la sesión en el sistema. No deben aparecer residuos en la pantalla durante el intento de inicio de sesión; si es así, ello puede indicar una línea telefónica con ruidos, lo que puede ser parte del problema. Durante el inicio de sesión, varios avisos de inicio de sesión *no* deben desplazarse por la pantalla. Si están presentes, ello puede indicar de nuevo una línea telefónica con problemas o valores del módem incorrectos.
2. Compruebe las configuraciones del módem e intente desactivar los códigos ARQ si actualmente están activados. En la mayoría de los módems compatibles con Hayes, se trata del valor &A0. La inhabilitación de los códigos de resultados ARQ no afecta a las conexiones controladas mediante errores ni impide que el módem devuelva mensajes CONNECT estándares (si los códigos de resultados están habilitados) tal como es necesario para la serie de marcación **slattach**.

**Problema:** El usuario no puede realizar **ping** a través de una conexión **SLIP** por módem. El mandato **ping** puede colgarse o devolver mensajes de error.

#### **Causas posibles:**

1. Los módems y/o los puertos tty pueden estar configurados para utilizar el control de flujo XON/XOFF.
2. Es posible que el proceso **slattach** se haya terminado en el sistema principal remoto o que la conexión del módem se haya descartado.
3. Las direcciones asignadas a los sistemas principales de **SLIP** pueden ser incorrectas.

#### **Acciones:**

1. Examine las configuraciones de los módems locales y remotos. Deben estar establecidas para utilizar el control de flujo RTS/CTS (hardware) o para no utilizar ningún control de flujo. El usuario debe intentar ejecutar ping desde cada sistema. Ejecute ping del sistemaA al sistemaB.
2. Verifique que el proceso **slattach** todavía esté en ejecución tanto en el sistema local como en el remoto. Utilice el mandato: `ps -ef |grep slat`. Verifique que la interfaz sl# esté en un estado en ejecución. Utilice el mandato: `ifconfig sl#`.
3. Verifique que no exista ningún conflicto entre las direcciones de **SLIP** y aquellas asociadas con la otra interfaz de red (si las hay). Utilice el mandato: **netstat -ir**. Si la dirección o la clase de dirección es cuestionable, vuelva a configurar **SLIP** utilizando un esquema de dirección más sencillo como, por ejemplo, 1.1.1.1 para el sistema principal local y 1.1.1.2 para el sistema principal remoto.

#### **Cuestionario sobre SLIP**

Utilice este cuestionario para registrar los datos sobre las configuraciones de **SLIP**.

La información recopilada en estas hojas puede enviarse por fax a un representante de servicio cuando se requiera asistencia adicional con la configuración de **SLIP**.

1. ¿Esa configuración de **SLIP** funcionaba anteriormente? (S/N) \_\_\_\_\_

2. ¿De qué tipo de máquinas se trata? (Por ejemplo: UNIX/PC, DOS/PC, etc.)

Sistema local: \_\_\_\_\_ Sistema remoto: \_\_\_\_\_

Si el sistema principal no es un sistema IBM UNIX, indique el tipo de software que se utiliza para establecer la conexión **SLIP**.

3. ¿Qué versiones del sistema operativo IBM UNIX hay en cada una de las unidades del sistema? Emite el mandato `/bin/oslevel`. Si este mandato no se reconoce, utilice el método siguiente:

```
1slpp -h bos.rte
```

look for the *active commit* line release level.

Sistema local: \_\_\_\_\_ Sistema remoto: \_\_\_\_\_

4. Lista todas las interfaces disponibles en ambos sistemas (por ejemplo, sl0, sl1). Para ello, utilice el mandato: lsdev -Cc if

Sistema local: \_\_\_\_\_ Sistema remoto: \_\_\_\_\_

-----  
-----  
-----

El número de interfaz de **SLIP** debe coincidir con el número de dispositivo tty. Por ejemplo, /dev/tty53 debe utilizarse con sl53.

5. ¿**SLIP** se está configurando a través de SMIT o mediante mandatos? Las configuraciones de SLIP mediante mandatos no son permanentes y no están presentes después de rearrancar el sistema.

-----

6. ¿**SLIP** se está configurando a través de módems o como una línea serie directa?

-----

7. Si se están utilizando módems, liste el fabricante y el tipo de módem para los sistemas locales y remotos.

TIPO	VELOCIDAD EN BAUDIOS (Sí/No)	CABLEADO DE IBM Si no es un cable IBM, ¿qué tipo?
Local: _____	---	-----
Remoto: _____	---	-----

8. Si se utilizan módems, ¿cuál es el tipo de portadora del teléfono? (línea de alquiler o con conmutación normal)

-----

9. ¿En qué hardware se está utilizando la línea **SLIP**?

Adaptador de 128 puertos (con RAN de 16 puertos): \_\_\_\_

Adaptador de 2 puertos: \_\_\_\_

Adaptador de 8 puertos: \_\_\_\_

Puertos serie S1 o S2 nativos: \_\_\_\_

10. ¿Es posible realizar ping desde el sistema local al sistema remoto?

(S/N) \_\_\_\_\_ (en el sistema local escriba: ping <dirección remota> )

11. ¿Es posible realizar ping desde el sistema remoto al sistema local?

(S/N) \_\_\_\_\_ (en el sistema remoto escriba: ping <dirección local> )

12. ¿Los puertos del tty están inhabilitados tanto en el sistema local como en el remoto?

(S/N) \_\_\_\_\_

Utilice el mandato: pdisable | grep tty#. Sólo los números de tty inhabilitados se muestran como salida a este mandato.

13. ¿Se visualiza algún mensaje de error? En este caso, lístelos a continuación:

-----  
-----  
-----  
-----

## Asynchronous Terminal Emulation

El programa Asynchronous Terminal Emulation (ATE) permite a los terminales del sistema operativo emular un terminal, proporcionando de este modo una forma en que los usuarios pueden conectarse a la mayoría de otros sistemas compatibles con terminales asíncronos.

ATE lo consigue haciendo que el sistema remoto vea un terminal como una pantalla del sistema o como un terminal DEC VT100. La opción VT100 permite al usuario iniciar la sesión en sistemas que no sean compatibles con el terminal, pero que sí lo sean con los terminales VT100.

ATE utiliza tanto las conexiones directas (por cable) como las conexiones por módem para la comunicación entre el sistema del usuario y un sistema remoto, tal como se muestra en la ilustración siguiente.

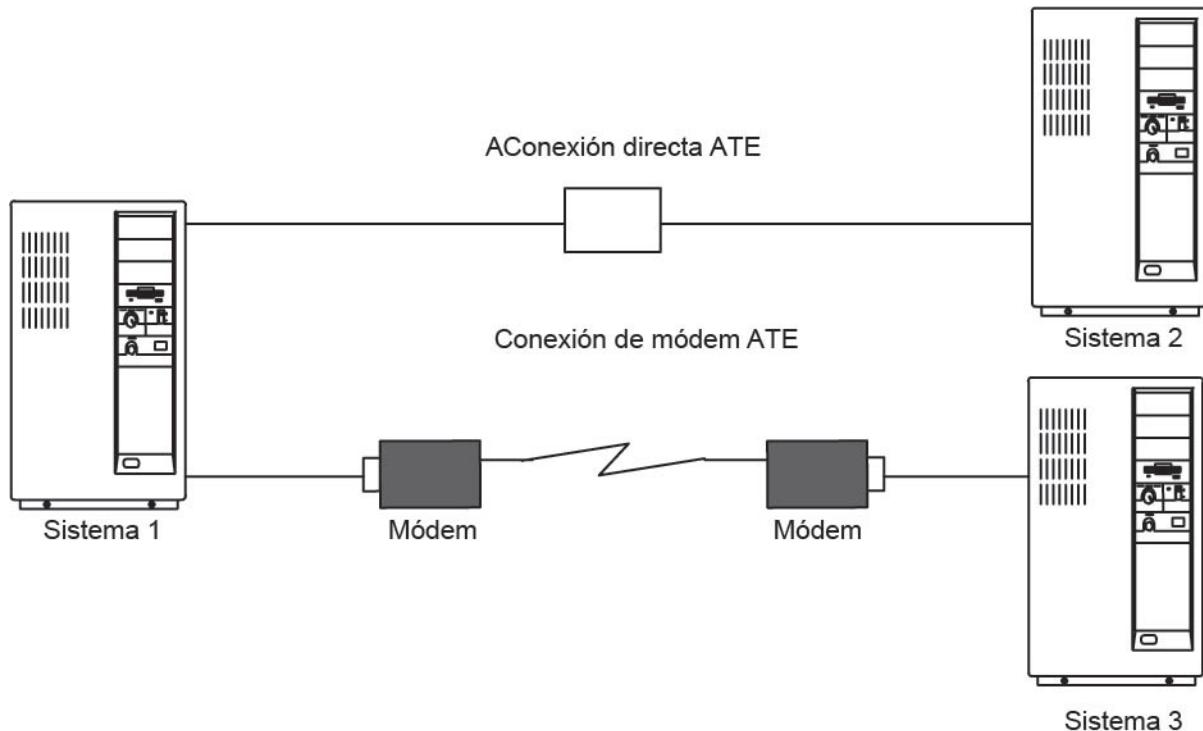


Figura 41. Tipos de conexiones ATE

En función del tipo de conexión utilizado, el usuario puede configurar ATE para que se conecte con un sistema de la habitación contigua o con un sistema al otro extremo del país. Para una conexión directa, el usuario debe conocer el puerto que debe utilizarse en el sistema. Para una conexión por módem, los usuarios deben conocer el puerto que debe utilizarse en el sistema y el número de teléfono del sistema remoto. Los usuarios también deben tener un ID de inicio de sesión y una contraseña en el sistema remoto.

ATE permite a un usuario ejecutar mandatos en el sistema remoto, enviar y recibir archivos y utilizar el protocolo **xmodem** para comprobar la integridad de los datos en los archivos transferidos entre sistemas. El usuario también puede capturar y archivar los datos procedentes del sistema remoto.

**Nota:** Para utilizar ATE, debe ser miembro del grupo UNIX-to-UNIX Copy Program (UUCP). Los usuarios con autorización root utilizan System Management Interface Tool (SMIT) para instalar usuarios individuales en grupos.

### Configuración de ATE

Antes de ejecutar ATE, el administrador del sistema debe instalar el software adecuado (si es necesario) y configurar los puertos y las conexiones de tty.

- ATE es un producto opcional del programa. Todos los archivos necesarios para el funcionamiento de ATE se encuentran en el producto del programa **bos.net.ate**, disponible en el soporte de almacenamiento de instalación. Utilice los mandatos siguientes para verificar que ATE esté disponible en su sistema:

```
lslpp -h | more    <retorno>
/bos.net.ate      <retorno>
```

Si ATE no está disponible en su sistema, instale la imagen de **bos.net.ate** desde el soporte de almacenamiento de instalación (cinta, disquete o servidor de red).

- Si ATE está instalado en el sistema, puede visualizarse una lista de los archivos asociados con este programa utilizando los mandatos siguientes:

```
lslpp -f | more    <retorno>
/bos.net.ate      <retorno>
```

- El usuario debe tener autorización de usuario root para configurar el puerto para el dispositivo de comunicación.

ATE utiliza tanto conexiones directas(por cable) como conexiones por módem. Las conexiones locales RS-232C permiten una distancia máximo de 15 metros (50 pies) entre las máquinas y las conexiones RS-422A permiten una distancia de hasta 1.200 metros (4000 pies) entre las máquinas.

Antes de utilizar ATE para llamar a un sistema remoto, verifique que el dispositivo de tty del sistema remoto esté listo para aceptar una llamada.

Para preparar ATE para su ejecución en el sistema, realice los pasos siguientes:

1. Instale una tarjeta de un adaptador asíncrono en la ranura adecuada de la unidad del sistema, a menos que el sistema tenga un puerto serie incorporado.
2. Conecte el cable RS-232C o RS-422A en la tarjeta del adaptador o en el puerto serie incorporado.
3. Añada el dispositivo de tty para el puerto de comunicación utilizando la vía rápida smit mkdev.
4. Seleccione el tipo de terminal que debe emularse con ATE y efectúe los ajustes necesarios para el entorno.

Los cambios más frecuentes son la velocidad de la línea, los valores de paridad, el número de bits por carácter y si la línea debe controlarse como una línea remota o local. Utilice bpc 8 y ninguna paridad si se necesita soporte a idiomas nacionales (NLS).

5. Configure el puerto para el dispositivo.

Para configurar un puerto para realizar llamadas de salida con ATE, utilice el mandato **pdisable**. Por ejemplo, para configurar el puerto tty1, escriba:

```
pdisable tty1
```

Para configurar un puerto para que otros realicen llamadas de entrada, utilice el mandato **penable**. Por ejemplo, para permitir que otros sistemas realicen llamadas de entrada en el puerto tty2, escriba:

```
penable tty2
```

6. Asegúrese de que el dispositivo se haya definido en el sistema remoto previamente.

Una vez se ha definido el dispositivo, el programa ATE debe personalizarse para reflejar los valores del dispositivo en el sistema remoto. Personalice los valores predeterminados con los submandatos alter

y modify o editando el archivo predeterminado `ate.def`. Para cambiar los valores predeterminados para una conexión telefónica, utilice una entrada del archivo del directorio de marcación.

### Menús principales de ATE

ATE visualiza menús distintos en función de los submandatos que se utilicen.

Si inicia ATE con el mandato **ate**, se visualizará el menú Unconnected Main Menu, que le permite:

- Cambiar temporalmente las características de ATE (**modify, alter**)
- Conectarse a otro sistema (**directory, connect**)
- Obtener ayuda (**help**)
- Ejecutar mandatos del sistema operativo de la estación de trabajo en el sistema (**perform**)
- Salir de ATE (**quit**)

En función del submandato emitido desde el Unconnected Main Menu (Menú principal no conectado), ATE visualiza diversos submenús:

Tabla 110. Submenús de ATE	
Cuando se utiliza	ATE visualiza
submandato <b>modify</b>	Modify Menu (para obtener información, consulte el mandato <a href="#">ate</a> )
Submandato <b>alter</b>	Alter Menu (para obtener información, consulte el mandato <a href="#">ate</a> )
Submandato <b>connect</b> o <b>directory</b> para conectarse a un sistema remoto	Connected Main Menu
Submandato <b>directory</b>	directorio de marcación (una lista de números de teléfono)

Desde Connected Main Menu, puede emitir submandatos para:

- Enviar y recibir archivos del sistema remoto (**send, receive**)
- Enviar una señal de interrupción al sistema remoto (**break**)
- Finalizar la conexión con el sistema remoto (**terminate**)

Además, los submandatos **modify, alter, help, perform** y **quit** realizan las mismas funciones que los que se proporcionan con el Unconnected Main Menu.

Puede controlar determinadas acciones de ATE con secuencias de teclas de control. Estas secuencias de teclas reciben el nombre de CAPTURE\_KEY, MAINMENU\_KEY y PREVIOUS\_KEY. Las secuencias de teclas aparecen descritas en el apartado “Secuencias de teclas de control en ATE” en la página 727. ATE se instala con combinaciones de teclas predeterminadas para dichas teclas, pero las combinaciones de teclas se pueden cambiar modificando el archivo de ATE por omisión, `ate.def`.

### Unconnected Main Menu de ATE

Utilice el mandato **ate** para visualizar el Unconnected Main Menu de ATE.

Después de establecer una conexión, utilice el submandato **connect** de ATE para visualizar el Unconnected Main Menu.

Desde el Unconnected Main Menu de ATE se pueden emitir los submandatos siguientes. Para emitir el submandato, escriba la primera letra del submandato en el indicador de mandatos del menú. Por ejemplo, escriba **d** para emitir el submandato **directory**.

Item	Descripción
<b>alter</b>	Cambia temporalmente las características de transmisión de datos como, por ejemplo, la velocidad de transmisión.

<b>Item</b>	<b>Descripción</b>
<b>connect</b>	Establece una conexión.
<b>directory</b>	Visualiza un directorio de marcación.
<b>help</b>	Visualiza información de ayuda.
<b>modify</b>	Modifica temporalmente los valores locales como, por ejemplo, el archivo de captura para los datos de entrada.
<b>perform</b>	Le permite ejecutar mandatos de sistema operativo de la estación de trabajo con ATE.
<b>quit</b>	Sale del programa ATE.

**Nota:** De las secuencias de teclas de control CAPTURE\_KEY, MAINMENU\_KEY y PREVIOUS\_KEY, sólo se puede utilizar PREVIOUS\_KEY desde el Unconnected Main Menu de ATE.

#### ***Connected Main Menu de ATE***

Utilice el submandato **connect** desde el Unconnected Main Menu de ATE para visualizar el Connected Main Menu.

También puede pulsar MAINMENU\_KEY mientras esté conectado a un sistema remoto.

Desde el Connected Main Menu de ATE se pueden emitir los submandatos siguientes. Para ver las definiciones de estos submandatos, consulte el mandato [ate](#). Para emitir el submandato, escriba la primera letra del submandato en el indicador de mandatos del menú. Por ejemplo, escriba a para emitir el submandato **alter**.

<b>Item</b>	<b>Descripción</b>
<b>alter</b>	Cambia temporalmente las características de transmisión de datos como, por ejemplo, la velocidad de transmisión.
<b>break</b>	Envía una señal de interrupción al sistema remoto.
<b>help</b>	Visualiza información de ayuda.
<b>modify</b>	Modifica temporalmente los valores locales que utiliza el emulador como, por ejemplo, el archivo de captura para los datos de entrada.
<b>perform</b>	Le permite ejecutar mandatos de sistema operativo de la estación de trabajo con ATE.
<b>quit</b>	Sale del programa ATE.
<b>receive</b>	Recibe archivos de un sistema remoto.
<b>send</b>	Envía archivos a un sistema remoto.
<b>terminate</b>	Finaliza la conexión de ATE.

Desde el Connected Main Menu de ATE, se pueden utilizar las tres secuencias de teclas de control de ATE.

#### **Secuencias de teclas de control en ATE**

Utilice las siguientes teclas de control con ATE. Modifique la secuencia de teclas para cada función editando el archivo `ate.def`.

Item	Descripción
CAPTURE_KEY	<p>Inicia o detiene la operación para guardar los datos que aparecen en la pantalla durante una conexión. La secuencia de teclas por omisión para CAPTURE_KEY es Control-B.</p>
	<p>CAPTURE_KEY tiene un efecto de alternancia o commutación. Al pulsar esta tecla de control, se empezarán a guardar los datos. Si vuelve a pulsarla, la operación se detendrá. Los datos se guardan en el archivo de captura definido en el archivo <code>ate.def</code>.</p>
	<p>El nombre del archivo de captura por omisión es el archivo <code>\$HOME/kapture</code>. Utilice el submandato <b>modify</b> para modificar temporalmente este nombre. Edite el archivo por omisión de ATE para cambiar de forma permanente el nombre del archivo de captura. Consulte el apartado “<a href="#">Edición del archivo de ATE por omisión</a>” en la página 737.</p>
	<p>La secuencia de teclas CAPTURE_KEY no funciona mientras el terminal está realizando una operación de transferencia de archivos y sólo es válida cuando se establece una conexión. Si pulsa la secuencia de teclas CAPTURE_KEY antes de establecer una conexión, el siguiente mandato que se entre no se ejecutará satisfactoriamente y se visualizará un mensaje de error.</p>
PREVIOUS_KEY	<p>Le devuelve a la pantalla de visualización anterior. PREVIOUS_KEY también se utiliza para detener una operación de transferencia de archivos. La secuencia de teclas por omisión para PREVIOUS_KEY es Control-R.</p>
	<p>PREVIOUS_KEY se puede utilizar desde cualquier menú principal de ATE.</p>
MAINMENU_KEY	<p>Visualiza el Connected Main Menu para que pueda emitir un submandato de ATE. La secuencia de teclas por omisión para MAINMENU_KEY es Control-V. Utilice esta tecla de control para visualizar el Connected Main Menu tras establecer una conexión con un sistema remoto.</p>
	<p>Si pulsa la secuencia de teclas MAINMENU_KEY antes de establecer una conexión, el siguiente mandato que se entre no se ejecutará satisfactoriamente y se visualizará un mensaje de error.</p>
	<p>Si personaliza el archivo por omisión de ATE, podrá cambiar de forma permanente los valores de las teclas de control y el nombre del archivo de captura. Consulte el apartado “<a href="#">Edición del archivo de ATE por omisión</a>” en la página 737.</p>

### Personalización de ATE

ATE crea el archivo predeterminado `ate.def` en el directorio actual la primera vez que el usuario ejecuta ATE. Edite el archivo `ate.def` para personalizar distintos aspectos de ATE.

Por ejemplo, el usuario puede cambiar el nombre del archivo de directorio de marcación, el tipo de protocolos de transferencia utilizados para enviar y recibir archivos desde el sistema remoto y la velocidad en baudios que ATE espera que el módem utilice. Consulte el apartado “[Edición del archivo de ATE por omisión](#)” en la página 737 para obtener más información sobre el archivo `ate.def`.

Los usuarios pueden realizar cambios temporales en ciertos aspectos de ATE con los submandatos **modify** y **alter**. Estos submandatos pueden cambiar todos los valores predeterminados de ATE a excepción de las secuencias de teclas de control (que sólo pueden cambiarse editando el archivo predeterminado) y el nombre del directorio de marcación (que puede cambiarse con el submandato **directory** o editando el archivo por omisión). Los cambios realizados con los submandatos **modify**, **alter** o **directory** sólo son aplicados a la sesión de ATE actual. La siguiente vez que el usuario ejecute ATE, los valores utilizados serán los definidos en el archivo predeterminado.

Cuando se utiliza un módem con ATE, el usuario puede crear un directorio de marcación con un máximo de 20 números de teléfono. El submandato **directory** visualiza los números de teléfono en forma de

menú y permite al usuario seleccionar el sistema al que desea llamar. Consulte el apartado “Configuración de un directorio de marcación de ATE” en la página 733 para obtener más información.

Al utilizar un directorio de marcación, el usuario se ahorra el tener que buscar el número de teléfono cuando llame a un sistema determinado. El usuario también puede especificar determinadas características de transmisión de datos en el archivo del directorio de marcación. Esto resulta útil si algunas conexiones utilizan características distintas de los valores predeterminados de ATE.

Puede crear un directorio de marcación personalizado y el administrador del sistema puede crear un directorio de marcación para todo el sistema. Especifique el directorio de marcación que se va a utilizar en el archivo de ATE predeterminado. Consulte el apartado “Configuración de un directorio de marcación de ATE” en la página 733 para obtener más información.

#### **Archivo de configuración ate.def**

El archivo `ate.def` establece los valores predeterminados que deben utilizarse en las conexiones asíncronas y en las transferencias de archivos.

Este archivo se crea en el directorio actual durante la primera ejecución de ATE. El archivo `ate.def` contiene los valores predeterminados que el programa ATE utiliza para las siguientes tareas:

- Características de transmisión de datos
- Funciones del sistema local
- Archivo del directorio de marcación
- Teclas de control.

La primera vez que se ejecuta el programa ATE desde un directorio en concreto, éste crea un archivo `ate.def` en dicho directorio.

```
LENGTH      8
STOP        1
PARITY      0
RATE        1200
DEVICE      tty0
INITIAL    ATDT
FINAL
WAIT        0
ATTEMPTS   0
TRANSFER   p
CHARACTER  0
NAME        kapture
LINEFEEDS  0
ECHO        0
VT100       0
WRITE       0
XON/XOFF   1
DIRECTORY  /usr/lib/dir
CAPTURE_KEY 002
MAINMENU_KEY 026
PREVIOUS_KEY 022
```

Edita el archivo `ate.def` con cualquier editor de textos ASCII para modificar los valores de estas características de forma permanente. Modifique los valores de estas características de forma temporal con los submandatos **alter** y **modify** de ATE, a los que se accede desde el menú principal de ATE.

Escriba el nombre de los parámetros en mayúsculas en el archivo `ate.def`. Escriba los parámetros exactamente como aparezcan en el archivo predeterminado original. Defina solamente un parámetro por línea. Si el valor definido para un parámetro no es correcto, ATE devuelve un mensaje del sistema. Sin embargo, el programa continúa ejecutándose utilizando el valor predeterminado. Éstos son los parámetros del archivo `ate.def`:

#### **LENGTH**

Especifica el número de bits de un carácter de datos. Esta longitud debe coincidir con la longitud que el sistema remoto espere.

Opciones: 7 u 8  
Valor predeterminado: 8

### **STOP**

Especifica el número de bits de parada que se añaden a un carácter para indicar el final del mismo durante la transmisión de datos. Este número debe coincidir con el número de bits de parada que el sistema remoto utilice.

Opciones: 1 o 2  
Valor predeterminado: 1

### **PARITY**

Comprueba si un carácter se ha transmitido satisfactoriamente a o desde un sistema remoto. Debe coincidir con la paridad del sistema remoto.

Por ejemplo, si el usuario selecciona la paridad par, cuando el número de bits 1 del carácter sea impar, el bit de paridad se activa para formar un número par de bits 1.

Opciones: 0 (ninguna), 1 (impar) o 2 (par)  
Valor predeterminado: 0.

### **RATE**

Determina la velocidad en baudios o el número de bits transmitidos por segundo (bps). La velocidad debe coincidir con la velocidad del módem y con la del sistema remoto.

Opciones: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200  
Valor predeterminado: 1200

### **DISPOSI- TIVO**

Especifica el nombre del puerto asíncrono utilizado para realizar una conexión con un sistema remoto.

Opciones: Nombres de puertos creados localmente.  
Valor predeterminado: tty0.

### **INITIAL**

Define el prefijo de marcación, una serie que debe preceder el número de teléfono cuando el usuario efectúa marcaciones automáticas con un módem. Para ver los mandatos de marcación adecuados, consulte la documentación del módem.

Opciones: ATDT, ATDP u otras, en función del tipo de módem.  
Valor predeterminado: ATDT.

### **FINAL**

Define el sufijo de marcación, una serie que debe seguir al número de teléfono cuando el usuario efectúa marcaciones automáticas con un módem. Para ver los mandatos de marcación adecuados, consulte la documentación del módem.

Opciones: En blanco (ninguno) o un sufijo de módem válido.  
Valor predeterminado: Ninguno.

### **WAIT**

Especifica el tiempo de espera entre los reintentos de marcación. El período de espera no empieza hasta que excede el tiempo de espera de la conexión o hasta que ésta se interrumpe. Si el parámetro ATTEMPTS está establecido en 0, no se produce ningún reinicio de marcación.

Opciones: 0 (ninguno) o un entero positivo que indique el número de segundos que debe esperarse.  
Valor predeterminado: 0

## ATTEMPTS

Especifica el número máximo de veces que el programa ATE intentará volver a marcar para establecer una conexión. Si el parámetro ATTEMPTS está establecido en 0, no se produce ningún reinicio de marcación.

Opciones: 0 (ninguno) o un entero positivo que indique el número de intentos.  
Valor predeterminado: 0

## TRANSFER

Define el tipo de protocolo asíncrono que transfiere archivos durante una conexión.

### p (pacing)

El protocolo de transferencia de archivos controla la velocidad de transmisión de datos esperando un carácter determinado o durante cierto número de segundos entre cada transmisión de línea.

Esto ayuda a evitar la pérdida de datos cuando los bloques de transmisión son demasiado grandes o se envían demasiado rápido para que el sistema pueda procesarlos.

### x (xmodem)

Un protocolo de transferencia de archivos de 8 bits para detectar errores de transmisión de datos y retransmitir los datos.

Opciones: p (pacing), x (xmodem)  
Valor predeterminado: p.

## CHARACTER

Especifica el tipo de protocolo de ritmo que debe utilizarse. Señal para transmitir una línea. Seleccione un carácter.

Cuando el submandato **send** encuentra un carácter de salto de línea mientras transmite datos, el submandato espera hasta recibir el carácter de pacing antes de enviar la línea siguiente.

Cuando el submandato **receive** está listo para recibir datos, envía el carácter de pacing y espera 30 segundos antes de recibir los datos. El submandato **receive** vuelve a enviar un carácter de pacing siempre que encuentra un carácter de retorno de carro en los datos. El submandato **receive** finaliza cuando no recibe ningún dato durante 30 segundos.

Opciones: cualquier carácter.  
Valor predeterminado: 0

## Intervalo

Número de segundos que el sistema espera entre cada línea que transmite. El valor de la variable Intervalo debe ser un entero. El valor predeterminado es 0, que indica un retardo de pacing de 0 segundos.

Valor predeterminado: 0.

## NAME

Nombre de archivo de los datos de entrada (archivo de captura).

Opciones: Un nombre de archivo válido de menos de 40 caracteres de longitud.  
Valor predeterminado: kapture

## LINEFEEDS

Añade un carácter de salto de línea después de cada carácter de retorno de carro en la serie de datos de entrada.

Opciones: 1 (activado) o 0 (desactivado).  
Valor predeterminado: 0.

## **ECHO**

Visualiza la entrada escrita por el usuario. En un sistema remoto que proporcione soporte a echo, cada carácter enviado se devuelve y se visualiza en la pantalla. Cuando el parámetro ECHO está activado, cada carácter se visualiza dos veces: primero, cuando se escribe y otra vez cuando se devuelve de una conexión. Cuando el parámetro ECHO está desactivado, cada carácter se visualiza sólo cuando se devuelve de una conexión.

Opciones: 1 (activado) o 0 (desactivado).  
Valor predeterminado: 0.

## **VT100**

La consola local emula un terminal DEC VT100, por lo que es posible utilizar código DEC VT100 con el sistema remoto. Con el parámetro VT100 desactivado, la consola local funciona como una estación de trabajo.

Opciones: 1 (activado) o 0 (desactivado).  
Valor predeterminado: 0.

## **WRITE**

Captura los datos de entrada y los dirige al archivo especificado en el parámetro NAME, así como la pantalla. Las combinaciones de retorno de carro o salto de línea se convierten en caracteres de salto de línea antes de escribirse en el archivo de captura. En un archivo existente, los datos se añaden al final del archivo.

Es posible utilizar el parámetro CAPTURE\_KEY (normalmente la secuencia de teclas Control-B) para activar o desactivar la modalidad de captura durante una conexión.

Opciones: 1 (activado) o 0 (desactivado).  
Valor predeterminado: 0.

## **XON/XOFF**

Controla la transmisión de datos en un puerto, de la forma siguiente:

- Cuando se recibe una señal XOFF, la transmisión se detiene.
- Cuando se recibe una señal XON, la transmisión se reanuda.
- Se envía una señal XOFF cuando el almacenamiento intermedio de recepción está casi lleno.
- Se envía una señal XON cuando el almacenamiento intermedio ya no está lleno.

Opciones: 1 (activado) o 0 (desactivado).  
Valor predeterminado: 1.

## **DIRECTORY**

Indica el archivo que contiene el directorio de marcación del usuario.

Valor predeterminado: el archivo /usr/lib/dir.

## **CAPTURE\_KEY**

Define la secuencia de teclas de control que comuta la modalidad de captura. Cuando se pulsa, CAPTURE\_KEY (normalmente la secuencia de teclas Control-B) inicia o detiene la captura (el guardado) de los datos que se visualizan en la pantalla durante una conexión activa.

Opciones: Cualquier carácter de control ASCII.  
Valor predeterminado: 002 octal ASCII (STX).

## **MAINMENU\_KEY**

Define la secuencia de teclas de control que devuelve el Connected Main Menu para que el usuario pueda emitir un mandato durante una conexión activa. MAINMENU\_KEY (normalmente la secuencia de teclas Control-V) funciona sólo desde el estado conectado.

Opciones: Cualquier carácter de control ASCII.  
Valor predeterminado: 026 octal ASCII (SYN).

## **PREVIOUS\_KEY**

Define la secuencia de teclas de control que visualiza la pantalla anterior en cualquier momento durante el programa. La pantalla que se visualiza varía en función de la pantalla en uso cuando el usuario pulsa PREVIOUS\_KEY (normalmente la secuencia de teclas Control-R).

Opciones: Cualquier carácter de control ASCII.  
Valor predeterminado: 022 octal ASCII (DC2).  
El carácter de control ASCII se correlaciona con la señal de interrupción.

## **Configuración de un directorio de marcación de ATE**

El archivo del directorio de marcación de ATE lista los números de teléfono que el programa ATE utiliza para establecer conexiones remotas por módem.

Para configurar un directorio de marcación de ATE, deben satisfacerse los requisitos siguientes:

- El programa Asynchronous Terminal Emulation (ATE) debe estar configurado en el sistema
- Para configurar un directorio de marcación para todo el sistema, el usuario debe tener acceso de grabación sobre el archivo /usr/lib/dir.

Los usuarios pueden poner al archivo del directorio de marcación cualquier nombre de archivo válido y colocarlo en cualquier directorio sobre el que posean acceso de lectura y escritura. Edite el archivo del directorio de marcación con cualquier editor de textos ASCII. La información del directorio de marcación predeterminado para el programa ATE se incluye en el archivo /usr/lib/dir, tal como se muestra a continuación:

**Nota:** En el contenido siguiente, algunas entradas de ATE se han dividido en líneas distintas para mejorar la legibilidad. Sin embargo, en el archivo del directorio de marcación real todos los elementos de una entrada deben declararse en una sola línea continua.

```
# COMPONENT_NAME: BOS dir
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1985, 1989
# Materiales bajo licencia - Propiedad de IBM
#
# Derechos restringidos para los usuarios de EE.UU. - El uso, duplicación o
# divulgación están sujetos a las restricciones del GSA ADP Schedule
# Contract con IBM Corp.
#
# dir - directorio de marcación de ejemplo
#
#
# Micom    9,555-9400 1200 7 1 2 0 0
# R20     9,555-9491 1200 7 1 2 0 0
# QT      9,555-8455 1200 7 1 2 0 0
# Dallas1 9,555-7051 1200 8 1 0 0 0
```

Los usuarios pueden acceder a la información del directorio de marcación desde ATE utilizando el submandato **directory** disponible en el **UNCONNECTED MAIN MENU**. La pantalla mostrará la información sobre el directorio tal como ésta aparecería en el programa ATE.

Los usuarios pueden tener más de un directorio de marcación. Para cambiar el archivo del directorio de marcación que el programa ATE utiliza, el usuario debe modificar el archivo ate.def en el directorio actual.

**Nota:** El archivo del directorio de marcación puede contener hasta 20 líneas (una entrada por línea). ATE no tiene en cuenta las líneas posteriores.

El archivo del directorio de marcación se parece a una página del listín telefónico y contiene entradas para los sistemas remotos a los que se llama con el programa ATE. El formato de una entrada del directorio de marcación es el siguiente:

```
Name Phone Rate Length StopBit Parity Echo Linefeed
```

Los campos deben ir separados por un espacio por lo menos. Es posible utilizar más espacios para facilitar la legibilidad de cada entrada. Los campos son los siguientes:

**Name**

Identifica un número de teléfono. El nombre puede ser cualquier combinación de 20 caracteres o menos. Utilice el carácter \_ (subrayado) en vez de un espacio en blanco entre las palabras de un nombre como, por ejemplo, base\_datos.

**Phone**

El número de teléfono que debe marcarse. El número puede tener hasta 40 caracteres. Consulte la documentación del módem para ver una lista de los dígitos y los caracteres aceptables. Por ejemplo, si debe marcarse el 9 para acceder a una línea externa, incluya un 9, (el número 9 y una coma) antes del número de teléfono, de la forma siguiente:9,1112222.

Aunque el número de teléfono puede tener hasta 40 caracteres, el submandato del directorio sólo visualiza los 26 primeros caracteres.

**Rate**

La velocidad en baudios o de transmisión en bits por segundo (bps). Determina el número de caracteres que se transmiten por segundo. Seleccione una velocidad en baudios que sea compatible con la línea de comunicaciones que se utiliza. Las siguientes son velocidades aceptables:

50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 9600 o 19200.

Para las velocidades en baudios que no son POSIX, si se establece la validad en 50 el ATE utiliza la velocidad en baudios configurada establecida mediante SMIT para este dispositivo.

**Length**

Número de bits que forman un carácter. La entrada para el campo Longitud puede ser 7 u 8.

**StopBit**

Los bits de parada señalan el final de un carácter. La entrada para el campo StopBit puede ser 1 o 2.

**Parity**

Comprueba si un carácter se ha transmitido satisfactoriamente desde el sistema remoto o hacia el mismo. La entrada para el campo Parity puede ser 0 (ninguna), 1 (impar) o 2 (par).

**Echo**

Determina si los caracteres que hay escritos se visualizan localmente. La entrada para el campo Echo puede ser 0 (desactivado) o 1 (activado).

**Linefeed**

Añade un carácter de salto de línea al final de cada línea de datos procedente de un sistema remoto. El carácter de salto de línea tiene una función similar a la de los caracteres de retorno de carro y de línea nueva. La entrada para el campo Linefeed puede ser 0 (desactivado) o 1 (activado).

**Nota:** Es posible que sea necesario realizar modificaciones o reasignaciones en caso de conflicto entre las teclas de control de distintas aplicaciones. Por ejemplo, si las teclas de control correlacionadas para el programa ATE entran en conflicto con las de un editor de textos, deberá volver a asignar las teclas de control de ATE.

**Nota:** El carácter de control ASCII seleccionado puede estar en formato octal, decimal o hexadecimal, de la forma siguiente:

**octal**

De 000 a 037. El cero inicial es obligatorio.

**decimal**

De 0 a 31.

## hexadecimal

De 0x00 a 0x1F. El 0x inicial es obligatorio. La x puede ir en mayúsculas o en minúsculas.

Cree un archivo `ate .def` que defina estas características para cambiar las características de la emulación ATE. Por ejemplo, para cambiar la velocidad (RATE) a 300 bps, el dispositivo (DEVICE) a `tty3`, la modalidad de transferencia (TRANSFER) a `x` (protocolo xmodem) y el directorio (DIRECTORY) a `my.dir`, cree un `ate .def` con las entradas siguientes, en el directorio que ejecute el programa ATE:

```
RATE      300
DEVICE    tty3
TRANSFER  x
DIRECTORY my.dir
```

El programa utiliza los valores definidos desde el momento en que el programa ATE se inicia desde este directorio.

1. Cree el archivo del directorio de marcación:

- a) Cambie al directorio donde residirá el archivo del directorio de marcación.
- b) Copie el archivo `/usr/lib/dir` para utilizarlo como plantilla. Cambie el nombre del archivo por cualquier nombre de archivo válido.
- c) Cree entradas de número de teléfono utilizando el formato proporcionado en el formato de archivo del directorio de marcación.
- d) Guarde el archivo.

**Nota:** Si el nuevo archivo del directorio de marcación va a ser el archivo predeterminado para todo el sistema, guárdelo con el nombre `/usr/lib/dir`.

2. Si el nombre de archivo del directorio de marcación no es el valor predeterminado (`/usr/lib/dir`), edite el archivo `ate .def` en el directorio desde el que se ejecuta el programa ATE. Cambie el parámetro `DIRECTORY` del archivo `ate .def` por el nuevo archivo del directorio de marcación.  
Consulte el apartado “[Edición del archivo de ATE por omisión](#)” en la página 737
3. Inicie ATE y visualice el directorio de marcación con el submandato **directory**.

## Marcación con ATE

Utilice este procedimiento para marcar desde un sistema utilizando ATE y un archivo de directorios de marcación `/usr/lib/dir` personalizado.

Antes de intentar la marcación, compruebe que se cumplan todos los requisitos y las condiciones siguientes.

- El ATE debe estar instalado.
- Un módem debe estar conectado, configurado y listo para su uso.
- El usuario debe ser miembro del grupo UUCP (consulte el apartado “[Configuración de ATE](#)” en la página 725 para obtener más información).
- El directorio de marcación de `/usr/lib/dir` ya debe haberse personalizado con la información correcta.
- El directorio de trabajo actual del usuario (`pwd`) debe contener un archivo `ate .def` que esté correctamente actualizado.
- El puerto `/dev/tty` debe tener el campo de inicio de sesión ENABLE de SMIT establecido en inhabilitar, compartir o retrasar.

1. Escriba:

```
ate
```

2. En el menú principal, escriba d y pulse Intro.
3. Escriba el nombre de archivo del directorio que desee visualizar y pulse Intro. Para utilizar el directorio actual, simplemente pulse Intro.

4. Escriba el número de entrada del directorio adecuado en la columna # para marcar el número de teléfono correspondiente.

### Transferencia de un archivo utilizando ATE

Utilice este procedimiento para transferir un archivo desde un sistema principal local al sistema remoto.

Antes de intentar transferir un archivo utilizando ATE, compruebe que se cumplan todos los requisitos y las condiciones siguientes:

- Ya debe haberse establecido una conexión utilizando el programa **ATE**.
- El protocolo de transferencia de archivos Xmodem ya debe existir tanto en el sistema local como en el remoto. En el sistema operativo, Xmodem se encuentra en el directorio /usr/bin.

1. Ejecute el mandato **xmodem** siguiente en el sistema remoto después de iniciar la sesión:

```
xmodem -r archivo_nuevo
```

donde **r** el distintivo de Xmodem a recibir y *archivo\_nuevo* es el nombre del archivo que debe recibirse. No es necesario que este nombre coincida con el del archivo que se está transfiriendo.

2. Pulse Intro.

3. Aparece el mensaje siguiente:

```
ate: 0828-005 El sistema está listo para recibir el archivo archivo_nuevo.  
Utilice Control-X para detener xmodem.
```

Si el mensaje no se visualiza, es posible que el sistema no tenga instalado el programa **xmodem** o que se encuentre en la VÍA DE ACCESO de mandato.

4. Pulse Control-V para volver al CONNECTED MAIN MENU de ATE.

5. Pulse la tecla S para enviar un archivo.

6. Aparece el mensaje siguiente:

```
Escriba el nombre del archivo que desee enviar y pulse Intro. Para utilizar el nombre  
del último archivo (), simplemente pulse Intro.
```

7. Entre el nombre y la vía de acceso completa del archivo que debe transferirse.

8. Pulse Intro.

9. ATE mostrará el mensaje siguiente y empezará a transferir el archivo:

```
ate: 0828-024 El programa está listo para enviar el archivo archivo_nuevo. Recibirá otro  
mensaje cuando finalice la transferencia del archivo.  
ate: 0828-025 El sistema está enviando el bloque 1.  
ate: 0828-025 El sistema está enviando el bloque 2.  
ate: 0828-015 La transferencia del archivo ha finalizado.  
ate: 0828-040 Pulse Intro
```

10. Pulse Intro cuando la transferencia haya finalizado.

### Recepción de un archivo utilizando ATE

Utilice este procedimiento para recibir un archivo transferido desde un sistema principal remoto.

Antes de intentar recibir un archivo utilizando ATE, compruebe que se cumplan todos los requisitos y las condiciones siguientes:

- Ya debe haberse establecido una conexión utilizando el programa ATE.
- El protocolo de transferencia de archivos Xmodem ya debe existir tanto en el sistema local como en el remoto. En el sistema operativo, Xmodem se encuentra en el directorio /usr/bin.

1. Ejecute el mandato **xmodem** siguiente en el sistema remoto después de iniciar la sesión:

```
xmodem -s archivo_nuevo
```

donde **s** es el mandato **xmodem** que debe enviarse y *archivo\_nuevo* es el nombre y la vía de acceso completa del archivo que debe transferirse.

2. Pulse Intro.

3. Aparece el mensaje siguiente:

```
ate: 0828-005 El sistema está listo para enviar el archivo archivo_nuevo.  
Utilice Control-X para detener el módem.
```

Si el mensaje no se visualiza, es posible que el sistema no tenga instalado el programa **xmodem** o que se que se encuentre en la vía de acceso (PATH) para el mandato.

4. Pulse Control-V para volver al CONNECTED MAIN MENU de ATE.

5. Pulse la tecla R para recibir el archivo.

6. Aparece el mensaje siguiente:

```
Escriba el nombre del archivo en el que desee almacenar los datos recibidos y  
pulse  
Intro. Para utilizar el nombre del último archivo (), simplemente pulse Intro.
```

7. Entre el nombre y la vía de acceso completa del archivo que debe transferirse.

8. Pulse Intro.

9. ATE mostrará el mensaje siguiente y empezará a transferir el archivo:

```
ate: 0828-020 El programa está listo para recibir el archivo archivo_nuevo. Cuando  
finalice la transferencia del archivo, recibirá otro mensaje.  
ate: 0828-028 El sistema está recibiendo el bloque 1.  
ate: 0828-028 El sistema está recibiendo el bloque 2.  
ate: 0828-040 Pulse Intro.
```

10. Pulse Intro cuando la transferencia haya finalizado.

### **Edición del archivo de ATE por omisión**

Para editar el archivo de ATE predeterminado, el programa de ATE debe estar configurado en el sistema.

Para cambiar los valores del archivo *ate.def*:

1. Abra el archivo *ate.def* con un editor de texto ASCII.

2. Escriba los valores nuevos para los parámetros que va a modificar. El resto de los valores puede suprimirse o ignorarse. El sistema utiliza sus valores predeterminados para todos los parámetros suprimidos.

3. Guarde el archivo *ate.def* modificado.

Los cambios realizados en el archivo *ate.def* se activarán la próxima vez que se ejecute ATE desde el directorio que contiene el archivo *ate.def* personalizado.

Puede conservar una copia del archivo *ate.def* en cualquier directorio en el que tenga permisos de lectura y grabación. Por ejemplo, si el usuario necesita ejecutar el programa ATE con valores predeterminados diferentes en momentos distintos, guarde varias copias del archivo *ate.def*, con los valores apropiados, en subdirectorios diferentes del directorio \$HOME. No obstante, las sucesivas copias del archivo *ate.def* utilizan almacenamiento del sistema. Como alternativa, cambie temporalmente la mayoría de los valores con los submandatos **alter** y **modify** de ATE. Utilice una entrada del directorio de marcación para cambiar los valores de una conexión de módem individual. Consulte el apartado “Configuración de un directorio de marcación de ATE” en la página 733.

### **Resolución de problemas en ATE**

Cuando se encuentre con los siguientes problemas habituales en ATE, plántese las soluciones siguientes.

**Problema:**

Al transferir o recibir archivos, parece que el mandato **xmodem** se cuelga. El problema se corrige mediante Control-X.

**Solución:**

Examine el menú Alter para verificar que se esté utilizando el protocolo xmodem (o el método de transferencia).

**Problema:**

Al transferir o recibir archivos, el archivo se desplaza a través de la pantalla y se muestra un mensaje que indica que la transferencia o recepción ha finalizado mientras que, en realidad, no ha sido así.

**Solución:**

Examine el menú Alter para verificar que se esté utilizando el protocolo **xmodem** (o el método de transferencia).

**Problema:**

Al iniciar ATE, el usuario recibe el error siguiente:

```
ate: 0828-008 El sistema ha intentado abrir el puerto /dev/tty0 pero no ha podido.  
Si el nombre del puerto no es correcto, cámbielo utilizando el menú Alter.  
O realice la acción que indica el mensaje del sistema que aparece a continuación.  
  
Connect: Los permisos de acceso al archivo no permiten la acción especificada.  
ate: 0828-040 Pulse Intro.
```

**Solución:**

La línea Connect: del mensaje de error define el problema de forma más detallada. Verifique que el usuario que intenta ejecutar ATE sea miembro del grupo UUCP. Para comprobarlo, el usuario puede entrar *id* en la línea de mandatos; debería aparecer uucp en el listado de salida.

**Problema:**

Al intentar realizar una conexión con ATE, se recibe el error siguiente:

```
ate: 0828-008 El sistema ha intentado abrir el puerto /dev/tty0 pero no ha podido.  
Si el nombre del puerto no es correcto, cámbielo utilizando el menú Alter.  
O realice la acción que indica el mensaje del sistema que aparece a continuación.  
  
Connect: No existe un archivo o un directorio en el nombre de vía de acceso.  
ate: 0828-040 Pulse Intro.
```

**Solución:**

Se ha seleccionado un tty incorrecto o no disponible para que ATE lo utilice. Examine la pantalla de Alter en ATE.

**Problema:**

El archivo se transfiere correctamente pero el archivo tiene un tamaño mayor que el archivo original.

**Solución:**

El protocolo xmodem rellena el archivo durante la transferencia. Para evitarlo, utilice el mandato **tar** para comprimir el archivo y transferirlo. Esto también permite superar otra limitación de xmodem, donde sólo puede enviarse un archivo cada vez. El usuario puede comprimir varios archivos juntos mediante **tar** en una sola imagen tar y transferirlos utilizando xmodem.

**Mandatos y submandatos de ATE**

A continuación se muestra la lista de los mandatos y submandatos de ATE, con una breve descripción de lo que hacen.

Vea el apartado “Formatos de archivo ATE” en la página 739 para obtener información adicional.

## Item Descripción

**ate** Inicia el programa ATE. Para ver la definición de los submandatos que aparecen a continuación, consulte el mandato **ate**:

### **break**

Da entrada a la actividad actual en un sistema remoto.

### **connect**

Conecta con un sistema remoto.

### **directory**

Visualiza el directorio de marcación de ATE y permite elegir una entrada en el directorio para conectarse a un sistema remoto.

### **help**

Facilita ayuda para los submandatos ATE.

### **perform**

Permite emitir mandatos de sistema operativo de la estación de trabajo mientras se utiliza ATE.

### **quit**

Sale del programa ATE.

### **receive**

Recibe un archivo de un sistema remoto.

### **send**

Envía un archivo a un sistema de archivos remotos.

### **terminate**

Finaliza una conexión ATE con un sistema remoto.

Además, el mandato **xmodem** resulta útil para transferir archivos con el protocolo xmodem, que detecta posibles errores de transmisión de datos durante las transmisiones asíncronas.

## Formatos de archivo ATE

Los formatos de archivo Asynchronous Terminal Emulation (ATE) incluyen los formatos **ate.def** y de directorio de marcación.

Item	Descripción
<b>ate.def</b>	Establece los valores predeterminados para las conexiones.
<b>Directorio de marcación</b>	Define los números de teléfono y los valores de las conexiones de módem específicas.

Vea el apartado “[Mandatos y submandatos de ATE](#)” en la página 738 para obtener información adicional.

## Programa de utilidad de pantalla dinámica

El programa de utilidad de pantalla dinámica o el mandato **dscreen** es un programa de utilidad que permite que un solo terminal físico se conecte a varias sesiones (pantallas) virtuales del terminal al mismo tiempo.

Está pensado principalmente para su utilización con terminales que tengan dos o más páginas de memoria de pantalla (por ejemplo, la pantalla IBM 3151 Modelos 310 o 410 con el cartucho de ampliación). Con estos terminales, al comutador entre las pantallas virtuales también se comuta entre las páginas de pantalla del terminal físico, lo que permite guardar y restaurar todas las imágenes de la pantalla virtual. En los terminales sin varias páginas de memoria de pantalla, el mandato **dscreen** también puede utilizarse para comutar entre las sesiones de la pantalla virtual, aunque el aspecto de la pantalla no se conservará.

**Nota:** Para conseguir soporte completo del programa de utilidad **dscreen**, el terminal debe ser capaz de comutar las páginas de pantallas internas del mandato y debe recordar la posición del cursor para cada

página. Mientras el programa de utilidad **dscreen** funcionará en tanto en terminales inteligentes como tontos, las imágenes de las pantallas no se guardan durante los cambios de pantallas en los terminales tontos.

### Archivo de información de configuración del terminal de dscreen

El archivo de información de configuración del terminal del programa de utilidad **dscreen** (o archivo **dsinfo**) se utiliza para definir un conjunto de teclas distinto para su utilización con el programa de utilidad **dscreen**.

Esto podría hacerse, por ejemplo cuando las teclas definidas originalmente en el programa de utilidad **dscreen** entran en conflicto con una aplicación de software que se utilice en el sistema.

El tipo del terminal del archivo **dsinfo** presupone una sola página de memoria de pantalla. Por lo tanto, si un terminal proporciona soporte a páginas de memoria de pantalla adicionales, el archivo **dsinfo** debe personalizarse para utilizar la secuencia adecuada para el control de la memoria de las páginas. Consulte el manual de consulta del terminal adecuado para ver la secuencia de control específica.

El archivo **dsinfo** por omisión es `/usr/lbin/tty/dsinfo`. Utilice el distintivo **-i** para especificar un archivo **dsinfo** distinto. El resto de este apartado hace referencia al archivo por omisión. Sin embargo, la misma información es aplicable a cualquier archivo **dsinfo** personalizado que se cree.

Para obtener más información sobre el archivo **dsinfo**, consulte el apartado “[Asignación dinámica de pantallas](#)” en la página 742.

### Asignación de acciones a las teclas de dscreen

Cuando se ejecuta el mandato **dscreen**, éste inicia una pantalla virtual. Algunas de las teclas del teclado del terminal son pasadas a través de la pantalla virtual; en lugar de esto, el programa de utilidad **dscreen** intercepta estas teclas y realiza ciertas acciones cuando se pulsan.

Entre las acciones se incluyen:

Item	Descripción
<b>Seleccionar</b> (consulte el apartado “ <a href="#">Teclas de selección de dscreen</a> ” en la página 740)	Seleccionar una pantalla especificada.
<b>Bloquear</b> (consulte el apartado “ <a href="#">Teclas de bloqueo de dscreen</a> ” en la página 741)	Bloquea toda la entrada y toda la salida.
<b>Nueva</b> (consulte el apartado “ <a href="#">Teclas nuevas de dscreen</a> ” en la página 741)	Inicia una sesión de pantalla nueva.
<b>Finalizar</b> (consulte el apartado “ <a href="#">Teclas Finalizar y Salir de dscreen</a> ” en la página 741)	Finaliza el programa de utilidad <b>dscreen</b> .
<b>Salir</b> (consulte el apartado “ <a href="#">Teclas Finalizar y Salir de dscreen</a> ” en la página 741)	Sale del programa de utilidad <b>dscreen</b> .
<b>Anterior</b> (consulte el apartado “ <a href="#">Tecla anterior de dscreen</a> ” en la página 741)	Commuta a la pantalla anterior.
<b>Lista</b> (consulte el apartado “ <a href="#">Tecla de lista de dscreen</a> ” en la página 741)	Lista las teclas asignadas de <b>dscreen</b> y las acciones de las mismas.

La función de cada tecla depende del terminal y de la descripción del terminal en el archivo `/usr/lbin/tty/dsinfo`.

### Teclas de selección de dscreen

Cuando se crea una pantalla virtual nueva, se le asigna una tecla de selección.

Cuando se pulsa la tecla de selección, se realizan las acciones siguientes:

- Una commutación del terminal físico a la página de vídeo asociada con la pantalla virtual en concreto.

- La entrada y la salida se dirige entre el terminal físico y la pantalla virtual de la forma adecuada.

Una vez se hayan asignado pantallas virtuales a todas las teclas de selección definidas en el archivo **dsinfo**, no es posible crear más pantallas. Las sesiones de las pantallas individuales finalizan cuando el proceso de shell original sale. Esto libera la tecla de selección asociado para que otra pantalla virtual pueda utilizarla. El programa de utilidad **dscreen** finaliza cuando no hay más pantallas activas.

#### **Teclas de bloqueo de dscreen**

Las teclas de bloqueo se utilizan para detener la salida de forma similar a la tecla Control-S cuando se utiliza el control de flujo IXON.

La finalidad de estas teclas consiste en permitir la configuración transparente de las sesiones del terminal en dos sistemas utilizando un terminal que tenga dos puertos serie.

#### **Teclas nuevas de dscreen**

Al pulsar una tecla nueva, se crea una pantalla lógica nueva a la que se asigna una de las teclas de selección.

Cada pantalla nueva requiere:

- Una tecla de selección tal como esté definida en el archivo **dsinfo**
- Un dispositivo de pseudo terminal **dscreen**
- Memoria suficiente para las distintas estructuras utilizadas en el rastreo de las pantallas
- Un proceso desde el que ejecutar el shell.

Si alguno de estos requisitos no está disponible, la operación de pantalla nueva fallará y un mensaje indicará el motivo de la anomalía.

#### **Teclas Finalizar y Salir de dscreen**

Cuando se pulsan las teclas Finalizar y Salir, se produce una secuencia de acciones.

Al pulsar la tecla Finalizar, se produce lo siguiente:

- Se envía una señal **SIGHUP** a todas las sesiones de pantallas
- Se borra
- Se sale con un estado de 0.

Si se pulsa la tecla Salir se realizan las mismas acciones pero se sale con un estado de 1.

#### **Tecla anterior de dscreen**

Si se pulsa una tecla anterior, el terminal comuta a la pantalla que se había visualizado la última vez.

#### **Nota:**

1. No commute entre pantallas cuando se esté grabando en la pantalla actual; es posible que una secuencia de escape quede truncada y el terminal quede en un estado desconocido.
2. La visualización de algunos terminales permiten guardar la posición del cursor para pantallas individuales pero es posible que no guarden otros estados como, por ejemplo, la modalidad de inserción, la inversión de vídeo, etc. Si éste es el caso, los usuarios deberían evitar estas modalidades mientras comuten entre pantallas.

#### **Tecla de lista de dscreen**

Al pulsar la tecla de lista se muestra una lista de las teclas y las acciones asociadas a las mismas en la pantalla del terminal.

Sólo se mostrarán las teclas que el programa de utilidad **dscreen** reconozca. Cuando se crea una pantalla nueva utilizando el programa de utilidad **dscreen**, aparece el mensaje Pulse **TECLA** para obtener ayuda, donde **TECLA** es el nombre de la tecla de lista que se visualiza en el terminal. Observe que el mensaje sólo aparece si hay definida una tecla de lista.

## Asignación dinámica de pantallas

La entrada de descripción del terminal del archivo /usr/lib/tty/dsinfo tiene el mismo número de teclas de selección de pantallas que el número de páginas de pantallas físicas que tiene el terminal. Si se definen más teclas de selección que el número de páginas de pantallas físicas, el programa de utilidad **dscreen** asignará dinámicamente páginas de pantallas físicas a pantallas virtuales.

Cuando se selecciona una pantalla virtual que no tiene una página de memoria de pantalla asociada, el programa de utilidad **dscreen** asigna a la pantalla virtual la pantalla física que haga más tiempo que no se ha utilizado. En función de las especificaciones del archivo de descripción /usr/lib/tty/dsinfo es posible que se observe una indicación de que la pantalla física está conectada a una pantalla virtual distinta; por ejemplo, que la pantalla se borre.

### Archivo dsinfo

El archivo dsinfo es una base de datos de descripciones del terminal que el programa de utilidad **dscreen** de varias pantallas utiliza.

El archivo contiene la información siguiente:

- Las teclas del programa de utilidad **dscreen** y las funciones que realizan
- El número de páginas de memoria de pantalla para el terminal
- Las secuencias de códigos enviadas o recibidas para utilizar las funciones anteriores.

Las entradas de tipo de terminal del archivo dsinfo por omisión se parecen a los siguientes valores en el terminal ASCII 3151:

```
# El Cartucho de ampliación (N/P: 64F9314) necesario para esta entrada
ibm3151|3151|IBM 3151,
dsks=\E!a^M|Mayúsculas-F1|,           # Seleccionar la primera pantalla
dsks=\E!b^M|Mayúsculas-F2|,           # Seleccionar la segunda pantalla
dsks=\E!c^M|Mayúsculas-F3|,           # Seleccionar la tercera pantalla
dsks=\E!d^M|Mayúsculas-F4|,           # Seleccionar la cuarta pantalla
dskc=\E!e^M|Mayúsculas-F5|,           # Crear una pantalla nueva
dske=\E!f^M|Mayúsculas-F6|\E pA\EH\EJ, # Ir a la pantalla 1 y finalizar
dskl=\E!g^M|Mayúsculas-F7|,           # Listar teclas de función (ayuda)
dskp=\E!h^M|Mayúsculas-F8|,           # Ir a la pantalla anterior
dskq=\E!i^M|Mayúsculas-F9|\E pA\EH\EJ, # Ir a la pantalla 1 y salir
dsp=\E pA\EH\EJ,                     # Secuencia del terminal para la pantalla 1
dsp=\E pb|\EH\EJ,                     # Secuencia del terminal para la pantalla 2
dsp=\E pc|\EH\EJ,                     # Secuencia del terminal para la pantalla 3
dsp=\E pd|\EH\EJ,                     # Secuencia del terminal para la pantalla 4
dst=10,                                # Permitir alm. intermedio tiempo espera
                                         # excedido 1 seg.
```

### Formato de las entradas para dsinfo

Las entradas del archivo dsinfo están formadas por campos separados por comas.

El primer campo es una lista de nombres alternativos para el terminal, cada uno separado mediante un carácter de conducto ( | ). Cualquier texto precedido por una almohadilla (#) se considera un comentario y **dscreen** no lo tiene en cuenta. Los campos restantes son series que describen las posibilidades del terminal al programa de utilidad **dscreen**. En estas series, se reconocen los códigos de escape siguientes:

Tabla 111. Campos de archivo dsinfo	
Secuencia de escape	Descripción
\E,\e	carácter de escape
\n,\l	carácter de línea nueva (o salto de línea)
\r	retorno de carro
\t	carácter de tabulación
\b	carácter de retroceso
\f	carácter de salto de página

Tabla 111. Campos de archivo dsinfo (continuación)

Secuencia de escape	Descripción
\s	carácter de espacio
\nnn	carácter con el valor octal nnn
^x	Control-X para cualquier valor x adecuado

Cualquier otro carácter precedido de una barra inclinada invertida generará el propio carácter. Las series se introducen como *tipo=serie*, donde *tipo* es el tipo de la serie, tal como se lista a continuación y *serie* es el valor de la serie.

Es importante que los campos de entrada del archivodsinfo estén separados mediante comas. Si se omite una coma o si ésta se trunca del final de una entrada del archivo dsinfo, el programa de utilidad **dscreen** no podrá leer el archivo y aparecerá un error en la pantalla.

#### Tipos de series de disinfo

Aquí pueden consultarse los tipos de series de disinfo.

Los tipos de series son los siguientes:

Item	Descripción
<b>dskx</b>	Un tipo de serie que empieza por dsk describe una tecla. El tipo debe tener una longitud de cuatro letras y la cuarta letra x indica la acción que se realiza cuando se recibe la tecla. Los tipos de teclas son los siguientes:
<b>Tipo</b>	<b>Acción</b>
<b>dsks</b>	Comutar pantallas
<b>dskb</b>	Bloquear entrada y salida
<b>dske</b>	Finalizar <b>dscreen</b>
<b>dskq</b>	Salir de <b>dscreen</b> (estado de salida=1)
<b>dskc</b>	Crear pantalla nueva
<b>dskp</b>	Comutar a pantalla anterior
<b>dskl</b>	Listar teclas y acciones

**dskx**

Un tipo de serie que empieza por dsk describe una tecla. El tipo debe tener una longitud de cuatro letras y la cuarta letra x indica la acción que se realiza cuando se recibe la tecla. Los tipos de teclas son los siguientes:

**Tipo**

**Acción**

**dsks**

Comutar pantallas

**dskb**

Bloquear entrada y salida

**dske**

Finalizar **dscreen**

**dskq**

Salir de **dscreen** (estado de salida=1)

**dskc**

Crear pantalla nueva

**dskp**

Comutar a pantalla anterior

**dskl**

Listar teclas y acciones

Cualquier otro tipo de tecla(es decir, un tipo de serie dskx que no termine en s, b, e, q, p o l) no provocará ninguna acción **dscreen** interna pero se mostrará en el listado de teclas y se reconocerá y ejecutará. Debe utilizarse un tipo de dsxn (n indica Ningún funcionamiento) cuando no se desea ninguna acción **dscreen** interna.

La serie de valores de cada tecla tiene tres subseries, separadas mediante caracteres de conducto (|).

**Nota:** Utilice \ | para incluir el carácter | en una de las subseries.

La primera subserie es la secuencia de caracteres que el terminal envía cuando se pulsa la tecla. La segunda subserie es una etiqueta para la tecla que se imprime cuando se visualiza una lista de teclas. La tercera subserie es una secuencia de caracteres que **dscreen** envía al terminal cuando se pulsa esta tecla antes de realizar la acción que esta tecla solicita.

Item	Descripción
<b>dsp</b>	<p>Un tipo de serie de dsp describe una pantalla física en el terminal. Debe haber una serie dsp para cada pantalla física del terminal. La serie de valores de cada pantalla física tiene dos subseries, separadas mediante un carácter de conducto (   ).</p> <p>La primera subserie es la secuencia de caracteres que se envían al terminal para su visualización y salida en la página física del terminal.</p> <p>La segunda subserie se envía al terminal cuando la página se utiliza para algo nuevo. Esta segunda subserie suele estar establecida en la secuencia de borrar pantalla. Se envía bajo las dos condiciones siguientes:</p> <ol style="list-style-type: none"> <li>1. Cuando se crea una sesión de terminal virtual nueva.</li> <li>2. Cuando hay más terminales virtuales que pantallas físicas. Si se selecciona un terminal virtual que necesita que <b>dscreen</b> vuelve a utilizar una de las pantallas físicas, enviará esta secuencia a la pantalla para indicar que el contenido de la pantalla no coincide con la salida del terminal virtual conectado.</li> </ol> <p><b>Nota:</b> La ejecución con más terminales virtuales que pantallas físicas puede resultar confusa y no es aconsejable; puede evitarse no definiendo más teclas de selección de pantalla (dsks= ) que las pantallas físicas (dsp= ) de la entrada de dsinfo.</p>
<b>dst A</b>	<p>Serie con un tipo de tiempo de espera excedido de entrada de <b>dscreen</b> de ajustes de dst. El valor de la serie es un número decimal. El valor de tiempo de espera excedido se proporciona en décimas de segundo y tiene un valor máximo de 255 (valor predeterminado=<b>1</b> [o 0,1 segundos]).</p> <p>Cuando <b>dscreen</b> reconoce un prefijo de una secuencia de teclas de entrada pero no tiene todos los caracteres de la secuencia, esperará el envío de más caracteres hasta que esté reconocible. Si se produce un tiempo de espera excedido antes de que se reciban más caracteres, los caracteres se envían a la pantalla virtual y <b>dscreen</b> no considerará que estos caracteres forman parte de la secuencia de una tecla de entrada.</p> <p>Puede ser necesario elevar este valor si una o más de las teclas que <b>dscreen</b> debe activar constituye de hecho una serie de pulsaciones(es decir, asignando Control-Z 1, Control-Z 2, Control-Z 3, etc., para la selección de las pantallas y Control-Z N para la pantalla nueva y así sucesivamente).</p>

### Ejemplos de dysinfo

Los siguientes ejemplos de dysinfo son para Wyse-60 con tres sesiones de pantalla.

```
wy60|wyse60|wyse modelo 60,
dsks="^A|^M|Mayúsculas-F1|,
dsks="^Aa|^M|Mayúsculas-F2|,
dsks="^Ab|^M|Mayúsculas-F3|,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ew0\E+,
dsk1=\202|Control-F3|,
dsp=\Ew0|\E+,
dsp=\Ew1|\E+,
dsp=\Ew2|\E+,
```

Con esta entrada:

- De mayúsculas-F1 a Mayúsculas-F3 se utilizan para seleccionar las pantallas de la 1 a la 3.
- Control-F1 crea una pantalla nueva.
- Control-F2 envía: Esc w 0 Esc + a la pantalla (comutando a la ventana 0 y borrando la pantalla) y a continuación finaliza **dscreen**.
- Control-F3 lista las teclas y sus funciones.

Cada vez que se utiliza una pantalla física para una pantalla nueva, se envía la secuencia Esc + al terminal, con lo que se borra la pantalla.

El ejemplo siguiente es para un Wyse-60 con tres sesiones de pantalla pero una de las pantallas se encuentra en un segundo sistema que se comunica a través del segundo puerto serie del terminal:

```
wy60-1|wyse60-1|wyse modelo 60 - primer puerto serie
dsks=^A`^M|Mayúsculas-F1|,
dsks=^Aa^M|Mayúsculas-F2|,
dsks=^Ab^M|Mayúsculas-F3|\Ed#^Ab\r^T\Ee9,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Control-F3|,
dsp=\Ew0|\E+,dsp=\Ew1|\E+
wy60-2|wyse60-2|wyse modelo 60 - segundo puerto serie
dsks=^A`^M|Mayúsculas-F1|\Ed#^A`\r^T\Ee8,
dsks=^Aa^M|Mayúsculas-F2|\Ed#^Aa\r^T\Ee8,
dsks=^Ab^M|Mayúsculas-F3|,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Control-F3|,
dsp=\Ew2|\E+,
```

**dscreen** debe ejecutarse en ambos sistemas, con el tipo de terminal wy60-1 en el primer sistema y el tipo de terminal wy60-2 en el segundo sistema (utilizando la opción **-t** para **dscreen**). La entrada wy60-1 se examinará en primer lugar.

Las dos primeras entradas de teclas permanecen igual que en la entrada wy60 original. Sin embargo, la tercera tecla tiene el tipo dskb, lo que significa un bloqueo tanto de la entrada como de la salida. Cuando se pulsa esta tecla, la secuencia:

```
Esc d # Control-A b CR Control-T Esc e 9
```

se envía al terminal; después de esto, la salida se bloquea y **dscreen** continúa explorando la entrada en busca de secuencias de claves pero descarta todas las otras entradas.

La secuencia Esc d # coloca al terminal en modalidad de impresión transparente, que envía un eco de todos los caracteres hasta un Control-T a través del otro puerto serie.

Los caracteres Control-A b CR se envían al otro puerto serie informan al proceso **dscreen** del otro sistema de que debe activar la ventana asociada con la tecla Mayúsculas-F3.

La secuencia de teclas Control-T sale de la modalidad de impresión transparente. La secuencia de teclas Esc 9 hace que el terminal conmute al otro puerto serie AUX para las comunicaciones de datos.

En este punto, el otro componente toma el control, envía un Esc w 2 al conmutador a la tercera pantalla física y reanuda la comunicación normal.

La entrada wy60-2 sigue el mismo patrón general para las teclas Mayúsculas-F1 y Mayúsculas-F2:

- Conmutación a la modalidad de impresión transparente
- Envío de la serie de teclas de función al otro sistema
- Desactivación de la impresión transparente
- Conmutación al otro puerto serie

La tecla de Finalización, Control-F2, funciona igual para los dos sistemas; envía la secuencia de teclas de finalización al otro sistema a través del mecanismo de impresión transparente, conmuta el terminal a la ventana 0, borra la pantalla y sale.

## Controlador del dispositivo Serial over Ethernet

Permite crear dispositivos serie virtuales y dispositivos teletipo (tty) en el sistema operativo AIX. Para ello, utilice el servidor de dispositivos Ethernet (EDS) compatible con el protocolo Petición de comentarios (RFC) 2217.

Con el controlador de dispositivo Serial over Ethernet (SoE), puede crear dispositivos serie virtuales y dispositivos teletipo (tty) en el sistema operativo AIX. Para ello, utilice el servidor de dispositivos Ethernet (EDS) compatible con el protocolo Petición de comentarios (RFC) 2217. Entre los ejemplos de EDS, se incluyen los dispositivos Digi y Perle. Las funciones del controlador de dispositivos SoE es parecida a la

de un puerto COM (comunicación) real, como, por ejemplo, adaptadores de 2 puertos, 8 puertos y 128 puertos.

EDS también se denomina Ethernet Serial Server o Ethernet Terminal Server. Un EDS es un equipo externo, que no es de IBM, al que se conecta Ethernet. El equipo contiene uno o varios puertos serie (RS/232) a los que se pueden conectar módems externos. Un EDS es compatible si admite RFC 2217 (Telnet Com Port Control Protocol), una extensión del protocolo Telnet. Si se utiliza este protocolo, EDS funciona como servidor RFC 2217. Un EDS puede aceptar sesiones Telnet del sistema cliente RFC 2217 y enviar los datos recibidos de Telnet a un puerto COM. Los datos recibidos en el puerto COM se envían al sistema cliente RFC 2217.

Un EDS también puede enviar información sobre los cambios de estado de los dispositivos serie al sistema cliente RFC 2217. El sistema cliente RFC 2217 gestiona el control de flujo con EDS y envía información de configuración a EDS a través de este protocolo.

La LPAR de AIX actúa como sistema cliente RFC 2217. La LPAR de AIX establece una sesión de Telnet con un EDS, que es un servidor de RFC 2217. En la imagen siguiente, se muestra cómo se comunica una LPAR de AIX con un EDS para proporcionar un puerto serie virtual:

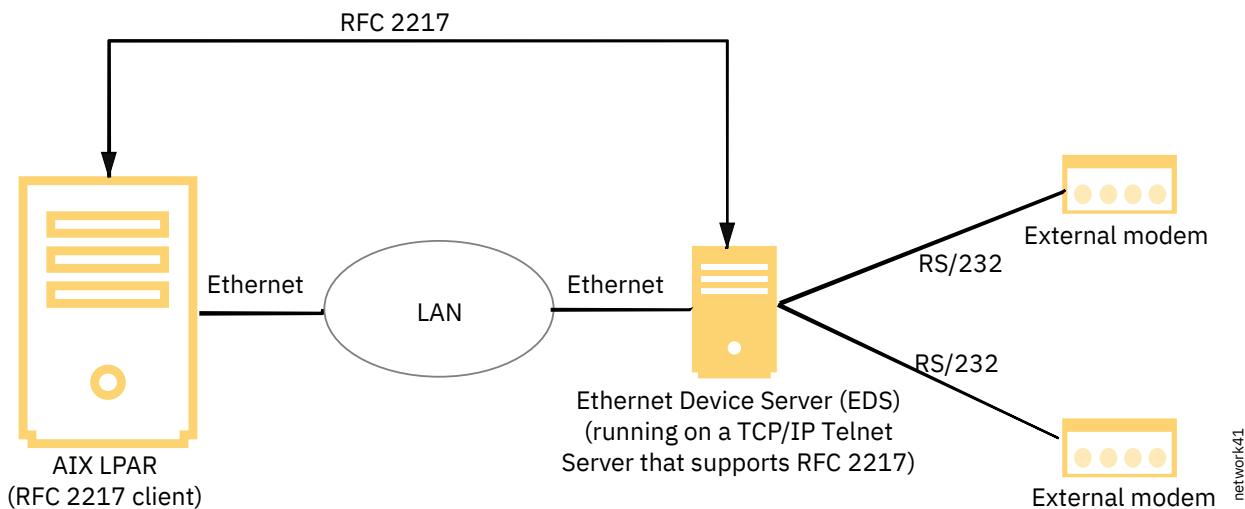


Figura 42. Configuración de Ethernet Driver Server

### Configuración de Ethernet Device Server

Normalmente, Ethernet Device Server (EDS) proporciona una interfaz basada en web para la configuración y la gestión. Por ejemplo, si un dispositivo Digi PortServer tiene una dirección IP 9.5.80.73, puede acceder a la interfaz de configuración y gestión especificando el URL <http://9.5.80.73> en un navegador web. Cada puerto serie de un EDS tiene un número de puerto TCP asignado. Para acceder a un puerto serie específico, establezca una sesión Telnet con la dirección IP de EDS y el número de puerto TCP asignado al puerto serie, por ejemplo, 9.5.80.73:2001. Esta sesión Telnet la crea internamente el controlador SoE.

### Configuración de la LPAR de AIX para crear un puerto serie virtual

El controlador de dispositivo SoE mantiene la semántica para crear los dispositivos de adaptador SoE (sa) y teletipo (tty) de una manera parecida a cómo se crea un dispositivo para un dispositivo serie físico.

Para crear un puerto serie virtual en una LPAR de AIX, siga estos pasos especificando los mandatos siguientes o utilizando las opciones de menú de SOE de SMIT:

1. Para crear un dispositivo sa, ejecute el mandato siguiente. Especifique la dirección IP del EDS.

```
# mkdev -c adapter -s pseudo -t soe -a netaddr=dirección_IP_EDS
```

Por ejemplo:

```
# mkdev -c adapter -s pseudo -t soe -a netaddr=9.126.88.123  
sa2 Available
```

2. Para crear un dispositivo tty, ejecute el mandato siguiente. Especifique el dispositivo de adaptador SoE (sa) visualizado en la salida del mandato del paso 1 y un puerto TCP.

```
# mkdev -t tty -s rs232 -p dispositivo_sa -w número Puerto_tty -a -a port_num=puerto_TCP
```

Por ejemplo:

```
# mkdev -t tty -s rs232 -p sa2 -w 0 -a port_num=2002  
tty1 Available
```

Este mandato crea un dispositivo tty en el directorio /dev. Cualquier aplicación puede utilizar el dispositivo tty que se acaba de crear para comunicarse con el dispositivo de destino conectado al puerto serie en un EDS.

**Nota:** Cada puerto serie de un EDS debe configurarse con un puerto TCP exclusivo y cada dispositivo tty configurado utilizando el controlador de dispositivo SoE debe correlacionarse con este puerto exclusivo. Un puerto tty de un EDS no puede compartirse entre varios dispositivos tty de la LPAR de AIX.

### Cómo mover dispositivos de terminal tty a través de dispositivos en serie asíncronos

Se puede mover un dispositivo de terminal de teletipo (tty) de un dispositivo (dispositivo de respaldo) serie asíncrono (SA) a otro dispositivo asíncrono. También se puede mover de un puerto físico a otro puerto físico del mismo dispositivo asíncrono. El sistema operativo AIX soporta tanto la opción **smitty** como la línea de mandatos para mover el dispositivo de terminal tty.

**Nota:**

- Tras mover a un dispositivo nuevo, los valores de configuración específicos del dispositivo tty (velocidad en baudios; modos de ejecución, etc) se mantendrán intactos.
- Un dispositivo de terminal tty no se puede abrir mediante terminal una aplicación ni utilizars cuando la operación de transferencia está en curso.

Los dispositivos asíncronos pueden ser un puerto de comunicaciones real como los adaptadores de 2, 8 y 128 puertos PCI o bien un puerto de comunicaciones compatible con RFC2217. El dispositivo SoE es una enumeración de un EDS (Ethernet Device Server).

Se puede mover un dispositivo tty de un adaptador asíncrono físico basado en PCI a otro dispositivo físico basado en PCI-based, o desde un dispositivo asíncrono físico basado en PCI-based a un dispositivo SoE, o viceversa, o bien se puede mover desde un tipo de dispositivo SoE a otro tipo de dispositivo SoE.

Por ejemplo, uno de los controladores de dispositivos SoE está configurado con la dirección IP 192.168.1.1 y tiene dispositivos de terminal TTY configurados y el usuario desea cambiar la dirección IP de este dispositivo SoE a 10.1.1.1. No puede ejecutar el mandato **chdev** para cambiar la dirección IP del controlador de dispositivo SoE hasta que todos los dispositivos del terminal tty asociado se hayan eliminado por completo mediante la ejecución del mandato **xmdev** o hasta que todos los dispositivos del terminal tty asociado se hayan movido a un estado definido ejecutando el mandato **xmdev**. Para cambiar la dirección IP de un controlador de dispositivo SoE respaldado por un EDS, puede mover el dispositivo del terminal tty a un dispositivo en serie asíncrono.

Para cambiar la dirección IP de un controlador de dispositivo SoE, complete los siguientes pasos:

1. Cree un controlador de dispositivo SoE con la dirección IP 10.1.1.1.
2. Mueva todos los controladores de dispositivo del terminal tty al dispositivo SoE con la dirección IP 192.168.1.1 al nuevo dispositivo SoE con la dirección IP 10.1.1.1 utilizando **smitty** o el mandato **chdev**.
3. Asegúrese de que ninguno de los dispositivos de terminal tty se esté utilizando o se encuentre en estado Abierto. Para mover un dispositivo de terminal tty de un puerto a otro en el mismo dispositivo

SA, ejecute el mandato **chdev** con el nuevo número de puerto como opción mediante el distintivo **-w**. A continuación se proporciona una sintaxis de mandato del mandato **chdev**:

```
chdev -1 <dispositivo tty> -w <número de puerto de destino>
```

Por ejemplo, para mover un dispositivo de terminal del puerto 0 al puerto 1, introduzca el siguiente mandato:

```
chdev -1 ttyX -w 1
```

Para mover un dispositivo de terminal tty de un dispositivo de respaldo a otro, el nombre del nombre del dispositivo de destino se debe especificar como una opción para el distintivo **-p**. A continuación se proporciona una sintaxis de mandato del mandato **chdev**:

```
chdev -1 <dispositivo tty> -p <padre de destino>
```

Por ejemplo, para mover un tty0 de dispositivo de terminal tty del dispositivo en serie SA1 al dispositivo en serie SA3, introduzca el siguiente mandato:

```
chdev -1 tty0 -p sa2
```

Para mover un dispositivo de terminal tty de un dispositivo de terminal físico, como adaptadores PCI de 2, 8 o 128 puertos a un controlador de dispositivo SoE (compatible con RFC2217), se debe especificar un número de puerto TCP a través de un distintivo **-a** como el atributo **número\_puerto**.

Por ejemplo, para mover un tty0 del dispositivo de terminal tty del dispositivo en serie SA2 al dispositivo en serie SA3, introduzca el siguiente mandato:

```
chdev -1 tty0 -p sa3 -a 2001
```

La sintaxis de mandato para mover un dispositivo de terminal tty de un controlador de dispositivo SoE respaldado con un EDS a otro dispositivo SoE respaldado por otro EDS:

```
chdev -1 <dispositivo tty> -p <padre de destino>
```

Por ejemplo, para mover un dispositivo de terminal tty del dispositivo en serie SA1 (respaldado por EDS1) al dispositivo en serie SA2 (respaldado por EDS2), introduzca el siguiente mandato:

```
chdev -1 tty0 -p sa2
```

## Parámetros ajustables

Se proporcionan los ajustables siguientes para ajustar algunos de los atributos que utiliza el controlador:

- **idle\_timeout**: especifica la cantidad de tiempo, medida en medios segundos, que la conexión TCP entre el controlador de dispositivo SoE y EDS deben estar inactivos antes de que se envíen sondeos de keepalive al dispositivo. Este valor corresponde a la opción de red TCP `tcp_keepidle` establecido por un controlador SoE para esta conexión TCP. El valor predeterminado es 360.
- **probe\_interval**: especifica el intervalo, medida en medios segundos, entre paquetes keepalive enviados para validar la conexión. Este valor corresponde a la opción de red TCP `tcp_keepintvl` establecido por un controlador SoE para esta conexión TCP. El valor predeterminado es 10.
- **probe\_count**: especifica el número de sondeos keepalive que se pueden enviar al dispositivo antes de terminar la conexión establecida con el EDS. Este valor corresponde a la opción de red TCP `tcp_keepcnt` establecido por un controlador SoE para esta conexión TCP. El valor predeterminado es 24.

## Resolución de errores comunes

Si no se ha configurado correctamente un controlador de dispositivo EDS o SoE, cuando se crea el dispositivo tty en la LPAR de AIX el estado del dispositivo tty puede pasar a un estado DOWN o ERROR. Si el

controlador de dispositivo se ha configurado correctamente, el estado del dispositivo tty debe ser UP. El estado del dispositivo tty se visualiza mediante el mandato **soestat**, que se puede utilizar para solucionar problemas.

Si el estado del dispositivo tty es DOWN, puede deberse a los motivos siguientes:

- Es posible que la dirección IP o el número de puerto no sean los correctos en un controlador de dispositivo SoE o EDS.
- Es posible que no sea posible acceder a EDS desde la LPAR de AIX en la que se ha configurado un controlador de dispositivo SoE debido a que la configuración de red o la topología de red no son las correctas.
- En EDS, se han creado varios dispositivos tty utilizando el mismo número de puerto TCP.

El estado del dispositivo tty puede ser ERROR debido a los motivos siguientes:

- No se ha seleccionado la modalidad RFC 2217 en EDS. Consulte la documentación del fabricante del EDS para averiguar cómo configurar la modalidad RFC 2217.
- La dirección IP proporcionada no es la de un EDS, sino de alguna otra máquina a la que se puede acceder desde la LPAR de AIX en la que se ha configurado el controlador de dispositivo SoE.

**Nota:** No se puede recuperar un dispositivo tty del estado ERROR para continuar utilizándolo. Una vez solucionado el problema, tiene que eliminar manualmente el dispositivo tty que se encuentra en estado ERROR y volver a crear un dispositivo tty, o mover el tty al estado defined y moverlo de nuevo al estado available.

## Entorno de control genérico de enlace de datos

---

El control genérico de enlace de datos (GDLC) es una definición de interfaz genérica que facilita a los usuarios de la aplicación y del kernel un conjunto común de mandatos para controlar los gestores de dispositivos de control de enlace de datos (DLC) en el sistema operativo.

Para la determinación de problemas, consulte el apartado [GDLC Problem Determination](#) de la publicación *Communications Programming Concepts*.

El control genérico de enlace de datos (GDLC) es una definición de interfaz genérica que facilita a los usuarios de la aplicación y del kernel un conjunto común de mandatos para controlar los gestores de dispositivos DLC en el sistema operativo.

La interfaz GDLC especifica los requisitos para las definiciones de punto de entrada, las funciones proporcionadas y las estructuras de datos para todos los gestores de dispositivos DLC. Entre los DLC compatibles con la interfaz GDLC se incluyen los siguientes:

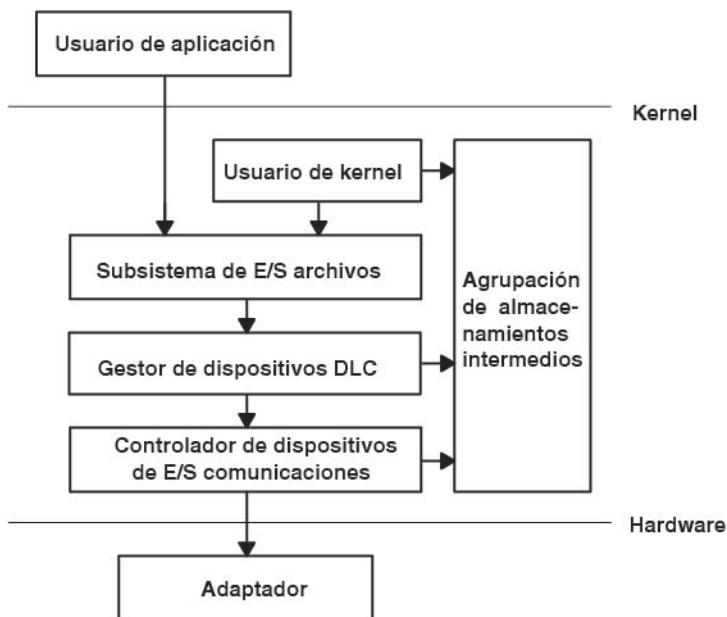
- 8023 (IEEE 802.3 para Ethernet)
- ETHER (Ethernet estándar)
- SDLC (Control síncrono de enlace de datos)
- TOKEN (Red en anillo)
- FDDI (Fiber Distributed Data Interface)

Los gestores de dispositivos DLC utilizan protocolos y funciones de capa más alta, más allá del ámbito del controlador de dispositivos del kernel. Sin embargo, los gestores residen en el kernel para conseguir un rendimiento máximo y utilizan un controlador de dispositivos del kernel para las peticiones de E/S al adaptador. Los usuarios DLC se encuentran en el kernel o por encima del mismo.

El Control síncrono de enlace de datos (SDLC) y el Control de enlace de datos IEEE 802.2 son ejemplos de gestores de dispositivos DLC. Cada gestor de dispositivos DLC funciona con un controlador de dispositivos o un conjunto de controladores de dispositivos específico. Por ejemplo, SDLC funciona con un controlador de dispositivos multiprotocolo para el producto del sistema y el adaptador asociado al mismo.

En la figura "Entorno del gestor de dispositivos DLC" se muestra la estructura básica del entorno DLC. Los usuarios que se encuentren en el kernel tienen acceso a los almacenamientos intermedios de memoria de comunicaciones (mbufs) y llaman a los puntos de entrada "add" a través de los servicios del kernel **fp**.

Los usuarios por encima del kernel acceden a los controladores de dispositivos de interfaz a kernel estándares y el sistema de archivos llama a los puntos de entrada **dd**. Las transferencias de datos necesitan el traslado de los datos entre espacio del usuario y del kernel.



### Entorno de gestor de dispositivos DLC

Figura 43. Entorno del gestor de dispositivos DLC

Esta ilustración muestra el enlace entre el usuario de la aplicación y el adaptador (a nivel de hardware). En medio se encuentra las áreas siguientes: Usuario del kernel, Subsistema de E/S de archivos, Gestor de dispositivos DLC, Controlador de dispositivos de E/S de comunicaciones y Agrupación de almacenamientos intermedios. Estas entidades intermedias se encuentran a nivel del kernel.

Los componentes del entorno del Gestor de dispositivos DLC son los siguientes:

Item	Descripción
<b>Usuario de la aplicación</b>	Reside por encima del kernel como una aplicación o un método de acceso.
<b>Usuario del kernel</b>	Reside en el kernel como un proceso del kernel o un gestor de dispositivos.
<b>Subsistema de E/S de archivos</b>	Convierte las subrutinas de puntero de archivos y descriptor de archivos en accesos de puntero de archivos de la tabla de conmutación.
<b>Agrupación de almacenamientos intermedios</b>	Proporciona servicios de almacenamiento intermedio de datos para el subsistema de comunicaciones.
<b>Controlador de dispositivos de E/S de comunicaciones</b>	Controla los registros de E/S de los adaptadores y del acceso directo a memoria (DMA) y direcciona los paquetes de recepción a varios DLC.
<b>Adaptador</b>	Conecta con el soporte de comunicaciones.

Un gestor de dispositivos escrito de acuerdo con las especificaciones GDLC puede ejecutarse en todas las configuraciones de hardware del sistema operativo que contengan un controlador de dispositivos de comunicaciones y el adaptador de destino correspondiente. Cada gestor de proporciona soporte a varios usuarios por encima, así como a varios controladores de dispositivos y adaptadores por debajo. En general, los usuarios utilizan un solo adaptador de forma simultánea o cada usuario utiliza varios adaptadores. Los gestores de dispositivos DLC varían según las restricciones de sus protocolos.

La Figura 44 en la página 751 ilustra una configuración de varios usuarios:

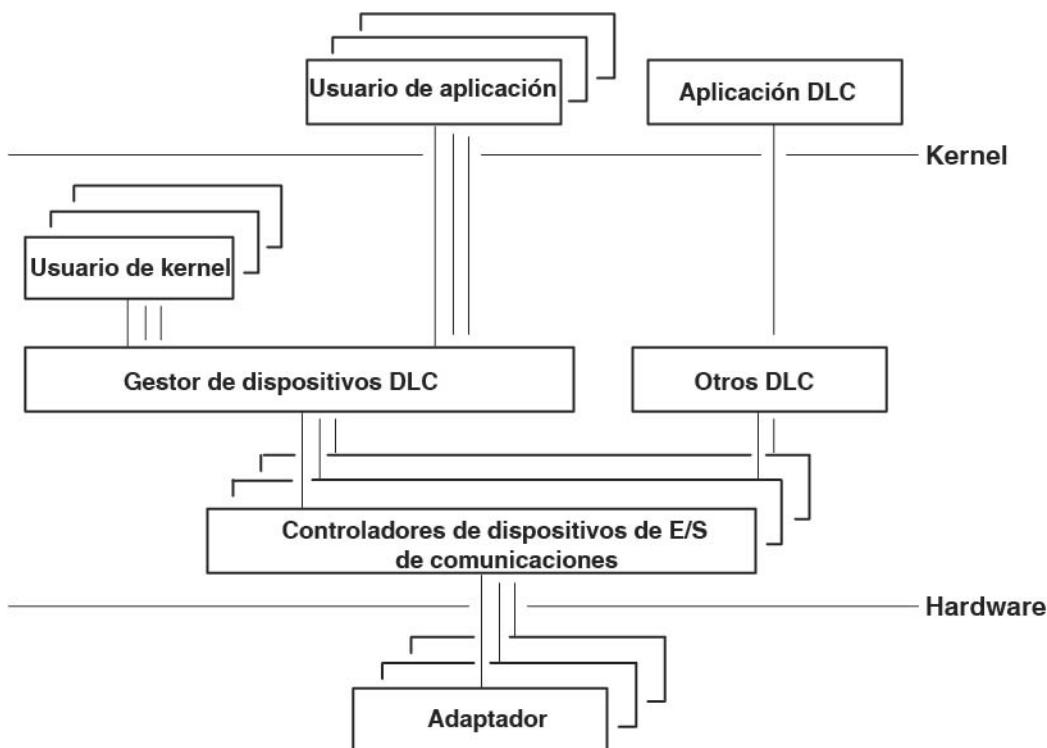


Figura 44. Configuración de varios usuarios y varios adaptadores

Esta ilustración muestra otra vista a nivel de kernel entre el usuario de la aplicación y el adaptador. Presenta varias entidades que representan varios usuarios.

## Criterios de GDLC

Una interfaz GDLC debe cumplir los criterios siguientes.

- Ser flexible y accesible para los usuarios tanto de la aplicación como del kernel.
- Ofrecer la posibilidad para varios usuarios y varios adaptadores, permitiendo que los protocolos se beneficien de varias sesiones y puertos.
- Proporcionar soporte tanto a los servicios orientados a conexiones como a los servicios sin conexión siempre que sea posible.
- Permitir una transferencia de datos transparente para requisitos especiales más allá del ámbito del gestor de dispositivos DLC que se utilice.

## Interfaz GDLC

Cada gestor de dispositivos DLC es una entrada /dev estándar que funciona en el kernel como un gestor de dispositivos multiplexado para un protocolo en concreto.

Para un adaptador que DLC no esté utilizando, cada subrutina open a un gestor de dispositivos DLC crea un proceso de kernel. También se emite una subrutina open al manejador de dispositivos del adaptador de destino. En caso necesario, pueden emitirse subrutinas open adicionales para varios puertos de adaptadores DLC del mismo protocolo. Las subrutinas open que tengan como objetivo el mismo puerto no crean procesos del kernel adicionales, sino que enlazan la subrutina open con el proceso existente. Siempre hay un proceso de kernel para cada puerto en uso.

La estructura interna de un gestor de dispositivos DLC tiene la misma estructura básica que el manejador de dispositivos del kernel, con la excepción de que el proceso del kernel sustituye el manejador de interrupciones en los sucesos asíncronos. Los bloques de lectura, grabación, control de E/S y selección funcionan tal como se muestra en la figura "Gestor de dispositivos del kernel estándar".

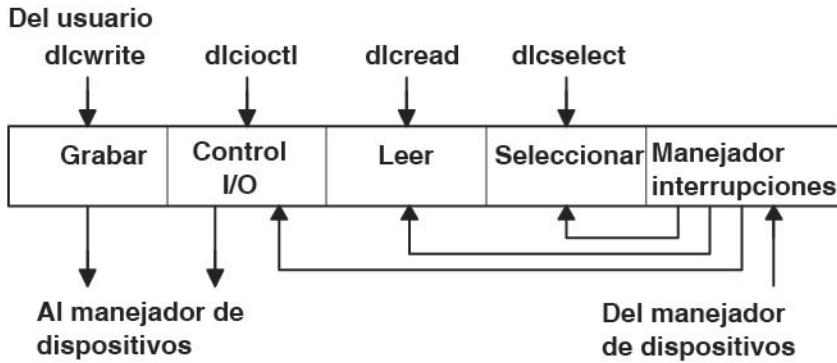


Figura 45. Gestor de dispositivos del kernel estándar

Esta ilustración muestra la estructura interna del gestor de dispositivos DLC. Esta estructura está formada por un bloque de grabación, control de E/S, lectura, selección y manejador de interrupciones. El Gestor de dispositivos recibe la información del usuario donde se pasa a las distintas áreas antes de pasarse al manejador de dispositivos.

## Controles de enlace de datos GDLC

Los DLC pueden instalarse por separado o en grupo. Un gestor de dispositivos DLC se añade al kernel automáticamente y se establece en estado "Disponible" para cada tipo de DLC instalado.

La instalación puede verificarse emitiendo el mandato **ls1pp** de la forma siguiente:

```
ls1pp -h dlctype
```

donde **dlctype** es uno de los siguientes:

Item	Descripción
<b>bos.dlc.8023</b>	Control de enlace de datos IEEE Ethernet (802.3)
<b>bos.dlc.ether</b>	Control de enlace de datos Ethernet estándar (802.3)
<b>bos.dlc.fddi</b>	Control de enlace de datos FDDI
<b>bos.dlc.sdlc</b>	Control de enlace de datos SDLC
<b>bos.dlc.token</b>	Control de enlace de datos Token-Ring

La información sobre un DLC instalado puede visualizarse a través de la herramienta System Management Interface Tool (SMIT) o la línea de mandatos. En puertos de comunicaciones o sistemas con una utilización densa, es posible que sea necesario modificar los atributos del DLC para ajustar el rendimiento del DLC. Si el rendimiento de la recepción es lento y las anotaciones cronológicas de errores del sistema indican que se están produciendo un desbordamiento de la cola de anillo entre el DLC y el manejador de dispositivos, aumente la profundidad de la cola DLC para los datos de entrada. Finalmente, es recomendable eliminar un DLC instalado del kernel cuando no sea necesario durante un período de tiempo largo. Esta eliminación no elimina el DLC del sistema pero permite que los recursos del kernel se liberen para otras tareas hasta que el DLC vuelve a necesitarse. Las instrucciones para todas estas tareas se indican en el apartado ["Gestión de controladores de dispositivos DLC"](#) en la página 756.

## Operaciones de punto de entrada ioctl de interfaz GDLC

La interfaz de Control genérico de enlace de datos(GDLC) proporciona soporte a las siguientes operaciones de subrutina **ioctl**.

Item	Descripción
DLC_ENABLE_SAP	Habilita un punto de acceso a servicio (SAP).
DLC_DISABLE_SAP	Inhabilita un SAP.

<b>Item</b>	<b>Descripción</b>
DLC_START_LS	Inicia una estación de enlace en un SAP determinado como el que llama o el que escucha.
DLC_HALT_LS	Detiene una estación de enlace.
DLC_TRACE	Rastrea la actividad de una estación de enlace durante actividades cortas o largas.
DLC_CONTACT	Contacta con una estación remota para una estación de enlace local en concreto.
DLC_TEST	Prueba el enlace remoto para una estación de enlace local en concreto.
DLC_ALTER	Modifica los parámetros de configuración de una estación de enlace.
DLC_QUERY_SAP	Consulta las estadísticas de un SAP en concreto.
DLC_QUERY_LS	Consulta las estadísticas de una estación de enlace en concreto.
DLC_ENTER_LBUSY	Entra en modalidad de local ocupado en una estación de enlace en concreto.
DLC_EXIT_LBUSY	Sale de la modalidad de local ocupado en una estación de enlace en concreto.
DLC_ENTER_SHOLD	Entra en modalidad de retención corta en una estación de enlace en concreto.
DLC_EXIT_SHOLD	Sale de la modalidad de retención corta en una estación de enlace en concreto.
DLC_GET_EXCEP	Devuelve notificaciones de excepción asíncronas al usuario de la aplicación.
<b>Nota:</b> El usuario del kernel no utiliza esta operación de subrutina ioctl ya que todas las condiciones de excepción se pasan al usuario del kernel a través del manejador de excepciones.	
DLC_ADD_GRP	Añade una dirección de recepción de multidifusión o grupo a un puerto.
DLC_DEL_GRP	Elimina una dirección de recepción de multidifusión o grupo de un puerto.
DLC_ADD_FUNC_ADDR	Añade una dirección funcional de recepción de multidifusión o grupo a un puerto.
DLC_DEL_FUNC_ADDR	Elimina una dirección funcional de recepción de multidifusión o grupo de un puerto.
IOCINFO	Devuelve una estructura que describe el gestor de dispositivos de GDLC. Consulte el archivo /usr/include/sys/devinfo.h para obtener más información.

### Punto de acceso de servicio (SAP) de GDLC

Un punto de acceso de servicio (SAP) identifica un servicio concreto de un usuario que envía y recibe una clase de datos concreta.

Esto permite dirigir distintas clases de datos a los manejadores de servicios correspondientes de forma independiente. Los DLC que proporcionan soporte a varios SAP simultáneos tienen direcciones conocidas como SAP de destino y SAP de origen en sus cabeceras de paquetes. Los DLC que sólo pueden proporcionar soporte a un solo SAP no necesitan ni utilizan el direccionamiento SAP, pero siguen teniendo el concepto de habilitar el SAP. En general, hay un SAP habilitado para cada usuario de DLC en cada puerto.

La mayoría de valores de dirección de SAP los definen entidades de gestión de red con el estándar IEEE o valores definidos por el usuario tal como se especifica en la publicación *Token-Ring Network Architecture Reference*. Algunas de las direcciones SAP más comunes son las siguientes:

Item	Descripción
<b>SAP nulo (0x00)</b>	Proporciona ciertas funciones para responder a los nodos remotos aunque no se haya habilitado ningún SAP. Este SAP sólo proporciona soporte a servicios sin conexión y sólo responde a la identificación de intercambios (XID) y a las Unidades de datos del protocolo de enlace (LPDU) de TEST.
<b>Control de vía de acceso SNA (0x04)</b>	Indica la dirección SAP individual por omisión que los nodos de Arquitectura de red de sistemas (SNA).
<b>NETBIOS de red de PC (0xF0)</b>	Utilizado para toda la comunicación DLC gestionada mediante la emulación del Sistema de entrada/salida básico de red (NetBIOS).
<b>SAP de descubrimiento (0xFC)</b>	Utilizado por los servicios de descubrimiento de nombre de la red de área local (LAN).
<b>SAP global (0xFF)</b>	Identifica todos los SAP activos.

#### **Estación de enlace de GDLC**

Una estación de enlace (LS) identifica una conexión entre dos nodos para un par SAP en concreto.

Esta conexión puede funcionar como un servicio sin conexiones (diagrama de datos) o servicio orientado a la conexión (transferencia de datos totalmente secuenciados con recuperación de errores). En general, se inicia una LS para cada conexión remota.

#### **Modalidad de local ocupado de GDLC**

Cuando una LS funciona en una modalidad orientada a las conexiones, necesita detener el envío de paquetes de información de la estación remota por motivos como, por ejemplo, la falta de recursos. Entonces puede enviarse una notificación a la estación remota que haga que la estación local entre en modalidad de local ocupado.

Una vez los recursos están disponibles, la estación local comunica al remoto que ya no está ocupado y que los paquetes de información pueden volver a fluir. Con la modalidad de local ocupado sólo se detienen los paquetes de información secuenciados. Todos los otros tipos de datos no resultan afectados.

#### **Modalidad de retención corta de GDLC**

La modalidad de funcionamiento de retención corta puede utilizarse al funcionar a través de ciertas redes de datos.

La modalidad de retención corta resulta útil con redes de datos que tienen las características siguientes:

- Un tiempo de configuración de llamada corto
- Una estructura de tarifa que especifica un precio relativamente pequeño para la configuración de la llamada en comparación con el coste por el tiempo de conexión.

Durante la modalidad de retención corta, sólo se mantiene una conexión entre dos estaciones mientras hay datos disponibles para la transferencia entre las dos estaciones. Cuando no hay ningún dato por enviar, la conexión se elimina después del período de tiempo de espera especificado y sólo se restablece cuando hay nuevos datos por transferir.

#### **Prueba y rastreo de los enlaces de GDLC**

Para probar una conexión entre dos estaciones, indique a una LS que envíe un paquete de prueba desde la estación local. Este paquete recibe eco de la estación remota si la conexión funciona correctamente.

Algunos enlaces de datos proporcionan un soporte limitado a esta función debido a restricciones de protocolo. SDLC, por ejemplo, sólo genera el paquete de prueba del sistema principal o la estación

primaria. Sin embargo, la mayoría de los otros protocolos permiten que los paquetes de prueba se inicien desde cualquier estación.

Para rastrear un enlace, datos de la línea y sucesos especiales (como, por ejemplo, la activación de la estación, la terminación y los tiempos de espera excedidos), obtenga un canal de rastreo genérico e indique a una LS que grabe las anotaciones cronológicas de rastreo en el recurso de rastreo genérico para cada LS. Esta función ayuda a determinar el motivo de ciertos problemas de conexión de las comunicaciones. Se proporciona soporte a las entradas de rastreo cortas y largas.

### **Estadísticas de GDLC**

Un usuario de GDLC puede consultar tanto las estadísticas de un SAP como las estadísticas de una LS.

Las estadísticas de un SAP incluyen el estado actual del SAP e información sobre el manejador del dispositivo. Las estadísticas de una LS incluyen los estados de la estación actual y varios contadores de fiabilidad, disponibilidad y servicio que supervisan la actividad de la estación desde el momento en que se inicia.

## **Servicios del kernel especiales de GDLC**

El control genérico de enlace de datos (GDLC) proporciona servicios especiales para un usuario del kernel.

Sin embargo, debe existir un entorno de confianza en el kernel. En vez de ser el gestor de dispositivos DLC quien copie los datos de sucesos asíncronos en el espacio del usuario, el usuario del kernel debe especificar punteros de función que apunten a rutinas especiales denominados manejadores de funciones. El DLC llama a los manejadores de funciones en el momento de la ejecución. Esto permite conseguir el rendimiento máximo entre el usuario del kernel y las capas del DLC. Cada usuario del kernel debe restringir el número de manejadores de funciones a una longitud de vía de acceso mínima y utilizar el esquema del almacenamiento intermedio de memoria (mbuf) de las comunicaciones.

Un manejador de funciones nunca debe llamar a otra entrada de DLC directamente. Esto es debido a que las llamadas directas se realizan bajo bloqueo, lo que provoca una suspensión fatal. La única excepción a esta regla es que un usuario del kernel podría llamar al punto de entrada dlcwritex durante su servicio de cualquiera de las cuatro funciones de datos de recepción. Llamar al punto de entrada dlcwritex permite la generación de respuestas inmediatas sin un conmutador de tareas intermedio. Se necesita lógica especial en el gestor de dispositivos DLC para comprobar la identificación del proceso del usuario que llama a una operación de grabación. Si se trata de un proceso DLC y la posibilidad de colocación en colas internas del DLC se ha sobrepasado, la grabación se devuelve con un código de retorno anómalo (valor de retorno EAGAIN) en lugar de dejar el proceso de llamada (DLC) en suspensión. Entonces es la subrutina del usuario que llama quien debe devolver una notificación especial al DLC desde la función de recepción de datos para garantizar un reintento del almacenamiento intermedio de recepción con posterioridad.

Los manejadores de funciones proporcionados por el usuario son los siguientes:

<b>Item</b>	<b>Descripción</b>
<b>Rutina de datos de diagrama de datos recibidos</b>	Llamada siempre que se recibe un paquete de diagramas de datos para el usuario del kernel.
<b>Rutina de condiciones de excepción</b>	Llamada siempre que se produce un suceso asíncrono que debe enviar una notificación al usuario del kernel como, por ejemplo, SAP cerrado o Estación contactada.
<b>Rutina de datos de I-Frame recibidos</b>	Llamada siempre que se recibe un paquete de datos de secuencia normal para el usuario del kernel.
<b>Rutina de datos de red recibidos</b>	Llamada siempre que se reciben datos específicos de la red para el usuario del kernel.

Item	Descripción
<b>Rutina de datos XID recibidos</b>	Llamada siempre que se recibe un paquete de identificación de intercambio(XID) para el usuario del kernel.

El usuario del kernel no llama a los puntos de entrada dlcread y dlcselect para el DLC porque el gestor de dispositivos de DLC llama directamente a las entradas funcionales asíncronas. Generalmente, estos sucesos se ponen en cola en la manejador de funciones del usuario. Sin embargo, si el usuario del kernel no puede manejar la recepción de un paquete en concreto, el gestor de dispositivos DLC puede retener el último almacenamiento intermedio de recepción y entrar en una de las modalidades especiales de usuario ocupado:

#### Modalidad de usuario finalizado ocupado (sólo I-frame)

Si el usuario del kernel no puede manipular una I-frame (debido a problemas como, por ejemplo, el bloqueo de las colas), se devuelve un código de retorno DLC\_FUNC\_BUSY y DLC retiene el puntero del almacenamiento intermedio y entra en modalidad de local ocupado para detener las transacciones I-frame de la estación remota. El usuario del kernel debe llamar a la función Salir de local ocupado para restablecer la modalidad de local ocupado y volver a iniciar la recepción de I-frames. Sólo es posible detener las I-frames con una secuencia normal. Los datos XID, los datos de red y los diagramas de datos no se ven afectados por la modalidad de local ocupado.

#### Modalidad temporización terminado ocupado (todos los tipos de tramas)

Si el usuario del kernel no puede manipular la recepción de un paquete en concreto y desea que DLC retenga el almacenamiento intermedio de recepción durante un breve período de tiempo y a continuación vuelva a llamar a la función de recepción del usuario, se devuelve un código de retorno DLC\_FUNC\_RETRY a DLC. Si la recepción del paquete es una I-frame secuenciada, la estación entra en modalidad de local ocupado durante este período. En todos los casos, se inicia un temporizador; una vez vence el temporizador, vuelve a llamarse a la entrada funcional de recepción de datos.

### Gestión de controladores de dispositivos DLC

Es necesario añadir un DLC al sistema antes de utilizarlo.

Cada DLC instalado se añade de forma automática después de la instalación y cada vez que se reinicia el sistema (consulte el apartado “Controles de enlace de datos GDLC” en la página 752). Si un DLC se ha eliminado y no ha vuelto a reiniciarse posteriormente, es posible volver a añadirlo.

Tabla 112. Tareas para la gestión de los controladores de dispositivos DLC		
Tarea	Vía rápida de SMIT	Mandato o archivo
Adición de un DLC instalado	Elija uno (según el nombre del controlador de dispositivos): smmit cmddlc_sdlc smmit cmddlc_token smmit cmddlc_qllc smmit cmddlc_ether <sup>1</sup> smmit cmddlc_fddi y seleccione <b>Añadir</b>	<b>mkdev</b> <sup>2</sup>
Modificación de los atributos del DLC <sup>3,4</sup>	Elija uno (según el nombre del controlador de dispositivos): smmit cmddlc_sdlc_ls smmit cmddlc_token_ls smmit cmddlc_qllc_ls smmit cmddlc_ether_ls <sup>1</sup> smmit cmddlc_fddi_ls	<b>chdev</b> <sup>2</sup>

Tabla 112. Tareas para la gestión de los controladores de dispositivos DLC (continuación)

Tarea	Vía rápida de SMIT	Mandato o archivo
Inicio de un rastreo de supervisión de la red de área local de DLC <sup>5</sup>	smit trace	<b>trace -j nnn</b> donde el valor <i>nnn</i> es el ID de enganche que debe rastrearse
Detención del rastreo de supervisión de la red de área local de DLC	smit trcstop	<b>trcstop</b> <sup>2</sup>
Generación de un informe de rastreo de supervisión de la red de área local de DLC	smit trcprt	<b>trcprt -d nnn</b> donde el valor <i>nnn</i> es el ID de enganche de que debe generarse un informe
Listado de la información actual del DLC <sup>3</sup>	Elija uno (según el nombre del controlador de dispositivos): smit cmddlc_sdlc_ls smit cmddlc_token_ls smit cmddlc_qllc_ls smit cmddlc_ether_ls <sup>1</sup> smit cmddlc_fddi_ls	<b>lsdev</b> <sup>2</sup> o <b>lsattr</b> <sup>2</sup>
Eliminación de un DLC <sup>3,6</sup>	Elija uno (según el nombre del controlador de dispositivos): smit cmddlc_sdlc_rm smit cmddlc_token_rm smit cmddlc_qllc_rm smit cmddlc_ether_rm <sup>1</sup> smit cmddlc_fddi_rm	<b>rmdev</b> <sup>2</sup>

**Nota:**

1. La vía rápida de SMIT para un gestor de dispositivos Ethernet incluya los controladores de dispositivos tanto de Ethernet estándar como de Ethernet IEEE 802.3.
2. Se proporcionan detalles sobre las opciones de la línea de mandatos en las descripciones de los mandatos para **mkdev**, **chdev**, **trace**, **trcstop**, **trcprt**, **lsdev**, **lsattr**, y **rmdev**.
3. Un DLC debe haberse instalado y añadido antes de poder listar, mostrar, modificar o eliminar sus atributos (consulte el apartado “Controles de enlace de datos GDLC” en la página 752). La modificación de un atributo sólo es satisfactoria si no hay activa ninguna operación de apertura del DLC de destino. Antes de emitir la acción de cambio, es posible que el usuario tenga que impedir que servicios como, por ejemplo, SNA, OSI o NetBIOS utilicen el DLC.
4. La modificación del tamaño de la cola de recepción afecta a los recursos del sistema directamente. Realice esta modificación sólo si el DLC experimenta problemas con la cola de recepción como, por ejemplo, un rendimiento lento o desbordamientos entre el DLC y el controlador de dispositivos.
5. Tenga cuidado al habilitar el rastreo de supervisión ya que ésta afecta directamente al rendimiento de los DLC y los asociados a los mismos.
6. La eliminación de un DLC sólo es satisfactoria si no hay activa ninguna operación de apertura en el DLC de destino. Antes de emitir la acción de eliminación, es posible que el usuario deba impedir que servicios como, por ejemplo, SNA, OSI o NetBIOS utilicen el DLC.

## Consulta de los adaptadores de comunicaciones y redes

Aquí pueden consultarse distintos ejemplos de configuración tanto para adaptadores PCI como para adaptadores asíncronos.

## Adaptadores PCI

Aquí se presenta información de instalación y configuración para adaptadores PCI.

Los temas descritos son el soporte y la configuración de los adaptadores PCI WAN (Red de área amplia) “Controlador de dispositivo de red HDLC multiprotocolo de 2 puertos” en la página 758 y “Adaptador PCI ARTIC960Hx” en la página 759).

### Controlador de dispositivo de red HDLC multiprotocolo de 2 puertos

El controlador de dispositivo de control de enlace de datos de alto nivel (HDLC) del adaptador multiprotocolo de 2 puertos es un componente del subsistema de E/S de comunicaciones. Este controlador de dispositivo proporciona soporte para la operación HDLC a través del adaptador multiprotocolo de 2 puertos a velocidades máximas de 1.544 Mbps.

Las opciones siguientes proporcionan acceso al controlador de dispositivo de red HDLC multiprotocolo de 2 puertos:

- Systems Network Architecture (SNA)
- La versión de SDLC (Synchronous data link control - control síncrono de enlace de datos) de la interfaz de programación GDLC
- Aplicaciones escritas por el usuario compatibles con MPQP-API (Multiprotocol Quad Port-Application Programming Interface - Interfaz de programación de aplicaciones de puerto de doble palabra multiprotocolo) de SDLC

**Nota:** Las opciones anteriores requieren el uso del archivo especial `mpcn`, que permite el acceso al controlador de dispositivo HDLC del adaptador multiprotocolo de 2 puertos a través del subsistema de emulación del controlador de dispositivo COMIO SDLC. Este subsistema se debe instalar y configurar para cada dispositivo de red HDLC.

- Aplicaciones escritas por el usuario compatibles con la API CDLI (Common Data Link Interface - Interfaz de enlace de datos común) HDLC

El controlador de dispositivo de adaptador multiprotocolo de 2 puertos permite la conectividad con sistemas principales remotos utilizando el adaptador multiprotocolo de 2 puertos, directamente a través de una línea alquilada o a través de circuitos conmutados. El controlador de dispositivo puede proporcionar una pasarela entre entornos de grupo de trabajo y recursos de proceso de datos remotos.

### Configuración de adaptador multiprotocolo de 2 puertos

Utilice estas explicaciones para configurar un adaptador multiprotocolo de 2 puertos.

Tabla 113. Tareas para configurar el adaptador multiprotocolo de 2 puertos	
Tarea	Vía rápida de SMIT
Añadir un controlador de dispositivo al adaptador	<code>smit mkhd1cdpmpdd</code>
Reconfigurar el controlador de dispositivo en el adaptador	<code>smit chhd1cdpmpdd</code>
Eliminar un controlador de dispositivo en el adaptador	<code>smit rmhd1cdpmpdd</code>
Dejar disponible un controlador de dispositivo definido	<code>smit cfghd1cdpmpdd</code>
Añadir un emulador COMIO SDLC en el adaptador	<code>smit mksdlcsciedd</code>
Reconfigurar el emulador COMIO SDLC en el adaptador	<code>smit chsdlcsciedd</code>
Eliminar un emulador COMIO SDLC en el adaptador	<code>smit rmsdlcsciedd</code>
Dejar disponible un emulador COMIO SDLC definido	<code>smit cfgsdlcsciedd</code>

### **Adaptador PCI ARTIC960Hx**

El emulador de controlador de dispositivo COMIO MPQP del adaptador PCI ARTIC960Hx es un componente del subsistema de E/S de comunicaciones. Este controlador de dispositivo proporciona soporte para el adaptador PCI ARTIC960Hx a una velocidad máxima de 2 M bps.

Los módems utilizados deben proporcionar la temporización, puesto que sólo se soporta la temporización externa.

Las opciones siguientes proporcionan acceso al controlador de dispositivo COMIO MPQP del adaptador PCI ARTIC960Hx:

- Systems Network Architecture (SNA)
- Interfaz de programación de GDLC (control de enlace de datos genérico)
- Aplicaciones escritas por el usuario compatibles con MPQP-API (Multiprotocol Quad Port-Application Programming Interface - Interfaz de programación de aplicaciones de puerto de doble palabra multiprotocolo), por ejemplo aplicaciones SDLC y BiSync.

Estas opciones requieren el uso del archivo especial `mpqx`, que permite el acceso al adaptador PCI ARTIC960Hx a través del controlador de dispositivo de emulación COMIO MPQP. Este controlador de dispositivo se debe instalar y configurar para cada puerto del adaptador PCI ARTIC960Hx. El archivo especial `mpqx` reside en el directorio /dev.

**Nota:** La `x` de `mpqx` especifica la instancia del controlador de dispositivo, por ejemplo `mpq0`.

El controlador de dispositivo de emulación COMIO MPQP permite la conectividad con sistemas de principales remotos utilizando el adaptador PCI ARTIC960Hx, directamente a través de una línea alquilada. El controlador de dispositivo puede proporcionar una pasarela entre entornos de grupo de trabajo y recursos de proceso de datos remotos.

### **Configuración de controlador de emulación COMIO MPQP sobre el adaptador PCI ARTIC960Hx**

Utilice estas explicaciones para configurar el controlador de emulación COMIO MPQP sobre el adaptador PCI ARTIC960Hx.

<i>Tabla 114. Tareas para configurar el controlador de emulación COMIO MPQP</i>	
Tarea	Vía rápida de SMIT
Añadir un controlador de dispositivo	<code>smit mksd</code>
Reconfigurar el controlador de emulación COMIO MPQP	<code>smit chsdd</code>
Eliminar un controlador de dispositivo	<code>smit rmtsdd</code>
Configurar un controlador de dispositivo definido	<code>smit cfgsdd</code>
Añadir un puerto	<code>smit mksdports</code>
Reconfigurar un puerto de emulación COMIO MPQP	<code>smit chsdp</code>
Eliminar un puerto	<code>smit rmtsdp</code>
Configurar un puerto definido	<code>smit cfgsdports</code>
Rastrear el controlador de emulación COMIO MPQP	<code>smit trace_link</code>

### **Adaptadores asíncronos**

Los adaptadores asíncronos de 8 y 16 puertos estándares que se muestran en esta tabla.

La tabla siguiente resume estos productos:

*Tabla 115. Adaptadores asíncronos*

<b>Conexión asíncrona</b>	<b>Tipo de bus</b>	<b>Código de características o tipo de máquina (modelo)</b>	<b>Velocidad de datos máxima por puerto (KBits/seg)</b>	<b>Características destacables</b>
EIA 232 de 8 puertos	Micro Channel	2930	76,8	Estándar generalizado
EIA 422A de 8 puertos	Micro Channel	2940	76,8	Mayor distancia
MIL-STD 188 de 8 puertos	Micro Channel	2950	Selezionable en base a la velocidad del reloj del generador de la velocidad en baudios de UART.	MIL-STD 188-114 para interfaz digital de voltaje no equilibrado
EIA 232 de 8 puertos	ISA	2931	115,2	Mayor eficacia
EIA 232 de 8 puertos	ISA	2932	115,2	Mayor eficacia
EIA 422 de 8 puertos	PCI	2943	230	Mayor eficacia
EIA 232 de 16 puertos	Micro Channel	2955	76,8	Centro de conexión local
EIA 422A de 16 puertos	Micro Channel	2957	76,8	Mayor distancia
-	ISA	2933	-	-
-	PCI	2944	-	-

La tabla siguiente muestra las características detalladas de los productos.

*Tabla 116. Características de los productos de conexión asíncrona*

	<b>Puertos serie nativos</b>	<b>8 puertos</b>		<b>16 puertos</b>	<b>128 puertos con RAN</b>	
		<b>MC</b>	<b>ISA</b>		<b>MC</b>	<b>ISA</b>
Número de puertos asíncronos por adaptador	n/d	8	8	16	128	128
Número máximo de adaptadores	n/d	8	7	8	7	7
Número máximo de puertos asíncronos	2 o 3	64	56	128	896	896
Número de puertos asíncronos por RAN	n/d	n/d	n/d	n/d	16	16
Número máximo de RAN	n/d	n/d	n/d	n/d	56	56

Tabla 116. Características de los productos de conexión asíncrona (continuación)

	<b>Puertos serie nativos</b>	<b>8 puertos</b>		<b>16 puertos</b>	<b>128 puertos con RAN</b>	
Velocidad máxima (Kbits/seg)	Seleznable en base a la velocidad del reloj del generador de la velocidad en baudios de UART.	76,8	115,2	76,8	230	230
Método de conexión	estándar	directa	directa	directa	nodo	nodo
Interfaces eléctricas asíncronas soportadas	EIA 232	EIA 232 EIA 422A <sup>4</sup> MIL-STD <sup>4</sup> 188-11 4 <sup>4</sup>	EIA 232 EIA 422A	EIA 232 EIA 422A	EIA 232 EIA 422	EIA 232 EIA 422
Conektor estándar	DB25M/ MODU	DB25M	DB25M	DB25M	RJ-45 <sup>2</sup>	RJ-45 <sup>2</sup>
Opciones del cable DB25	n/d	n/d	n/d	n/d	RJ-45-DB25	RJ-45-DB25
Opción de montaje en bastidor	n/d	n/d	n/d	n/d	sí	sí
Fuente de alimentación	n/d	n/d	n/d	n/d	externa	externa
Señales soportadas (EIA 232)	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS <sup>3</sup> -DTR - DCD -	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI

**Nota:**

1. El zócalo acepta los conectores RJ-45 de 8p, RJ-11 de 6p o RJ-11 de 4p con una reducción en las señales soportadas.
2. RTS está conectado alto (+12V) en la caja del conector de despliegue del cable de la interfaz de 16 puertos EIA 232 (FC 2996).
3. Micro Channel solamente.

Cada producto que se ofrece está caracterizado por un caso representativo donde comprobar sus puntos fuertes. A continuación se muestran recomendaciones para cada uno:

**Conceptos relacionados**

Dispositivo de terminal TTY

Un dispositivo de terminal tty es un dispositivo de caracteres que realiza la entrada y la salida de carácter en carácter.

**Información relacionada**

Guía de instalación y utilización del Adaptador PCI EIA-232 asíncrono de 2 puertos

**Micro Channel de 8 puertos**

Entre las características del adaptador Micro Channel de 8 puertos se incluye una ranura de bus Micro Channel disponible para la E/S asíncrona.

Otras características incluyen lo siguiente:

- Menos de ocho puertos con escasa o ninguna ampliación.
- Todos los terminales locales están situados a 61 metros (200 pies) del sistema.
- Terminales remotos necesarios (soporte mediante multiplexor/módem OEM)
- Demanda de ancho de banda de dispositivo entre baja y moderada (hasta 76,8 Kbps).

#### **Bus ISA de 8 puertos EIA 232 o EIA 232/EIA 422**

Entre las características del adaptador del bus ISA de 8 puertos EIA 232 o EIA 232/EIA 422 se incluye una ranura para ISA.

Otras características incluyen lo siguiente:

- Se necesitan menos de ocho puertos con escasa o ninguna ampliación.
- Requiere todos los puertos EIA 232, todos EIA 422 o una combinación de puertos EIA 232 y EIA 422.
- Interrupción de carácter de descarga y proceso de E/S de terminal de la CPU principal.
- Velocidades asíncronas de hasta 115,2 Kbps.
- Rendimiento máximo para los módems de alta velocidad (28,8 Kbps) con compresión de datos.

#### **Micro Channel de 16 puertos**

Entre las características del adaptador Micro Channel de 16 puertos se incluyen una ranura de bus Micro Channel disponible para la E/S asíncrona.

Otras características incluyen lo siguiente:

- Ocho puertos ahora, menos de 16 puertos con escasa o ninguna ampliación.
- Todos los terminales locales están situados a 61 metros (200 pies) del sistema.
- Terminales remotos necesarios (soporte mediante multiplexor/módem OEM)
- Los dispositivos no necesitan todas las señales EIA 232.
- Demanda de ancho de banda de dispositivo entre baja y moderada (hasta 38,4 Kbps para los dispositivos asíncronos).

#### **Adaptador de 128 puertos (Micro Channel, ISA)**

Entre las características del Micro Channel de 128 puertos o del adaptador ISA se incluyen dieciséis puertos que pueden ampliarse a hasta 128 puertos sin ranuras adicionales.

Otras características incluyen lo siguiente:

- Disponible una ranura de bus Micro Channel, ISA o PCI para la E/S asíncrona. (Para obtener más información sobre PCI, consulte [“Consideraciones para la selección de un producto” en la página 662](#)).
- Terminal más distante situada a unos 300 metros (1000 pies) del sistema a la velocidad de datos máxima para Micro Channel y los adaptadores ISA.
- Terminales planificados: cercanos o en la instalación, distantes en la instalación o remotos.
- Se necesita un elevado rendimiento asíncrono con baja demanda del procesador.
- Se necesita la posibilidad de una impresora conectada al terminal.
- Se necesita conectar a las instalaciones remotas a través de módems síncronos o de fibra óptima.

#### **Listado de los adaptadores Micro Channel asíncronos de 128 puertos definidos utilizando SMIT**

Siga este procedimiento para listar todos los adaptadores asíncronos de 128 puertos definidos con independencia de si están disponibles o no.

1. Utilice la vía rápida smit lsd128psync. El sistema busca la información y la visualiza.
2. Salga de la interfaz de SMIT.

#### **Adaptador ISA/PCI asíncrono de 8 puertos**

El adaptador ISA asíncrono de 8 puertos es una característica de las comunicaciones serie multicanal e inteligente disponible para los sistemas Basada en procesador POWER.

Los adaptadores ISA contienen 128K de memoria de acceso aleatorio (RAM) de alta velocidad de dos puertos utilizada para el código del programa y el almacenamiento intermedio de los datos. Los puertos asíncronos los ejecuta un procesador IDT 3041 de 32 bits a 16 MHz que proporciona soporte a velocidades de rendimiento de 115 Kbps.

El procesador 3041 y la RAM de dos puertos ayudan a descargar del sistema gran parte del proceso de los caracteres. Grandes bloques de datos se transfieren directamente al adaptador y entonces se envían en los puertos serie de carácter en carácter.

La RAM de dos puertos es accesible para las operaciones de lectura y de grabación tanto para adaptador como para el sistema. El sistema ve la RAM de dos puertos como su propia memoria y accede a la misma utilizando los mismos mandatos de consulta de memoria de alta velocidad que utiliza para la memoria interna.

El adaptador ISA de 8 puertos EIA 232 sólo proporciona soporte a los dispositivos EIA 232. Este adaptador necesita que se instale en el sistema el paquete de dispositivos `devices.isa.cxia`.

El adaptador ISA de 8 puertos EIA 232/422 proporciona soporte a los dispositivos EIA 232 y EIA 422. Ambos tipos de dispositivos pueden configurarse en cualquier combinación en cada puerto. Este adaptador necesita que se instale en el sistema el paquete de dispositivos `devices.isa.pc8s`.

Los paquetes anteriores requieren el paquete `devices.common.IBM.cx`.

### **Instalación de adaptadores de 8 puertos**

El sistema operativo no puede detectar los adaptadores ISA de forma automática, por lo que deben instalarse manualmente.

1. Para configurar los adaptadores ISA EIA 232/EIA 422 asíncronos de 8 puertos de IBM debe utilizarse la vía rápida `smit mkdev_isa` para acceder a la pantalla **Añadir un adaptador ISA**.
2. Seleccione **pcxr** (para el adaptador EIA 232 de 8 puertos) o **pc8s** (para el adaptador EIA 232/EIA 422 de 8 puertos) y pulse Intro.
3. Seleccione el bus adecuado y pulse Intro.
4. En el campo Dirección de E/S de bus, establezca la dirección en la dirección del adaptador (establecida por los conmutadores DIP del adaptador). Para obtener información adicional sobre los conmutadores DIP, consulte la publicación *8 Port Asynchronous ISA Adapter Installation Guide*. El resto de la configuración del adaptador se realiza de forma automática cuando el sistema muestra `sax` disponible.
5. Cuando haya finalizado, seleccione **Ejecutar**.

**stty-cxma** es un programa de utilidad que establece y visualiza las opciones del terminal para los adaptadores Micro Channel de 128 puertos y ISA de 8 y 128 puertos que se encuentra en el directorio `/usr/lbin/tty`. El formato es el siguiente:

```
stty-cxma [-a] [opciones] [ttynname]
```

Si no se especifica ninguna opción, **stty-cxma** visualiza todos los valores especiales del controlador, las señales del módem y todos los parámetros estándares que **stty(1)** muestra para el dispositivo de tty al que la entrada estándar hace referencia. Se proporcionan opciones de mandatos para cambiar los valores de control de flujo, establecer opciones de impresión transparente, forzar líneas de control del módem y visualizar todos los valores de tty. Las opciones que no se reconocen se pasan a **stty(1)** para que las interprete. Las opciones son las mismas que las utilizadas para los adaptadores PCI. Para obtener más información, consulte el apartado “Opciones de terminal stty-cxma” en la página 704.

### **Puertos de E/S estándares**

La mayoría de los modelos de la unidad del sistema tienen dos puertos serie asíncronos integrados (estándares) EIA 232.

El modelo M20/M2A ofrece un solo puerto serie asíncrono integrado que puede convertirse para proporcionar soporte a dos dispositivos serie utilizando un cable de despliegue opcional. Los dispositivos serie asíncronos EIA 232 pueden conectarse directamente a los puertos serie estándares utilizando cables serie estándares con conectores de shell D de 9 patillas o de 25 patillas.

**Nota:** Para la plataforma basada en Itanium, los dispositivos serie asíncronos EIA 232 puede conectarse directamente a los puertos serie estándares utilizando los cables serie estándares con conectores D-shell de 9 patillas.

Las máquinas capaces de procesos múltiples tienen tres puertos serie.

#### **Configuración de un dispositivo de terminal asíncrono EIA 232**

Este procedimiento permite definir y configurar un dispositivo tty conectado a un adaptador asíncrono de un puerto serie estándar, de 8 puertos o de 16 puertos.

1. Utilice la vía rápida smit mkitty para acceder al menú **Añadir un TTY**.
2. Seleccione **Añadir un TTY**.
3. Seleccione **Terminal asíncrono tty rs232**.
4. Seleccione uno de los adaptadores disponibles de E/S estándar, de 8 puertos o de 16 puertos que aparecen en la pantalla.  
Si no se visualiza ningún adaptador o si éstos se encuentran en estado definido, vuelva a comprobar la configuración, el cableado y la instalación.
5. En los campos de diálogo que se muestran, puede añadir o modificar atributos del tty.
6. Cuando haya finalizado, seleccione **Ejecutar**.

#### **Configuración de un dispositivo de impresora/trazador asíncrono EIA 232**

Este procedimiento permite definir y configurar un dispositivo de impresora/trazador conectado a un puerto serie estándar, una adaptador asíncrono de 8 puertos o un adaptador asíncrono de 16 puertos.

1. Para crear un dispositivo de impresora/trazador en un adaptador asíncrono, utilice la vía rápida smit pdp para acceder al menú **Dispositivos de impresora/trazador**.
2. Seleccione **Añadir una impresora/trazador**.
3. Seleccione entre la lista de tipos de impresoras y trazadores que se muestra en la pantalla y pulse Intro.

Para este ejemplo, se ha realizado la selección siguiente:

osp (Otra impresora serie)

4. Seleccione la opción **rs232**.
5. Seleccione entre los controladores de 8 puertos disponibles en la pantalla. Si no se visualiza ningún controlador o si éstos se encuentran en estado definido, vuelva a comprobar la configuración, el cableado y la instalación.
6. En los campos de diálogo que se muestran, puede añadir o modificar atributos del dispositivo de impresora/trazador.
7. Cuando haya finalizado, seleccione **Ejecutar**.

#### **Adaptadores asíncronos Micro Channel de 8 puertos**

La familia de adaptadores asíncronos se basa en un diseño funcional común. Sin embargo, las características de cada adaptador en concreto vienen determinadas por las interfaces soportadas del dispositivo.

**Nota:** El apartado siguiente no es aplicable a la plataforma basada en Itanium.

La familia está formada por tres adaptadores:

- Adaptador asíncrono de 8 puertos - EIA 232
- Adaptador asíncrono de 8 puertos - MIL-STD-188
- Adaptador asíncrono de 8 puertos - EIA 422A

La familia de adaptadores de 8 puertos se basa en el chip de recepción y transmisión asíncrona universal dual (DUART) que proporciona dos canales de comunicaciones serie.

Los apartados siguientes contiene información detallada sobre los adaptadores de 8 puertos.

### **Adaptador asíncrono de 8 puertos - EIA 232**

El EIA 232 es un adaptador asíncrono de 8 puertos que proporciona soporte para conectar un máximo de ocho dispositivos serie asíncronos EIA 232D (como, por ejemplo, módems, terminales, trazadores e impresoras) a una unidad del sistema.

El sistema debe basarse en un bus Micro Channel o un bus ISA y permitir hasta ocho adaptadores de 8 puertos.

Este adaptador es totalmente programable y sólo proporciona soporte a las comunicaciones asíncronas. También permite añadir y eliminar bits de inicio y de parada y proporciona soporte a la paridad par, impar o sin paridad en los datos serie. Un generador de velocidad en baudios programable permite el funcionamiento entre 50 y 38.400 bps para el bus Micro Channel y entre 50 y 115.200 bps para el bus ISA. Los adaptadores proporcionan soporte a caracteres de 5, 6, 7 u 8 bits con 1, 1,5 o 2 bits de parada. Un sistema de interrupciones de prioridad controla las interrupciones de transmisión, recepción, error, estado de la línea y archivos.

### **Instalación del adaptador asíncrono de 8 puertos**

El adaptador asíncrono de 8 puertos cabe en una sola ranura de Micro Channel en el sistema. Siga los pasos siguientes para instalar el adaptador.

1. Verifique que todos los usuarios hayan salido del sistema y ejecute el mandato siguiente:

```
shutdown -F
```

2. Cuando el mandato **shutdown** finalice, gire el interruptor de alimentación del sistema hasta la posición de apagado.
3. Abra la caja del sistema e inserte el adaptador asíncrono de 8 puertos en una ranura libre de Micro Channel.
4. Conecte el conector de shell D de 78 patillas del cable de la interfaz de 8 puertos al adaptador de 8 puertos.
5. Vuelva a colocar los paneles de recubrimiento en la unidad del sistema.
6. Apriete el interruptor de alimentación del sistema hasta la posición de encendido. El sistema reconocerá y configurará el adaptador de 8 puertos durante el proceso de arranque.
7. Cuando el arranque finalice, inicie la sesión utilizando el proceso de arranque del ID de usuario root.

```
lsdev -Cc adapter | pg
```

Sólo aquellos adaptadores que se encuentren en un estado disponible están listos para que el sistema los utilice.

Si el adaptador que acaba de instalarse *no* está disponible, verifique:

- Que el adaptador esté instalado correctamente en la ranura de Micro Channel.
- Que todo el cableado necesario esté conectado y colocado estrechamente en su lugar.
- Ejecute el mandato: **errpt -a | pg** y examine el informe de errores del sistema por si aparecen errores relacionados con los adaptadores.
- Ejecute el mandato: **cfgmgr -v | pg**. Este mandato intentará volver a configurar el adaptador sin rearrancar. Observe si hay errores en la salida paginada.

Si la ejecución de **cfgmgr** falla, será necesario volver a arrancar.

### **Información sobre el hardware del adaptador asíncrono de 8 puertos**

La interfaz del sistema proporciona al chip DUART una dirección de 3 bits y datos de 8 bits, así como líneas de control. Los datos de la interfaz del sistema se serializan para la transmisión a un dispositivo externo. Los datos serie pueden incluir un bit de paridad en el límite de bytes. Por el contrario, los datos de un dispositivo externo se deserializan para su transmisión a la interfaz del sistema. Estos datos también pueden incluir un bit de paridad, que puede comprobarse opcionalmente. Si así se elige, el canal puede funcionar en modalidad FIFO (primero en entrar primero en salir).

En modalidad FIFO, es posible colocar en los almacenamientos intermedios hasta 16 bytes tanto en el transmisor como en el receptor. La interfaz serie utiliza el protocolo de inicio-parada tanto para los datos de transmisión como de recepción. Es decir, cada byte (más el bit de paridad) está limitado por uno o más bits de inicio y bits de parada, que permite la sincronización en base a cada carácter individual (byte).

El chip DUART utiliza un oscilador de 12,288 MHz para generar su temporización interna para controlar la lógica del transmisor y del receptor. El canal proporciona soporte al funcionamiento dúplex. Se implementan cuatro chips DUART en cada adaptador de 8 puertos.

Hay disponibles trece registros a los que el sistema puede acceder. Entre las características programables de cada canal se incluyen:

- Longitud de los caracteres: 5, 6, 7 u 8 bits
- Generación/detección de paridad: Par, impar o ninguna
- Número de bits de parada: 1, 1,5 o 2
- Habilitación/inhabilitación de interrupciones. Datos recibidos disponibles.
- El transmisor que retiene el registro está vacío
- Estado de línea
- Error de desbordamiento
- Error de paridad
- Error de trama
- Interrupción.

La tabla siguiente es un resumen de las características de la (interfaz del dispositivo) del puerto para los adaptadores.

<i>Tabla 117. Características del puerto del adaptador asíncrono de 8 puertos</i>			
Parámetro	EIA 232	MIL-STD 188	EIA 422A
Topología	Punto a punto	Punto a punto	Punto a punto
Velocidad de datos máxima	138,4 Kbps (MC)/115,2 (ISA)	138,4 Kbps	138,4 Kbps
Soportes de transmisión	Multiconductor	Multiconductor	Multiconductor
Número de hilos del cable	9 incluida la señal de toma de tierra	9 incluida la señal de toma de tierra	5 incluida la señal de toma de tierra
Longitud máxima del cable	61 m (200 pies)	130 m a 38,4 Kbps	1200 m < 90 Kbps
Conector de dispositivos	D de 25 patillas	D de 25 patillas	D de 25 patillas
Interfaz eléctrica	Sin equilibrar	Sin equilibrar	Equilibrada
Codificación de bits	Digital a dos niveles	Digital a dos niveles	Digital a dos niveles

La lógica de arbitraje de interrupciones establece la prioridad para los adaptadores según el esquema siguiente:

Adaptador	Prioridad
1	Más alta
2	
3	
4	
5	
6	

### Prioridad del canal de comunicaciones

Los canales DUART con interrupciones pendientes reciben servicio según un esquema de prioridad fija.

La prioridad más alta se asigna al puerto 0. La siguiente prioridad al puerto 1 y así sucesivamente. La prioridad más baja es el puerto 7.

### Descripción de la lógica de interrupción de los adaptadores asíncronos de 8 puertos

La lógica de interrupción se divide en la lógica de generación de interrupciones y en la lógica de arbitraje de interrupciones.

Las dos secciones lógicas se implementan en todos los adaptadores de 8 puertos. La lógica de generación de interrupciones proporciona al sistema la interfaz. Esta lógica genera las peticiones de interrupción del sistema y contiene la circuitería de compartimiento de interrupciones.

La función de la lógica de arbitraje de interrupciones consiste en identificar el adaptador de 8 puertos con la interrupción de mayor prioridad pendiente. La lógica coloca entonces la información sobre las interrupciones del puerto de prioridad más alta en el registro de arbitraje de interrupciones. Esto se lleva a cabo en una operación de lectura.

La lógica de arbitraje de interrupciones es exclusiva para el adaptador de 8 puertos y no debe confundirse con la lógica de arbitraje de Micro Channel.

#### Lógica de generación de interrupciones de 8 puertos

El adaptador asíncrono implementa ocho líneas de petición de interrupciones del sistema.

El adaptador implementa las ocho líneas siguientes de petición de interrupciones del sistema:

- IRQ 3
- IRQ 5
- IRQ 9
- IRQ 10
- IRQ 11
- IRQ 12
- IRQ 14
- IRQ 15

Durante el funcionamiento normal, sólo una línea de petición está activa. Todos los adaptadores de 8 puertos de un sistema deben utilizar el mismo nivel de interrupción para conseguir un rendimiento óptimo del sistema. La línea activa se selecciona escribiendo el registro POS adecuado durante el ciclo de configuración. El adaptador proporciona soporte al compartimiento de interrupciones e implementa una configuración del colector abierto. En esta disposición, la línea de interrupción tiene carga alta mediante una resistencia de carga del sistema. El adaptador tiene una línea de cargabaja para indicar una petición de interrupción activa.

#### Lógica de arbitraje de interrupciones de 8 puertos

La lógica de arbitraje de interrupciones determina la prioridad del servicio de software cuando dos o más adaptadores de 8 puertos o 16 puertos generan interrupciones.

Hasta ocho adaptadores de 8 puertos pueden co-residir en un sistema y funcionar simultáneamente. Esta lógica proporciona al sistema la identificación de los adaptadores y los puertos, así como el tipo de interrupción en una sola operación de lectura. Una vez se detecta una petición de interrupción, el sistema lee el registro de arbitraje de la interrupción de 16 bits, que se encuentra en la dirección de E/S0130.

### Señales de la interfaz de los adaptadores asíncronos de 8 puertos MIL-STD 188

Las siguientes señales de la interfaz están implementadas en cada puerto del adaptador.

<b>Señal</b>	<b>Definición</b>
<b>Tx Data</b>	Transmitir datos
<b>RTS</b>	Petición a enviar
<b>CTS</b>	Borrar para enviar
<b>DSR</b>	Conjunto de datos preparado
<b>Rx Data</b>	Recibir datos
<b>DCD</b>	Detección de portadora de datos
<b>DTR</b>	Terminal de datos preparado
<b>RI</b>	Indicador de llamada
<b>Sig Gnd</b>	Señal de toma de tierra

#### **Niveles de voltaje de las señales de MIL-STD 188 de 8 puertos**

Los niveles de voltaje para el adaptador MIL-STD 188 pueden explicarse mediante la inversión de la polaridad de la marca y el espacio o la marca normal y la polaridad del espacio.

Los niveles de voltaje para el adaptador MIL-STD 188 se explican en los apartados siguientes:

- Marca normal y polaridad de espacio
- Inversión de polaridad de la marca y el espacio.

La señal se encuentra en estado de marca cuando el voltaje del circuito de intercambio, medido en el punto de interfaz, es inferior a -4 V dc con respecto a la señal de toma de tierra. La señal se encuentra en estado de espacio cuando el voltaje es superior a +4 V dc con respecto a la señal de toma de tierra. La región entre +4 V dc y -4 V dc está definida como la región de transición y no representa un nivel válido. El voltaje inferior a -6 V dc o superior a +6 V dc tampoco constituye un nivel válido.

Durante la transmisión de los datos, el estado de marca representa el 1 binario y el estado de espacio el 0 binario.

Para los circuitos de control de la interfaz, la función está "activada" cuando el voltaje es superior a +4 V dc con respecto a la señal de toma de tierra y "desactivada" cuando el voltaje es inferior a -4 V dc con respecto a la señal de toma de tierra. En la tabla siguiente se muestran los niveles de las señales de MIL-STD 188:

<i>Tabla 118. Niveles de las señales de MIL-STD 188</i>			
<b>Voltaje de intercambio</b>	<b>Estado binario</b>	<b>Condición de la señal</b>	<b>Función de control de la interfaz</b>
Voltaje +	0	Espacio	Activada
Voltaje -	1	Marca	Desactivada

El estándar militar MIL-STD 188 requiere que los adaptadores proporcionen la posibilidad opcional de invertir las polaridades de los estados de marca y de espacio de las líneas de transmisión y de recepción. Esta función se proporciona de forma independiente en cada puerto.

El bit de registro de control del módem DUART 3 (salida 2) se utiliza para este fin. Cuando el 3 se establece en el valor 1, las polaridades de los estados de marca y de espacio se establecen en el estado normal. Cuando el bit 3 se establece en el valor 0, las polaridades de los estados de marca y de espacio se invierten.

La señal se encuentre en el *estado de espacio* cuando el voltaje es inferior a -4 V dc con respecto a la señal de toma de tierra. La señal se encuentra en el estado de marca cuando el voltaje es superior a +4 V dc con respecto a la señal de toma de tierra.

La región entre +4 V dc y -4 V dc está definida como la *región de transición* y no representa un nivel válido. El voltaje inferior a -6 V dc o superior a +6 V dc tampoco constituye un nivel válido.

Las características eléctricas de los puertos del adaptador asíncrono de 8 puertos MIL-STD 188 cumplen con las secciones de MIL-STD 188-114 que tratan sobre una interfaz de voltaje sin equilibrar. Es estándar es de fecha del 24 de marzo de 1976.

Los puertos del adaptador cumplen con los requisitos funcionales para el funcionamiento asíncrono (protocolo de inicio-parada) tal como se describen en el estándar EIA 232C con fecha de octubre de 1969 y en el estándar EIA 232D con fecha de enero de 1987.

#### **Señales de la interfaz de los adaptadores asíncronos de 8 puertos EIA 422A**

Las siguientes señales de la interfaz EIA 422A están implementadas en cada puerto del adaptador.

<b>Señal</b>	<b>Definición</b>
<b>TxA</b>	Transmitir datos
<b>TxB</b>	Transmitir datos
<b>RxA</b>	Recibir datos
<b>RxB</b>	Recibir datos
<b>Sig Gnd</b>	Señal de toma de tierra

#### **Niveles de voltaje de las señales de EIA 422A de 8 puertos**

El controlador de la línea genera un voltaje distinto comprendido entre 2 y 6 voltios (medido en el punto de interfaz del generador). La magnitud del voltaje diferencial en el receptor debe estar comprendida entre 200 milivoltios y 6 voltios (medidos en el punto de interfaz de la carga).

Las medidas se realizan en el terminal A (conductor positivo) con respecto al terminal B (conductor negativo). La tabla siguiente describe los estados de señal con respecto a los niveles de voltaje:

Tabla 119. Estados de las señales de EIA 422A de 8 puertos		
<b>Voltaje de intercambio</b>	<b>Estado binario</b>	<b>Condición de la señal</b>
Voltaje +	0	Espacio
Voltaje -	1	Marca

El adaptador asíncrono de 8 puertos EIA 422A proporciona soporte a un cableado de interior con una longitud de hasta 1200 m (4000 pies). Los cables de estas longitudes son susceptibles a sobrecargas de voltaje repentinamente debidas a voltajes inducidos como, por ejemplo, caídas de rayos indirectas. En el adaptador EIA 422A se ha implementado la circuitería de protección contra sobrecargas para protegerlo de estas sobrecargas de voltaje. La circuitería de protección contra sobrecargas se implementa en las líneas de datos de la interfaz del adaptador.

Se ha añadido circuitería con protección frente a fallos a los conductores de cada receptor EIA 422A para evitar condiciones de error cuando el receptor no está conectado a un controlador (cable abierto). La circuitería con protección frente a fallos establece el receptor en el estado de marca (1 binario) siempre que el receptor no está conectado a un controlador.

Las características eléctricas de los puertos del adaptador asíncrono de 8 puertos EIA 422A cumplen con el estándar EIA 422A con fecha de diciembre de 1978.

#### **Señales de la interfaz de los adaptadores asíncronos de 8 puertos EIA 232**

Las siguientes señales de la interfaz están implementadas en cada puerto del adaptador asíncrono de 8 puertos.

Las siguientes señales de la interfaz están implementadas en cada puerto del adaptador:

<b>Señal</b>	<b>Definición</b>
<b>TxD</b>	Transmitir datos
<b>RTS</b>	Petición a enviar

<b>Señal</b>	<b>Definición</b>
<b>CTS</b>	Borrar para enviar
<b>DSR</b>	Conjunto de datos preparado
<b>RxD</b>	Recibir datos
<b>DCD</b>	Detección de portadora de datos
<b>DTR</b>	Terminal de datos preparado
<b>RI</b>	Indicador de llamada
<b>Sig Gnd</b>	Señal de toma de tierra

#### **Niveles de voltaje de las señales de EIA 232 de 8 puertos**

La señal se encuentra en estado de marca cuando el voltaje del circuito de intercambio, medido en el punto de interfaz, es inferior a -3 V dc con respecto a la señal de toma de tierra. La señal se encuentra en estado de espacio cuando el voltaje es superior a +3 V dc con respecto a la señal de toma de tierra. La región entre +3 V dc y -3 V dc está definida como la *región de transición* y no representa un nivel válido. El voltaje inferior a -15 V dc o superior a +15 V dc tampoco constituye un nivel válido.

Durante la transmisión de los datos, el estado de marca representa el estado binario 1 y el estado de espacio el estado binario 0.

Para los circuitos de control de la interfaz, la función está activada cuando el voltaje es superior a +3 V dc con respecto a la señal de toma de tierra y desactivada cuando el voltaje es inferior a -3 V dc con respecto a la señal de toma de tierra. Consulte la tabla siguiente para ver los niveles de las señales de EIA 232:

*Tabla 120. Niveles de las señales de EIA 232*

<b>Voltaje de intercambio</b>	<b>Estado binario</b>	<b>Condición de la señal</b>	<b>Función de control de la interfaz</b>
Voltaje +	0	Espacio	Activada
Voltaje -	1	Marca	Desactivada

Las características eléctricas de los puertos del adaptador asíncrono de 8 puertos EIA 232 cumplen con el estándar EIA 232C con fecha de octubre de 1969 y con el estándar EIA 232D con fecha de enero de 1987.

Los puertos del adaptador cumplen con los requisitos funcionales para el funcionamiento asíncrono (protocolo de inicio-parada) tal como se describen en el estándar EIA 232C con fecha de octubre de 1969 y en el estándar EIA 232D con fecha de enero de 1987.

#### **Lógica de control de los adaptadores asíncronos de 8 puertos**

La sección de lógica de control basada en PAL coordina las actividades de todas las funciones importantes de los adaptadores.

Está cronometrada por un generador de ondas cuadradas de 40 MHz. Interactúa con el Micro Channel y entre sus funciones se incluye la decodificación de las direcciones, la comprobación de la paridad de las direcciones, la respuesta con las señales de control de E/S adecuadas y el control de la línea de petición de interrupción seleccionada (IRQ) (una de ocho líneas IRQ).

La lógica de control interactúa con los otros bloques de lógica del adaptador y en esta capacidad proporciona las líneas de control a los canales de comunicaciones (DUART) y la lógica de arbitraje de interrupciones. La lógica de control también interactúa con la lógica del controlador del bus de datos y proporciona control para la dirección del flujo de datos y para los bytes de datos de selección, que se colocan en el bus local. Controla el generador de paridad de datos, el comprobador de paridad y los pestillos.

## **Adaptadores asíncronos de 16 puertos**

La familia de adaptadores se basa en un diseño funcional común. Sin embargo, las características de cada adaptador en concreto vienen determinadas por las interfaces soportadas del dispositivo. La familia está formada por dos adaptadores, el adaptador asíncrono de 16 puertos EIA 422A y el adaptador asíncrono de 16 puertos EIA 232.

**Nota:** El apartado siguiente no es aplicable a la plataforma basada en Itanium.

La familia de adaptadores de 16 puertos se basa en el chip de recepción y transmisión asíncrona universal dual (DUART) que proporciona dos canales de comunicaciones serie. Podrá hallar más información sobre el chip DUART y el funcionamiento del mismo en la publicación [16-Port Asynchronous Adapter Hardware Information](#).

### **Adaptador asíncrono de 16 puertos - EIA 422A**

El adaptador asíncrono de 16 puertos EIA 232 proporciona soporte para conectar un máximo de 16 dispositivos serie asíncronos EIA 232 (impresoras y terminales) a una unidad del sistema.

Es posible utilizar hasta ocho adaptadores (cualquier combinación dentro de la familia) en una sola unidad del sistema.

Este adaptador es totalmente programable y sólo proporciona soporte a las comunicaciones asíncronas. Añade y elimina bits de inicio y bits de parada. Los adaptadores proporcionan soporte a la paridad par, impar o sin paridad en los datos serie. Un generador de velocidad en baudios programable permite un funcionamiento entre 50 y 38400 bps. Los adaptadores proporcionan soporte a caracteres de 5, 6, 7 u 8 bits con 1, 1,5 o 2 bits de parada. Un sistema de interrupciones de prioridad controla las interrupciones de transmisión, recepción, error, estado de la línea y archivos. Los 16 conectores para la conexión de dispositivos se proporcionan en el conjunto de cables de 16 puertos EIA 422A.

El adaptador de 16 puertos EIA 422A tiene las características siguientes:

- Tarjeta de factor de formato Micro Channel estándar.
- Velocidades de datos de hasta 38,4 Kbps por puerto.
- Almacenamiento intermedio de 16 bytes en las transmisiones y recepciones.
- Un solo conector de salida de 78 patillas (el cable de la interfaz de varios puertos se conecta a este conector).
- Circuitería de protección frente a sobrecargas.
- Proporciona soporte a cableados de hasta 1200 m (4000 pies).
- Proporciona soporte a las señales de las interfaces TxD y RxD.
- Interfaz de esclavo de Micro Channel 8 bits/16 bits.

### **Instalación del adaptador asíncrono de 16 puertos**

El adaptador asíncrono de 16 puertos cabe en una sola ranura de Micro Channel en el servidor. Para instalar el adaptador, siga estos pasos.

1. Verifique que todos los usuarios hayan salido del sistema y ejecute el mandato siguiente:

```
shutdown -F
```

2. Cuando el mandato **shutdown** finalice, gire el interruptor de alimentación hasta la posición de "apagado".
3. Abra la caja del servidor e inserte el adaptador asíncrono de 16 puertos en una ranura libre de Micro Channel.
4. Conecte el conector de shell D de 78 patillas del cable de la interfaz de 16 puertos al adaptador de 16 puertos.
5. Vuelva a colocar los paneles de recubrimiento en la unidad del sistema.
6. Apriete el interruptor de alimentación del sistema hasta la posición de encendido. El sistema reconocerá y configurará el adaptador de 16 puertos durante el proceso de arranque.

Cuando el arranque finalice, inicie la sesión utilizando el ID de usuario root y emita el mandato siguiente para comprobar la disponibilidad del sistema:

```
lsdev -Cc adapter | pg
```

Sólo aquellos adaptadores que se encuentren en el estado disponible están listos para que el sistema los utilice.

Si el adaptador que acaba de instalarse NO está disponible, verifique lo siguiente:

1. Que el adaptador esté instalado correctamente en la ranura de Micro Channel.
2. Que todo el cableado necesario esté conectado y colocado estrechamente en su lugar.
3. Ejecute el mandato: **errpt -a | pg** y examine el informe de errores del sistema por si aparecen errores relacionados con los adaptadores.
4. Ejecute el mandato: **cfgmgr -v | pg**. Este mandato intentará volver a configurar el adaptador sin rearrancar. Mire si hay errores en la salida paginada.
5. Si la ejecución de **cfgmgr** falla, será necesario volver a arrancar.

#### ***Información sobre el hardware del adaptador asíncrono de 16 puertos***

La interfaz del sistema proporciona al chip una dirección de 3 bits y datos de 8 bits, así como líneas de control. Los datos de la interfaz del sistema se serializan para la transmisión a un dispositivo externo. Los datos serie pueden incluir un bit de paridad en el límite de bytes. Por el contrario, los datos de un dispositivo externo se deserializan para su transmisión a la interfaz del sistema. Estos datos también pueden incluir un bit de paridad, que puede comprobarse opcionalmente. Si así se elige, el canal puede funcionar en modalidad FIFO (primero en entrar primero en salir).

En modalidad FIFO, es posible colocar en los almacenamientos intermedios hasta 16 bytes tanto en el transmisor como en el receptor. La interfaz serie utiliza el protocolo de inicio-parada tanto para los datos de transmisión como de recepción. Es decir, cada byte (más el bit de paridad) está limitado por un bit de inicio y un bit de parada, que permite la sincronización en base a cada carácter individual (byte).

El chip DUART utiliza un oscilador de 12,288 MHz para generar su temporización interna para controlar la lógica del transmisor y del receptor. El canal proporciona soporte al funcionamiento dúplex. Se implementan ocho chips DUART en cada adaptador de 16 puertos.

Hay disponibles trece registros a los que el sistema puede acceder. Entre las características programables de cada canal se incluyen:

- Longitud de los caracteres: 5, 6, 7 u 8 bits
- Generación/detección de paridad: Par, impar o ninguna
- Número de bits de parada: 1, 1,5 o 2
- Habilitación/inhabilitación de interrupciones. Datos recibidos disponibles.
- El transmisor que retiene el registro está vacío
- Estado de línea
- Error de desbordamiento
- Error de paridad
- Error de trama
- Interrupción.

La tabla siguiente es un resumen de las características de la (interfaz del dispositivo) del puerto para los adaptadores.

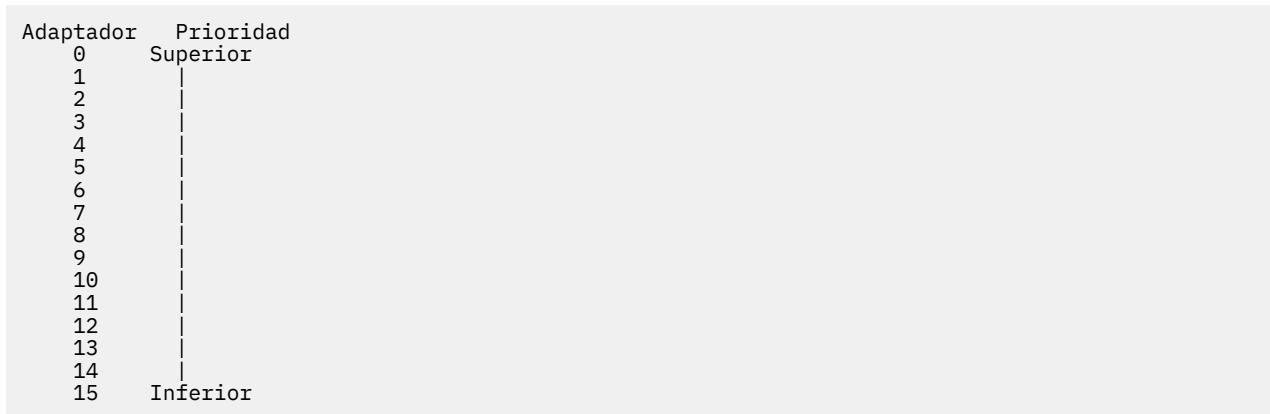
Tabla 121. Características del puerto del adaptador asíncrono de 16 puertos		
Parámetro	EIA 232	EIA 422A
Topología	Punto a punto	Punto a punto

Tabla 121. Características del puerto del adaptador asíncrono de 16 puertos (continuación)

Parámetro	EIA 232	EIA 422A
Velocidad de datos máxima (estándar)	20 Kbps	2 Mbps
Velocidad de datos máxima (placa)	38,4 Kbps	38,4 Kbps
Soportes de transmisión	Multiconductor	Multiconductor
Número de hilos del cable	5 incluida la señal de toma de tierra	5 incluida la señal de toma de tierra
Longitud máxima del cable	61 m (200 pies)	1200 m < 90 Kbps
Conecotor de dispositivos	D de 25 patillas	D de 25 patillas
Interfaz eléctrica	Sin equilibrar	Equilibrada
Codificación de bits	Digital a dos niveles	Digital a dos niveles

#### Prioridad de la placa del adaptador de los adaptadores asíncronos de 16 puertos

La lógica de arbitraje de interrupciones establece la prioridad para los adaptadores según un esquema específico.



Los canales DUART con interrupciones pendientes reciben servicio según un esquema de prioridad fija. La prioridad más alta se asigna al puerto 0. La siguiente prioridad al puerto 1 y así sucesivamente. La prioridad más baja es el puerto 15.

#### Lógica de interrupción de los adaptadores asíncronos de 16 puertos

Para los adaptadores asíncronos de 16 puertos, la lógica de interrupción se divide en la lógica de generación de interrupciones y la lógica de arbitraje de interrupciones.

Las dos secciones lógicas se implementan en todos los adaptadores de 16 puertos. La lógica de generación de interrupciones proporciona al sistema la interfaz. Esta lógica genera las peticiones de interrupción del sistema y contiene la circuitería de compartimiento de interrupciones.

La función de la lógica de arbitraje de interrupciones consiste en identificar el adaptador de 16 puertos con la interrupción de mayor prioridad pendiente. La lógica coloca entonces la información sobre las interrupciones del puerto de prioridad más alta en el registro de arbitraje de interrupciones. Esto se lleva a cabo en una operación de lectura.

La lógica de arbitraje de interrupciones es exclusiva para los adaptadores de 16 puertos y no debe confundirse con la lógica de arbitraje de Micro Channel.

#### Lógica de generación de interrupciones de 16 puertos

El adaptador asíncrono de 16 puertos implementa ocho líneas de petición de interrupciones del sistema.

El adaptador implementa las ocho líneas siguientes de petición de interrupciones del sistema (IRQ):

- IRQ 3
- IRQ 5
- IRQ 9
- IRQ 10
- IRQ 11
- IRQ 12
- IRQ 14
- IRQ 15

Durante el funcionamiento normal, sólo una línea de petición está activa. Todos los adaptadores de 16 puertos de un sistema deben utilizar el mismo nivel de interrupción para conseguir un rendimiento óptimo del sistema. La línea activa se selecciona escribiendo el registro POS adecuado durante el ciclo de configuración. El adaptador proporciona soporte al compartimiento de interrupciones e implementa una configuración del colector abierta tal como se define en la arquitectura de Micro Channel. En esta disposición, la línea de interrupción tiene carga alta mediante una resistencia de carga del sistema. El adaptador tiene una línea de carga baja para indicar una petición de interrupción activa.

#### *Lógica de arbitraje de interrupciones de 16 puertos*

La lógica de arbitraje de interrupciones determina la prioridad del servicio de software cuando dos o más adaptadores de 8 puertos o 16 puertos generan interrupciones.

Hasta ocho adaptadores de 8 puertos o de 16 puertos pueden co-residir en un sistema y funcionar simultáneamente. Esta lógica proporciona al sistema la identificación de los adaptadores y los puertos, así como el tipo de interrupción en una sola operación de lectura. Cuando se detecta una petición de interrupción, el sistema lee el registro de arbitraje de la interrupción de 16 bits, que se encuentra en la dirección de E/S 0130.

#### **Señales de la interfaz de los adaptadores asíncronos de 16 puertos EIA 232**

Las siguientes señales de la interfaz están implementadas en cada puerto del adaptador asíncrono de 16 puertos.

<b>Señal</b>	<b>Definición</b>
<b>TxD</b>	Transmitir datos
<b>DCD</b>	Detección de portadora de datos
<b>DTR</b>	Terminal de datos preparado
<b>RxD</b>	Recibir datos
<b>Sig Gnd</b>	Señal de toma de tierra

#### **Niveles de voltaje de las señales de EIA 232 de 16 puertos**

La señal se encuentra en estado de marca cuando el voltaje del circuito de intercambio, medido en el punto de interfaz, es inferior a -3 V dc con respecto a la señal de toma de tierra. La señal se encuentra en estado de espacio cuando el voltaje es superior a +3 V dc con respecto a la señal de toma de tierra. La región entre +3 V dc y -3 V dc está definida como la región de transición y no representa un nivel válido. El voltaje inferior a -15 V dc o superior a +15 V dc tampoco constituye un nivel válido.

Durante la transmisión de los datos, el estado de marca representa el estado binario 1 y el estado de espacio el estado binario 0.

Para los circuitos de control de la interfaz, la función está activada cuando el voltaje es superior a +3 V dc con respecto a la señal de toma de tierra y desactivada cuando el voltaje es inferior a -3 V dc con respecto a la señal de toma de tierra. Consulte la tabla siguiente para ver los niveles de las señales de EIA 232.

Tabla 122. Niveles de las señales de EIA 232

Voltaje de intercambio	Estado binario	Condición de la señal	Función de control de la interfaz
Voltaje +	0	Espacio	Activada
Voltaje -	1	Marca	Desactivada

Las características eléctricas de los puertos del adaptador asíncrono de 16 puertos EIA 232 cumplen con el estándar EIA 232C con fecha de octubre de 1969 y con el estándar EIA 232D con fecha de enero de 1987.

Los puertos del adaptador cumplen con los requisitos funcionales para el funcionamiento asíncrono (protocolo de inicio-parada) tal como se describen en el estándar EIA 232C con fecha de octubre de 1969 y en el estándar EIA 232D con fecha de enero de 1987.

#### **Señales de la interfaz de los adaptadores asíncronos de 16 puertos EIA 422A**

Las siguientes señales de la interfaz EIA 422A están implementadas en cada puerto del adaptador asíncrono de 16 puertos.

Señal	Definición
<b>TxA</b>	Transmitir datos
<b>TxB</b>	Transmitir datos
<b>RxA</b>	Recibir datos
<b>RxB</b>	Recibir datos
<b>Sig Gnd</b>	Señal de toma de tierra

#### **Niveles de voltaje de las señales de EIA 422A de 16 puertos**

El controlador de la línea genera un voltaje distinto comprendido entre 2 y 6 voltios (medido en el punto de interfaz del generador). La magnitud del voltaje diferencial en el receptor debe estar comprendida entre 200 milivoltios y 6 voltios (medidos en el punto de interfaz de la carga).

Las medidas se realizan en el terminal A (conductor positivo) con respecto al terminal B (conductor negativo). La tabla siguiente describe los estados de señal con respecto a los niveles de voltaje:

Tabla 123. Estado de las señales de EIA 422A de 16 puertos

Voltaje de intercambio	Estado binario	Condición de la señal
Voltaje +	0	Espacio
Voltaje -	1	Marca

El adaptador asíncrono de 16 puertos EIA 422A proporciona soporte a un cableado de interior con una longitud de hasta 1200 m (4000 pies). Los cables de estas longitudes son susceptibles a sobrecargas de voltaje repentina debidas a voltajes inducidos como, por ejemplo, caídas de rayos indirectas. En el adaptador EIA 422A se ha implementado la circuitería de protección contra sobrecargas para protegerlo de estas sobrecargas de voltaje. La circuitería de protección contra sobrecargas se implementa en las líneas de datos de la interfaz del adaptador.

Se ha añadido circuitería con protección frente a fallos a los conductores de cada receptor EIA 422A para evitar condiciones de error cuando el receptor no está conectado a un controlador (cable abierto). La circuitería con protección frente a fallos establece el receptor en el estado de marca (1 binario) siempre que el receptor no está conectado a un controlador.

Las características eléctricas de los puertos del adaptador asíncrono de 16 puertos EIA 422A cumplen con el estándar EIA 422A con fecha de diciembre de 1978.

**Tabla de conversión de valores ASCII, decimales, hexadecimales, octales y binarios**

En esta tabla puede consultarse información útil para convertir valores ASCII, decimales, hexadecimales, octales y binarios.

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios

ASCII	Decimal	Hexadecimal	Octal	Binario
nulo	0	0	0	0
inicio de cabecera	1	1	1	1
inicio de texto	2	2	2	10
final de texto	3	3	3	11
final de transmisión	4	4	4	100
consulta	5	5	5	101
reconocimiento	6	6	6	110
avisador	7	7	7	111
retroceso	8	8	10	1000
tabulador horizontal	9	9	11	1001
avance de línea	10	A	12	1010
tabulador vertical	11	B	13	1011
avance de página	12	C	14	1100
retorno de carro	13	D	15	1101
desplazamiento a teclado ideográfico	14	E	16	1110
desplazamiento a teclado estándar	15	F	17	1111
escape de enlace de datos	16	10	20	10000
control de dispositivos 1/Xon	17	11	21	10001
control de dispositivos 2	18	12	22	10010
control de dispositivos 3/Xoff	19	13	23	10011
control de dispositivos 4	20	14	24	10100
reconocimiento negativo	21	15	25	10101
desocupado síncrono	22	16	26	10110
final de bloque de transmisión	23	17	27	10111

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
cancelar	24	18	30	11000
final del soporte de almacenamiento	25	19	31	11001
final del archivo / sustituir	26	1A	32	11010
escape	27	1B	33	11011
separador de archivos	28	1C	34	11100
separador de grupos	29	1D	35	11101
separador de registros	30	1E	36	11110
separador de unidades	31	1F	37	11111
espacio	32	20	40	100000
!	33	21	41	100001
"	34	22	42	100010
#	35	23	43	100011
\$	36	24	44	100100
%	37	25	45	100101
&	38	26	46	100110
'	39	27	47	100111
(	40	28	50	101000
)	41	29	51	101001
*	42	2A	52	101010
+	43	2B	53	101011
,	44	2C	54	101100
-	45	2D	55	101101
.	46	2E	56	101110
/	47	2F	57	101111
0	48	30	60	110000
1	49	31	61	110001
2	50	32	62	110010
3	51	33	63	110011
4	52	34	64	110100
5	53	35	65	110101

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
6	54	36	66	110110
7	55	37	67	110111
8	56	38	70	111000
9	57	39	71	111001
:	58	3A	72	111010
;	59	3B	73	111011
<	60	3C	74	111100
=	61	3D	75	111101
>	62	3E	76	111110
?	63	3F	77	111111
@	64	40	100	1000000
A	65	41	101	1000001
B	66	42	102	1000010
C	67	43	103	1000011
D	68	44	104	1000100
E	69	45	105	1000101
F	70	46	106	1000110
G	71	47	107	1000111
H	72	48	110	1001000
I	73	49	111	1001001
J	74	4A	112	1001010
K	75	4B	113	1001011
L	76	4C	114	1001100
M	77	4D	115	1001101
N	78	4E	116	1001110
O	79	4F	117	1001111
P	80	50	120	1010000
Q	81	51	121	1010001
R	82	52	122	1010010
S	83	53	123	1010011
T	84	54	124	1010100
U	85	55	125	1010101
V	86	56	126	1010110
W	87	57	127	1010111

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
X	88	58	130	1011000
Y	89	59	131	1011001
Z	90	5A	132	1011010
[	91	5B	133	1011011
\	92	5C	134	1011100
]	93	5D	135	1011101
^	94	5E	136	1011110
-	95	5F	137	1011111
`	96	60	140	1100000
a	97	61	141	1100001
b	98	62	142	1100010
c	99	63	143	1100011
d	100	64	144	1100100
e	101	65	145	1100101
f	102	66	146	1100110
g	103	67	147	1100111
h	104	68	150	1101000
i	105	69	151	1101001
j	106	6A	152	1101010
k	107	6B	153	1101011
l	108	6C	154	1101100
m	109	6D	155	1101101
n	110	6E	156	1101110
o	111	6F	157	1101111
p	112	70	160	1110000
q	113	71	161	1110001
r	114	72	162	1110010
s	115	73	163	1110011
t	116	74	164	1110100
u	117	75	165	1110101
v	118	76	166	1110110
w	119	77	167	1110111
x	120	78	170	1111000
y	121	79	171	1111001

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
z	122	7A	172	1111010
{	123	7B	173	1111011
	124	7C	174	1111100
}	125	7D	175	1111101
~	126	7E	176	1111110
SUPR	127	7F	177	1111111
	128	80	200	10000000
	129	81	201	10000001
	130	82	202	10000010
	131	83	203	10000011
	132	84	204	10000100
	133	85	205	10000101
	134	86	206	10000110
	135	87	207	10000111
	136	88	210	10001000
	137	89	211	10001001
	138	8A	212	10001010
	139	8B	213	10001011
	140	8C	214	10001100
	141	8D	215	10001101
	142	8E	216	10001110
	143	8F	217	10001111
	144	90	220	10010000
	145	91	221	10010001
	146	92	222	10010010
	147	93	223	10010011
	148	94	224	10010100
	149	95	225	10010101
	150	96	226	10010110
	151	97	227	10010111
	152	98	230	10011000
	153	99	231	10011001
	154	9A	232	10011010
	155	9B	233	10011011

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
	156	9C	234	10011100
	157	9D	235	10011101
	158	9E	236	10011110
	159	9F	237	10011111
	160	A0	240	10100000
	161	A1	241	10100001
	162	A2	242	10100010
	163	A3	243	10100011
	164	A4	244	10100100
	165	A5	245	10100101
	166	A6	246	10100110
	167	A7	247	10100111
	168	A8	250	10101000
	169	A9	251	10101001
	170	AA	252	10101010
	171	AB	253	10101011
	172	AC	254	10101100
	173	AD	255	10101101
	174	AE	256	10101110
	175	AF	257	10101111
	176	B0	260	10110000
	177	B1	261	10110001
	178	B2	262	10110010
	179	B3	263	10110011
	180	B4	264	10110100
	181	B5	265	10110101
	182	B6	266	10110110
	183	B7	267	10110111
	184	B8	270	10111000
	185	B9	271	10111001
	186	BA	272	10111010
	187	BB	273	10111011
	188	BC	274	10111100
	189	BD	275	10111101

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
	190	BE	276	10111110
	191	BF	277	10111111
	192	C0	300	11000000
	193	C1	301	11000001
	194	C2	302	11000010
	195	C3	303	11000011
	196	C4	304	11000100
	197	C5	305	11000101
	198	C6	306	11000110
	199	C7	307	11000111
	200	C8	310	11001000
	201	C9	311	11001001
	202	CA	312	11001010
	203	CB	313	11001011
	204	CC	314	11001100
	205	CD	315	11001101
	206	CE	316	11001110
	207	CF	317	11001111
	208	D0	320	11010000
	209	D1	321	11010001
	210	D2	322	11010010
	211	D3	323	11010011
	212	D4	324	11010100
	213	D5	325	11010101
	214	D6	326	11010110
	215	D7	327	11010111
	216	D8	330	11011000
	217	D9	331	11011001
	218	DA	332	11011010
	219	DB	333	11011011
	220	DC	334	11011100
	221	DD	335	11011101
	222	DE	336	11011110
	223	DF	337	11011111

Tabla 124. Conversiones entre valores ASCII, decimales, hexadecimales, octales y binarios  
(continuación)

<b>ASCII</b>	<b>Decimal</b>	<b>Hexadecimal</b>	<b>Octal</b>	<b>Binario</b>
	224	E0	340	11100000
	225	E1	341	11100001
	226	E2	342	11100010
	227	E3	343	11100011
	228	E4	344	11100100
	229	E5	345	11100101
	230	E6	346	11100110
	231	E7	347	11100111
	232	E8	350	11101000
	233	E9	351	11101001
	234	EA	352	11101010
	235	EB	353	11101011
	236	EC	354	11101100
	237	ED	355	11101101
	238	EE	356	11101110
	239	EF	357	11101111
	240	F0	360	11110000
	241	F1	361	11110001
	242	F2	362	11110010
	243	F3	363	11110011
	244	F4	364	11110100
	245	F5	365	11110101
	246	F6	366	11110110
	247	F7	367	11110111
	248	F8	370	11111000
	249	F9	371	11111001
	250	FA	372	11111010
	251	FB	373	11111011
	252	FC	374	11111100
	253	FD	375	11111101
	254	FE	376	11111110
	255	FF	377	11111111

## **uDAPL (user-level Direct Access Programming Library)**

---

**uDAPL** (user Direct Access Programming Library) es una infraestructura de acceso directo para que sea ejecutada en transportes que son compatibles con acceso directo a datos como InfiniBand, RNIC, etc.

DAT Collaborative especifica el **uDAPL API** <http://www.datcollaborative.org>.

El código base de uDAPL se transfiere desde Open Fabrics a AIX y actualmente se soporta en adaptadores GX++ HCA and 4X DDR Expansion card (CFFh) InfiniBand.

**uDAPL** versión 1.2 se soporta en AIX 6.1 con 6100-06 y en versiones posteriores. La imagen de instalación de **uDAPL** se envía en el paquete de ampliación como *udapl.rte*. Esta imagen incluye los archivos de cabecera DAT, ubicados bajo **/usr/include/dat**. La imagen de instalación también incluye dos bibliotecas, *libdat.a* y *libdapl.a*.

Las aplicaciones incluyen los archivos de cabecera DAT y el enlace con la biblioteca DAT (*libdat.a* in **/usr/include/dat**). La capa DAT determina las bibliotecas apropiadas subyacentes de transporte específico.

Un proveedor AIX **uDAPL** se registra con el registro DAT utilizando entradas *dat.conf*. El archivo */etc/dat.conf* se incluye con las entradas predeterminadas y tiene detalles sobre el formato de la entrada.

Por razones de depuración, las bibliotecas **uDAPL** soportan el rastreo de sistema de AIX. Los ID de enganche de rastreo del sistema **uDAPL** incluyen 5C3 (para sucesos DAPL), 5C4 (para sucesos de error), 5C7 (para sucesos DAT) y 5C8 (para sucesos de error DAT). El nivel inicial de rastreo se puede modificar utilizando las variables de entorno *DAT\_TRACE\_LEVEL* y *DAPL\_TRACE\_LEVEL* que pueden tomar los valores numéricos de 0 a 10. El número de sucesos y la cantidad de datos rastreados aumenta con el nivel y con los niveles de rastreo clave existentes

```
TRC_LVL_ERROR = 1,  
TRC_LVL_NORMAL = 3,  
TRC_LVL_DETAIL = 7
```

Otras características de capacidad de servicio estándar de AIX, como el registro de errores de AIX, pueden ser útiles para la determinación de problemas. Y las características de capacidad de servicio de la capa de transporte subyacente, como el mandato *ibstat* y el componente de rastreo Infiniband, son también útiles para el diagnóstico de problemas.

Las API DAT devuelven los códigos de retorno estándar que se pueden decodificar con la ayuda del archivo */usr/include/dat/dat\_error.h*. La explicación detallada de los códigos de retorno se ubica en la especificación **uDAPL** de DAT Collaborative.

[“Protocolo Internet a través de InfiniBand \(IPoIB\)” en la página 471](#)

### **API de uDAPL compatibles con AIX**

De las muchas API de **uDAPL** especificadas por DAT Collaborative, hay algunas que no son compatibles con AIX.

Estas son API no compatibles con las implementaciones de **uDAPL** comunes del sector y tampoco serán compatibles con AIX.

<b>Item</b>	<b>Descripción</b>
<code>dat_cr_handoff</code>	// In DAT 1.2
<code>dat_ep_create_wi</code>	// In DAT 1.2
<code>th_srq</code>	
<code>dat_ep_recv_quer</code>	// In DAT 1.2
<code>y</code>	
<code>dat_ep_set_water</code>	// In DAT 1.2
<code>mark</code>	
<code>dat_srq_create</code>	// In DAT 1.2

Item	Descripción
dat_srq_post_rec	// In DAT 1.2
v	
dat_srq_resize	// In DAT 1.2
dat_srq_set_lw	// In DAT 1.2
dat_srq_free	// In DAT 1.2
dat_srq_query	// In DAT 1.2

Las API adicionales que no son compatibles con AIX son,

- dat\_lmr\_sync\_rdma\_read
- dat\_lmr\_sync\_rdma\_write
- dat\_registry\_add\_provider
- dat\_registry\_add\_provider

Para todas las API no compatibles, AIX sigue los mecanismos específicos descritos en la especificación DAT para identificar su falta de compatibilidad. Estos incluyen valores de atributo (como max\_srq equaling zero) y códigos de retorno específicos (como DAT\_MODEL\_NOT\_SUPPORTED). Al ser coherente con la implementación del sector y la especificación DAT, DAT\_NOT\_IMPLEMENTED se puede devolver para una función que no es compatible.

La compatibilidad de API relacionadas con RMR como *dat\_rmr\_create*, *dat\_rmr\_bind*, *dat\_rmr\_free* y *dat\_rmr\_query* depende de la prestación subyacente HCA, y el buen funcionamiento o las anomalías las determina la infraestructura subyacente IB. En la actualidad, los adaptadores GX++ HCA and 4X DDR Expansion card (CFFh) InfiniBand no son compatibles con estas operaciones RMR.

[“uDAPL \(user-level Direct Access Programming Library\)” en la página 784](#)

[“Atributos específicos del proveedor para uDAPL” en la página 785](#)

[“Protocolo Internet a través de InfiniBand \(IPoIB\)” en la página 471](#)

## Atributos específicos del proveedor para uDAPL

Hay algunos atributos específicos del proveedor compatibles con AIX. Los nombres de los atributos son **delayed\_ack\_supported**, **vendor\_extension**, **vendor\_ext\_version**, **debug\_query** y **debug\_modify**.

### **delayed\_ack\_supported**

El proveedor de AIX para el transporte de InfiniBand (IB) incluye un atributo de adaptador de interfaz (IA)específica del proveedor denominado **delayed\_ack\_supported**. El valor de este atributo es **verdadero** o **falso**. Cuando es **verdadero**, los puntos finales asociados con este IA tienen un atributo específico del proveedor modificable denominado **delayed\_ack**. Cuando el atributo **delayed\_ack\_supported** es **falso**, un atributo **delayed\_ack** de punto final específico del proveedor no se puede modificar. El valor predeterminado de un atributo **delayed\_ack** de punto final es **falso**. Al definirlo como **verdadero** (a través de *dat\_ep\_modify*) se habilita la característica delayed ack del adaptador de canal de host (HCA) de IB subyacente para el par de cola específico de IB asociado con el punto final. Todos los HCA no implementan esta característica de hardware y por lo tanto no está disponible para todos los IA. Habilitar la característica hace que HCA se demore al enviar acuse de recibo hasta que una operación de transferencia de datos sea visible en la memoria del sistema de un servidor. Esta es un poco más semántica que lo que se proporciona en la especificación de IB, al coste potencial de un pequeño aumento de latencia.

### **vendor\_extension**, **vendor\_ext\_version**, **debug\_query** and **debug\_modify**

Por razones de depuración, las bibliotecas **uDAPL** soportan el rastreo de sistema de AIX. El nivel inicial de rastreo se puede modificar utilizando las variables de entorno *DAT\_TRACE\_LEVEL* y *DAPL\_TRACE\_LEVEL*. Para cambiar estos niveles de rastreo de forma dinámica a través de API, ofrecemos soporte de nivel de rastreo dinámico en AIX. Para verificar si la biblioteca tiene soporte de nivel de rastreo

dinámico, las aplicaciones pueden consultar el atributo de IA específico del proveedor, **vendor\_extension**. Al volver de la consulta, la presencia del atributo **vendor\_extension** indica soporte de nivel de rastreo dinámico. El valor del atributo se establece en **verdadero**; pero independientemente de eso, la presencia del atributo indica soporte. Cuando el atributo **vendor\_extension** está presente, las aplicaciones pueden obtener los punteros de función a **dat\_trclvl\_query()** y **dat\_trclvl\_modify()** consultando los atributos de IA específicos del proveedor, **debug\_query** y **debug\_modify**. El valor de estos atributos tendrá el puntero para las funciones correspondientes. Para que esta interfaz **vendor\_extension** se haga extensible para un uso futuro, tenemos otro atributo IA específico del proveedor, **vendor\_ext\_version**. Desde que solo vamos a soportar una versión, el valor de este atributo se establecerá en **1.0**. Si el atributo **vendor\_extension** no existe, las aplicaciones no pueden modificar los niveles de rastreo de forma dinámica.

Un ejemplo de como manipular estos atributos se incluye en el código de muestra **uDAPL** instalado con la implementación de AIX.

[“uDAPL \(user-level Direct Access Programming Library\)” en la página 784](#)

[“Protocolo Internet a través de InfiniBand \(IPoIB\)” en la página 471](#)

## Soporte para el adaptador RoCE PCIe2 de 10 GbE

En primera instancia, el sistema operativo AIX sólo daba soporte al adaptador PCIe2 10GbE RDMA como un dispositivo sólo disponible para el RDMA (Remote Direct Memory Access). El software de soporte fue un software propietario de IBM basado la pila de AIX InfiniBand. A este soporte se le conoció como AIX RoCE. AIX 7 con 7100-02 o superior da soporte a este adaptador en dos modalidades, que son AIX RoCE y el soporte 10G Ethernet también llamado tarjeta de interfaz de red (AIX NIC). El AIX 7 con 7100-03 nuevo ahora da soporte a RDMA junto con la modalidad NIC y OpenFabrics Enterprise Distribution (OFED). El adaptador de bus de host (HBA), que no estaba disponible en versiones anteriores de los sistemas operativos AIX, gestiona la modalidad en que se habilita.

La tabla siguiente muestra la evolución del software del adaptador PCIe2 10GbE:

Nivel de AIX	MODO 1	MODO 2
Antes AIX 7 con 7100-02	RoCE de AIX	ND
AIX 7 con 7100-02	RoCE de AIX	NIC de AIX
AIX 7 con 7100-03	RoCE de AIX	NIC + OFED RoCE de AIX

Para descargar los últimos controladores de dispositivo para este adaptador, lleve a cabo los pasos siguientes:

1. Vaya al [sitio web de IBM](#) ([www.ibm.com](http://www.ibm.com))
2. Pulse **Sopporte y descargas**.
3. Descargue el firmware más reciente a la ubicación del host de AIX (/etc/microcode)
4. Ejecute la herramienta **diag** para actualizar el firmware seleccionando uno de los procedimientos siguientes:
  - Procedimiento de vía de acceso corto
    - a. Entre el mandato siguiente:

```
*diag -d entX -T download
```

**Nota:** Sustituya **entX** por **roceX** si está utilizando la pila RoCE desde una versión anterior.

- b. Seleccione el microcódigo que se guarda en el directorio /etc/microcode.
- Procedimiento de vía de acceso largo
  - a. Entre el mandato siguiente:

```
*diag
```

b. Pulse:

**Selección de tareas > Tareas de microcódigo > Descargar microcódigo**

c. Seleccione **entX o roceX**.

d. Seleccione el microcódigo que se guarda en el directorio /etc/microcode.

De forma predeterminada, el adaptador está configurado para dar soporte al modo RoCE de AIX. Complete los pasos de la sección “[NIC + OFED RDMA de AIX](#)” en la página 787 para cambiarlo a otro modo.

## NIC + OFED RDMA de AIX

Como el AIX 7 con 7100-02, el adaptador PCIe2 10 GbE RoCE se puede configurar para que se ejecute en la configuración de AIX NIC. Como el AIX 7 con 7100-03, la funcionalidad OFED RDMA también se puede añadir a la configuración AIX NIC. Si no dispone de las aplicaciones que hacen un uso intensivo de la red que se benefician de RDMA, puede utilizar el adaptador en la configuración de NIC.

Para utilizar el adaptador PCIe2 10 GbE RoCE Adapter en la configuración AIX NIC + OFED RoCE o en la configuración AIX RoCE, los siguientes conjuntos de archivos son necesarios y están disponibles en el CD del sistema operativo base de AIX 7 con 7100-03.

### **devices.ethernet.mlx**

Controlador de dispositivos principal del adaptador Ethernet convergente (mlxentdd) para dar soporte a la configuración NIC + OFED RoCE de AIX.

### **devices.pciex.b315506b3157265**

Soporte de empaquetado para el ASIC2 del adaptador Ethernet convergente ITE NGP.

### **devices.pciex.b3155067b3157365**

Soporte de empaquetado para el ASIC1 del adaptador Ethernet convergente ITE NGP.

### **devices.pciex.b315506714101604**

Empaquetado para el adaptador Ethernet convergente Mellanox de 2 puertos de 10 GbE con los transceptores conectables del pequeño factor de formulario (SFP+).

### **devices.pciex.b3155067141016104**

Empaquetado para el adaptador Ethernet convergente Mellanox de 2 puertos de 10 GbE que da soporte a cualquier transceptor SFP+.

### **devices.common.IBM.ib**

Controlador de dispositivo ICM que es necesario para utilizar la configuración RoCE de AIX.

### **devices.pciex.b3154a63**

Controlador de dispositivo del adaptador Ethernet convergente Mellanox de 10 GbE que es necesario para utilizar la configuración RoCE de AIX.

### **ofed.core**

Catálogo de archivos OFED Core Runtime Environment necesario solo si se necesita la OFED RDMA.

Una vez que se actualicen los catálogos de archivos existentes RoCE de AIX con los nuevos catálogos de archivos, puede parecer que ambos dispositivos roce y ent estén configurados. Si ambos dispositivos parecen que están configurados al ejecutar el mandato **lsdev** en los adaptadores, lleve a cabo los pasos siguientes:

1. Suprima las instancias *roceX* relacionadas con el adaptador RoCE PCIe2 de 10 GbE especificando el mandato siguiente:

```
# rmdev -dl roce0[, roce1][, roce2,...]
```

2. Suprima las instancias *entX* relacionadas con el adaptador RoCE PCIe2 de 10 GbE especificando el mandato siguiente:

```
# rmdev -dl ent1[,ent2][, ent3...]
```

3. Si hay uno o varios adaptadores de bus de host convergentes (hbaX) relacionados con el adaptador RoCE PCIe2 de 10 GbE, suprimalos especificando el mandato siguiente:

```
# rmdev -dl hba0[, hba1][,hba2...]
```

4. Ejecute el gestor de configuración para incorporar los cambios escribiendo el mandato siguiente:

```
# cfgmgr
```

Complete los pasos siguientes para cambiar a la configuración NIC + OFED RoCE de AIX desde la configuración de RoCE de AIX:

1. Detenga todas las aplicaciones de RDMA que se ejecutan en el adaptador RoCE PCIe2 de 10 GbE.
2. Suprima o vuelva a definir las instancias *roceX* especificando uno de los mandatos siguientes:

- # rmdev -d -l roce0
- # rmdev -l roce0

El mandato `rmdev -l roce0` conserva la definición de la configuración de `roce0` para que pueda utilizarla la próxima vez para crear instancias.

3. Cambie el atributo del valor `hba stack_type` de `aix_ib` (RoCE de AIX) a `ofed` (NIC + OFED RoCE de AIX) especificando el mandato siguiente:

```
# chdev -l hba0 -a stack_type=ofed
```

4. Ejecute la herramienta del gestor de configuración para que el adaptador del bus de host pueda configurar el adaptador RoCE PCIe2 de 10 GbE como un adaptador NIC especificando el mandato siguiente:

```
# cfgmgr
```

5. Verifique que el adaptador se está ejecutando en la configuración de NIC especificando el mandato siguiente:

```
# lsdev -C -c adapter
```

El ejemplo siguiente muestra los resultados cuando se ejecuta el mandato `lsdev` en el adaptador cuando se configura en modalidad AIX NIC + OFED RoCE:

```
ent1 Available 00-00-01 PCIe2 10GbE RoCE Converged Network Adapter
ent2 Available 00-00-02 PCIe2 10GbE RoCE Converged Network Adapter
hba0 Available 00-00 PCIe2 10GbE RoCE Converged Host Bus Adapter (b315506714101604)
```

Figura 46. Salida de ejemplo del mandato `lsdev` en un adaptador con la configuración AIX NIC + OFED RoCE

Porqué como AIX 7 con 7100-03, AIX también da soporte a OFED RDMA en la modalidad AIX NIC, si OFED RDMA necesita habilitarse, es necesario completar los dos pasos siguientes:

1. Instale el paquete `ofed.core`.
2. Defina el modo RDMA en los dispositivos `ent1` y `ent2` mediante el mandato siguiente:

```
# chdev -l ent1 -a rdma=desired
# chdev -l ent2 -a rdma=desired
```

El modo RDMA se definirá antes de que las interficies de `en1` or `en2` se hayan configurado.

3. Puede inhabilitar el modo RDMA mediante el mandato siguiente:

```
# chdev -l ent1 -a rdma=disabled
# chdev -l ent2 -a rdma=disabled
```

## RoCE de AIX

El adaptador RoCE PCIe2 de 10 GbE está preconfigurado para que funcione en el modo de configuración RoCE de AIX. Una red que utiliza RDMA proporciona un mejor rendimiento que la modalidad NIC para aplicaciones que consumen mucha red. Esta modalidad es a menudo útil para almacenamiento de red o cálculo de alto rendimiento.

La configuración RoCE de AIX necesita el uso de bibliotecas o interficies como las siguientes:

- La Direct Access Programming Library (uDAPL), que utiliza el sistema de base de datos de DB2
- La Message Passing Interface (MPI), que utiliza el cálculo de alto rendimiento (HPC)

roce\_rdmaconfiguration.dita#roce\_rdmaconfiguration/figscreenrdma muestra la salida cuando el adaptador se está ejecutando en el modo RoCE de AIX.

El adaptador RoCE PCIe2 de 10 GbE sólo muestra una instancia de adaptador cuando está en el modo RoCE de AIX, pero puede tener hasta dos puertos. Utilice el mandato **ibstat** para determinar el número de puertos configurados completando los pasos siguientes:

1. Determine si la ampliación de kernel de **icm** está configurada especificando el mandato siguiente:

```
# lsdev -C | grep icm
```

2. Si el kernel **icm** no está configurado, configúrelo especificando el mandato siguiente:

```
# mkdev -c management -s infiniband -t icm
```

3. Ejecute el mandato **ibstat** especificando el mandato siguiente:

```
# ibstat roce0
```

Mientras que el adaptador RoCE PCIe2 de 10 GbE está configurado inicialmente para utilizar el modo RoCE de AIX, puede que necesite cambiar de nuevo desde la configuración NIC + OFED RoCE de AIX. Para cambiar desde la configuración NIC + OFED RoCE de AIX a la configuración RoCE de AIX, lleve a cabo los pasos siguientes:

1. Verifique que el adaptador está en modo NIC + OFED RoCE de AIX especificando el mandato siguiente:

```
# lsdev -C -c adapter
```

El resultado del mandato **lsdev** es similar al ejemplo del roce\_nicconfiguration.dita#roce\_nicconfiguration/figscreennic.

2. Detenga el tráfico TCP/IP y desconecte las interfaces IP escribiendo el mandato siguiente:

```
# ifconfig en1 down detach; ifconfig en2 down detach
```

3. Suprima o ponga las instancias de NIC en un estado definido emitiendo uno de los mandatos siguientes:

- # rmdev -d -l ent1; rmdev -d -l ent2
- # rmdev -l ent1; rmdev -l ent2

El mandato **rmdev -l ent1; rmdev -l ent2** conserva la definición de los dispositivos Ethernet para que pueda utilizarla la próxima vez que cree instancias.

4. Cambie el atributo de hba stack\_type desde ofed (NIC + OFED RoCE de AIX) a aix\_ib (RoCE AIX) mediante el mandato siguiente:

```
# chdev -l hba0 -a stack_type=aix_ib
```

5. Ejecute la herramienta del gestor de configuración para que el adaptador de bus de host pueda configurar el adaptador RoCE PCIe2 de 10 GbE como un adaptador RoCE de AIX especificando el mandato siguiente:

```
# cfgmgr
```

6. Verifique que el adaptador se está ejecutando en la configuración de RoCE de AIX especificando el mandato siguiente:

```
# lsdev -C -c adapter
```

El ejemplo siguiente muestra los resultados al ejecutar el mandato **lsdev** para los adaptadores, y el adaptador está configurado en el modo RoCE de AIX.

```
roce0 Available 00-00-00 PCIe2 10GbE RoCE Converged Network Adapter  
hba0 Available 00-00-00 PCIe2 10GbE RoCE Converged Host Bus Adapter (b315506714101604)
```

*Figura 47. Resultado de ejemplo del mandato **lsdev** para los adaptadores cuando se está utilizando la configuración de RoCE de AIX*

## Sopporte al adaptador RoCE PCIe3 40 GbE

El adaptador PCIe3 40 GbE RDMA Over Converged Ethernet (RoCE) da soporte al RDMA (Remote Direct Memory Access) con OpenFabrics Enterprise Distribution (OFED) en el modo normal de NIC. Se admitirá y se habilitará el RDMA si el software de OpenFabrics está instalado.

Para descargar los últimos controladores de dispositivo para este adaptador, lleve a cabo los pasos siguientes:

1. Vaya al [sitio web de IBM](http://www.ibm.com) ([www.ibm.com](http://www.ibm.com)).
2. Pulse **Soporte y descargas**.
3. Descargue el firmware más reciente a la ubicación del host de AIX (/etc/microcode).
4. Ejecute la herramienta **diag** para actualizar el firmware seleccionando uno de los procedimientos siguientes:

- Procedimiento de vía de acceso corto

- a. Entre el mandato siguiente:

```
*diag -d entX -T download
```

**Nota:** Si el dispositivo Ethernet pertenece al mismo adaptador de bus de host (por ejemplo hba0, hba1 y así sucesivamente), descargue el firmware de uno de los dispositivos **ent**.

- b. Seleccione el microcódigo que se guarda en el directorio /etc/microcode.

- Procedimiento de vía de acceso largo

- a. Entre el mandato siguiente:

```
*diag
```

- b. Haga clic en

**Selección de tareas > Tareas de microcódigo > Descargar microcódigo**

.

- c. Seleccione **entX**.

- d. Seleccione el microcódigo que se guarda en el directorio /etc/microcode.

Para utilizar el adaptador RoCE PCIe3 40 GbE RoCE y el NIC + OFED RoCE de AIX, se necesitan los siguientes catálogos de archivos. Éstos están disponibles en el CD del sistema operativo base de AIX 7 con 7100-03.

devices.ethernetmlx	Controlador de dispositivos principal del adaptador Ethernet convergente (mlxentdd) para dar soporte a la configuración NIC + OFED RoCE de AIX.
devices.pciex.b31503101410b504	Paquete para el adaptador Mellanox 2 Ports 40 Gb Converged Ethernet que utiliza los puertos de cobre pasivos Quad Small Form-factor Pluggable (QSFP).
ofed.core	Catálogo de archivos OFED Core Runtime Environment necesario solo si se necesita la función OFED RDMA.

Para inhabilitar la función RDMA, introduzca el mandato siguiente:

```
chdev -l <Ethernet_device> rdma=disabled
```

Por ejemplo:

```
# chdev -l ent1 -a rdma=disabled
# chdev -l ent2 -a rdma=disabled
```

Para habilitar la función RDMA, introduzca el mandato siguiente:

```
chdev -l <Ethernet_device> rdma=desired
```



## Avisos

---

Esta información ha sido desarrollada para productos y servicios ofrecidos en EE.UU.

Es posible que IBM no ofrezca los productos, servicios o características que se tratan en este documento en otros países. Póngase en contacto con el representante de IBM local para obtener información sobre los servicios y productos actualmente disponibles en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que sólo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio equivalente que no vulnere los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

Puede que IBM tenga patentes o solicitudes de patente pendientes que cubran la materia descrita en este documento. La posesión de este documento no le otorga ninguna licencia sobre tales patentes.

Puede enviar consultas sobre licencias, por escrito, a:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
EE.UU.*

Para realizar consultas sobre licencias relacionadas con información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

*Intellectual Property Licensing  
Legal  
and Intellectual Property Law IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokio 103-8510, Japón*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCTAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCTAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunas jurisdicciones no permiten el rechazo de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que esta declaración no se aplique al usuario.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Se realizan cambios periódicos en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM podría realizar mejorar y/o cambios en los productos y/o los programas descritos en esta publicación en cualquier momento, sin previo aviso.

Cualquier referencia en este documento a sitios web que no son de IBM se proporciona únicamente para su comodidad y no significa en modo alguno que se recomiende dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales para este producto de IBM y el uso de dichos sitios web corre a cuenta y riesgo del Cliente.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el remitente.

Los titulares de licencias de este programa que deseen tener información sobre el mismo con el fin de: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deberán ponerse en contacto con:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
EE.UU.*

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, y puede incluir en algunos casos el pago de una tarifa.

IBM proporciona el programa bajo licencia que se describe en esta información y todo el material bajo licencia disponible bajo los términos del acuerdo IBM Customer Agreement, IBM International Program License Agreement o de cualquier acuerdo equivalente entre las partes.

Los ejemplos de cliente y datos de rendimiento citados, se presentan sólo con propósitos ilustrativos. Los resultados reales de rendimiento pueden variar dependiendo de las condiciones operativas y las configuraciones específicas.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, sus anuncios publicados u otras fuentes de información disponibles a nivel público. IBM no ha comprobado estos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni cualquier otra reclamación relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de productos que no son de IBM deben dirigirse a los proveedores de dichos productos.

Las declaraciones a respecto de futuras direcciones e intenciones de IBM están sujetas a cambio o cancelación sin previa notificación y representan solamente metas y objetivos.

Todos los precios de IBM que se muestran son precios de distribución sugeridos por IBM, son actuales y están sujetos a modificaciones sin previo aviso. Los precios del distribuidor pueden variar.

Esta información está pensada a efectos de planificación. La información aquí contenida está sujeta a cambios antes de que los productos que se describen estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de particulares, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con personas o empresas comerciales es pura coincidencia.

#### LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran las técnicas de programación en distintas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo en cualquier formato sin necesidad de efectuar ningún pago a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la cual se han escrito los programas de aplicación. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni implicar la fiabilidad, servicio o funcionamiento de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantía de ningún tipo. IBM no se hará responsable de los daños que surjan por el uso de los programas de ejemplo.

Todas las copias o fragmentos de las copias de estos programas de ejemplo o cualquier trabajo que de ellos se derive, deberán incluir un aviso de copyright como el que se indica a continuación:

© (nombre de su empresa) (año).

Partes de este código derivan de programas de ejemplo de IBM Corp. Sample Programs.

© Copyright IBM Corp. \_especificar el año o años\_.

## Consideraciones de la política de privacidad

---

Los productos de software de IBM, que incluyen el software como soluciones de servicios, ("Ofertas de software") pueden utilizar cookies u otras tecnologías para recopilar información de uso de producto y así mejorar la experiencia del usuario final y adaptar las interacciones con el usuario final o para otros fines.

En la mayoría de los casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software le ayudan a recopilar dicha información. En caso de que una Oferta de software utilice cookies para recopilar información de identificación personal, se detalla a continuación información específica sobre el uso que hace de las cookies esta oferta.

Esta Oferta de software no utiliza cookies ni otras tecnologías para recopilar información de identificación personal.

Si las configuraciones implementadas para esta Oferta de software le ofrece como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnología, debería buscar asesoramiento jurídico sobre las leyes aplicables con respecto a la recopilación de datos así como tener noción de los requisitos expresos de notificación y consentimiento.

Si desea obtener más información sobre el uso de varias tecnologías, incluyendo el uso de las cookies para la recopilación de datos, consulte la Política de privacidad de IBM en <http://www.ibm.com/privacy> y las declaraciones de privacidad en línea de IBM en <http://www.ibm.com/privacy/details>, la sección denominada "Cookies, balizas de web y otras tecnologías" y la "Declaración de privacidad de productos software y ofertas de Software-as-a-Service (SaaS) de IBM" en <http://www.ibm.com/software/info/product-privacy>.

## Marcas registradas

---

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Puede que otros productos o nombres de servicio sean marcas registradas de IBM u otras compañías. Se encuentra disponible una lista de las marcas registradas de IBM en el sitio web en [Copyright and trademark information](#) en [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

INFINIBAND, InfiniBand Trade Association y el logotipo de INFINIBAND son marcas registradas y/o marcas de servicio de INFINIBAND Trade Association.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas o marcas comerciales registradas de Intel Corporation o de sus filiales en Estados Unidos y/o en otros países.

La marca registrada Linux® se utiliza conforme a una sublicencia de The Linux Foundation, el licenciatario exclusivo de Linus Torvalds, propietario de la marca en todo el mundo.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas y logotipos registrados de Java son marcas registradas o marcas comerciales registradas de Oracle y/o sus empresas afiliadas.

UNIX es una marca registrada de The Open Group en Estados Unidos y/o en otros países.



# Índice

## Caracteres Especiales

-, submandato [16](#)  
! submandato [43](#), [45](#)  
? mandato [34](#)  
. submandato [29](#), [44](#)  
.3270keys, archivo [114](#)  
.forward, archivo [31](#)–[33](#)  
.k5login, archivo [116](#)  
.mailrc, archivo [11](#), [35](#)–[41](#)  
.netrc, archivo [114](#)  
.vacation.dir, archivo [33](#)  
.vacation.msg, archivo [33](#)  
.vacation.pag, archivo [33](#)  
/etc/aliases [7](#)  
/etc/clsnmp.conf [558](#), [562](#), [565](#)  
/etc/gateways [440](#)  
/etc/hosts [108](#)  
/etc/mail/aliases [46](#)  
/etc/mail/sendmail.cf [55](#)  
/etc/mail/statistics [55](#)  
/etc/named.ca [192](#)  
/etc/named.data [192](#)  
/etc/named.local [192](#)  
/etc/named.rev [192](#)  
/etc/netsvc.conf [47](#)  
/etc/protocols [169](#)  
/etc/rc.net [109](#)  
/etc/rc.tcpip [45](#), [431](#)  
/etc/sendmail.cf  
    TCP/IP [189](#)  
/etc/services [169](#)  
/etc/snmpd.conf [562](#), [571](#), [572](#)  
/etc/snmpdv3.conf [558](#), [562](#), [565](#)  
/tmp/traffic [54](#)  
/usr/bin/bellmail [105](#)  
/usr/bin/mail [105](#)  
/usr/bin/Mail [105](#)  
/usr/bin/mailx [105](#)  
/usr/bin/rmail [105](#)  
/usr/lib/sendmail.cf [201](#)  
/usr/lib/uucp/Devices [714](#)  
/usr/share/lib/Mail.rc [105](#)  
/usr/share/lib/Mail.rc, archivo [35](#), [36](#), [40](#)  
/var/spool/mail [105](#)  
/var/spool/mqueue [48](#), [105](#)  
+, submandato [16](#)  
=, submandato [15](#)  
~:, submandato [44](#)  
~!, submandato [29](#), [44](#)  
~? submandato [34](#)  
~[option] nombres de vía de acceso [534](#)  
~b, submandato [28](#)  
~c, submandato [28](#)  
~d, submandato [27](#), [44](#)  
~e, submandato [25](#), [42](#), [44](#)  
~f, submandato [26](#), [31](#), [32](#), [44](#)

~h, submandato [27](#)  
~m, submandato [26](#), [31](#), [32](#), [44](#)  
~p, submandato [25](#), [44](#)  
~q, submandato [25](#), [44](#)  
~r, submandato [26](#), [44](#)  
~s, submandato [28](#)  
~t, submandato [28](#)  
~v, submandato [25](#), [42](#), [44](#)  
~w, submandato [44](#)  
\$HOME/.mailrc [105](#)  
\$HOME/mboxc [105](#)  
óptica serie [176](#)

## Números

802.3 [175](#)  
802.3ad [449](#)

## A

a, submandato [37](#), [44](#)  
ACL (lista de control de accesos)  
    NFS, soporte [593](#)  
adaptador  
    16 puertos  
        descripción de EIA 422A [771](#)  
        información sobre el hardware [772](#)  
        instalación [771](#)  
        lógica de interrupción [773](#)  
        prioridad de la placa del adaptador [773](#)  
        señal de la interfaz EIA 232 [774](#)  
        señal de la interfaz EIA 422A [775](#)  
    8 puertos  
        información sobre el hardware [765](#)  
        lógica de control [770](#)  
        lógica de interrupción [767](#)  
        señal de la interfaz EIA 232 [769](#)  
        señal de la interfaz EIA 422A [769](#)  
        señal de la interfaz MIL-STD 188 [767](#)  
        aplicación [663](#)  
        conectado a nativo [661](#)  
        conectado a nodo [662](#)  
        conexión directa [661](#)  
        ISA de 8 puertos  
            configurar [763](#)  
adaptador con conexión directa [661](#)  
adaptador conectado a nativo [661](#)  
adaptador conectado a nodo [662](#)  
adaptadores  
    Adaptadores PCI  
        ARTIC960Hx [759](#)  
        EtherChannel [449](#)  
        IEEE 802.3ad [449](#)  
        multiprotocolo de 2 puertos [758](#)  
        pci  
            red de área amplia [758](#)  
    Adaptadores PCI

**Adaptadores PCI (continuación)**  
 ARTIC960Hx [759](#)  
**Address Resolution Protocol (Protocolo de resolución de direcciones)** [150](#)  
 Agregación de enlaces [449](#)  
 Agregación de enlaces IEEE 802.3ad  
     gestión  
     eliminación [463](#)  
**alias**  
     crear [37](#)  
     listar [37](#)  
**alias, correo** [46](#)  
**alias, submandato** [37](#)  
**almacenar**  
     correo en carpetas [17](#)  
     mail [11](#)  
**alter, submandato** [726, 727](#)  
**añadir a cabecera, submandatos** [44](#)  
**añadir a mensaje, submandatos** [44](#)  
**añadir usuarios a campos de cabecera** [28](#)  
**Archivo /etc/exports** [599](#)  
**Archivo /etc/xtab** [600](#)  
**archivo ate.def**  
     edición [737](#)  
     formato de archivo [739](#)  
**archivos**  
     .3270keys [114, 115](#)  
     .forward [31–33](#)  
     .k5login [116](#)  
     .mailrc [11, 35–41](#)  
     .netrc [114](#)  
     .vacation.dir [33](#)  
     .vacation.msg [33](#)  
     .vacation.pag [33](#)  
     /usr/share/lib/Mail.rc [35, 36, 40](#)  
     ASCII a binario [540, 541](#)  
     ate.def [726, 727, 737](#)  
     binario a ASCII [540, 541](#)  
     codificar [540, 541](#)  
     copiar de sistema principal local en sistema principal remoto [123](#)  
     copiar de sistema principal remoto en sistema principal local [122](#)  
     dead.letter [11](#)  
     decodificar [540, 541](#)  
     enviar [540](#)  
      impresión [125, 544](#)  
     intercambio [539](#)  
     mbox [11](#)  
     recepción [541](#)  
     transferencia [121](#)  
     vacation.def [33](#)  
**Archivos**  
     /etc/mail/sendmail.cf [55](#)  
     /etc/mail/statistics [55](#)  
     /tmp/traffic [54](#)  
     /var/spool/mqueue/log [53](#)  
**archivos de anotaciones cronológicas**  
     BNU [531](#)  
**Archivos NFS**  
     lista de [647](#)  
**archivos TCP/IP**  
     copiar de sistema principal local en sistema principal remoto [123, 124](#)  
**archivos TCP/IP (continuación)**  
     copiar de sistema principal remoto en sistema principal local [122, 124](#)  
**Archivos y directorios**  
     /usr/bin/bellmail [105](#)  
     /usr/bin/mail [105](#)  
     /usr/bin/Mail [105](#)  
     /usr/bin/mailx [105](#)  
     /usr/bin/rmail [105](#)  
     /usr/share/lib/Mail.rc [105](#)  
     /var/spool/mail [105](#)  
     /var/spool/mqueue [105](#)  
     \$HOME/.mailrc [105](#)  
     \$HOME/mbox [105](#)  
 ARTIC960Hx [759](#)  
**asignación dinámica de pantallas** [742](#)  
**asíncrona**  
     opciones [660](#)  
**asíncrona, comunicación** [667](#)  
**asinfo, archivo** [742](#)  
**ask, opción** [37](#)  
**askcc, opción** [37](#)  
**asynchronous terminal emulation**  
     Connected Main Menu [727](#)  
     directorio de marcación [733](#)  
     editar archivo predeterminado [737](#)  
     inicio [726](#)  
     lista de formatos de archivo [739](#)  
     lista de mandatos [738](#)  
     secuencias de teclas de control [727](#)  
     Unconnected Main Menu [726](#)  
**ATE**  
     configuración [725](#)  
     Connected Main Menu [727](#)  
     directorio de marcación [733](#)  
     editar archivo predeterminado [737](#)  
     inicio [726](#)  
     lista de formatos de archivo [739](#)  
     lista de mandatos [738](#)  
     marcación [735](#)  
     personalizar [728](#)  
     recepción de un archivo [736](#)  
     resolución de problemas [737](#)  
     secuencias de teclas de control [727](#)  
     transferencia de un archivo [736](#)  
     Unconnected Main Menu [726](#)  
     visión general [724](#)  
**ate, mandato** [726, 738](#)  
**ate.def**  
     archivo de configuración [729](#)  
     parámetros [729](#)  
**automount, daemon**  
     NFS (Network File System - Sistema de archivos de red)  
         sistemas de archivos [624](#)  
**autoprint, opción** [41](#)  
**avisos de mensaje de ausencia por vacaciones** [33](#)  
**ayuda, correo** [34](#)

## B

**bcc, campo** [28](#)  
**Bellmail** [7](#)  
**bibliotecas**

**bibliotecas (continuación)**  
 libauthm.a [113](#)  
 libvaliduser.a [113](#)  
**binarias, opciones de correo** [36](#)  
**BINLD** [390](#)  
**BNU**

- cancelación de trabajos remotos [547](#)
- cola de trabajos [541](#)
- comunicación entre locales y remotos [538](#)
- estado de intercambios [541](#)
- estado de operaciones [542](#)
- identificar sistemas compatibles [545](#)
- imprimir archivos [544](#)
- intercambiar mandatos [542](#)
- intercambio de archivos [539](#)
- marcar hasta establecer una conexión [539](#)
- marcar varios números [539](#)
- nombre\_sistema!, nombres de vía de acceso [534](#)
- nombre\_sistema!nombre\_sistema!, nombres de vía de acceso [534](#)
- nombres de vía de acceso [533](#)
- nombres de vía de acceso relativos [534](#)
- nombres de vías de acceso completos [533](#)
- ~[option] nombres de vía de acceso [534](#)
- sistemas conectados [541](#)
- TCP/IP [107](#)
- visión general [513](#)

**BNU (Basic Networking Utilities - Programas de utilidad básicos de red)**

- anomalías de inicio de sesión
- depuración [551](#)
- archivos de anotaciones cronológicas [531](#)
- conexión [537](#)
- daemons

  - visión general [534](#)

- ID de inicio de sesión de administración [537](#)
- mantenimiento [530](#)
- procedimientos del shell [533](#)
- seguridad [536](#)
- sistemas remotos

  - transporte de archivos a [535](#)

- sondeo

  - sistemas remotos [521](#)

- supervisión

  - automática [521](#)
  - conexión remota [543](#)
  - configuración [521](#)
  - transferencia de archivos [544](#)

**TCP/IP** [536](#)

- tip, mandato

  - variables [545](#)

- transferencia de archivos

  - planificación [535](#)
  - supervisión [544](#)

**BNU, archivos**

- administrativos [516](#)
- archivos de bloqueo [516](#)
- archivos de dispositivos

  - Conexiones físicas [522](#)
  - conexiones mediante autodialers [523](#)

- TCP/IP [524](#)
- configuración [514](#)
- estructura [514](#)
- permissions [538](#)

**BNU, archivos (continuación)**

- remote.unknown, archivo [537](#)
- supervisión de transferencia [544](#)
- systems, archivos [537](#)

**BNU, directorios**

- administrativos [516](#)
- directorio público [514](#)
- estructura [514](#)
- ocultos [516](#)
- spooling [516](#)

**break, submandato** [727, 738](#)
**bterm, mandato** [5](#)
**buzón**

- sistema [11](#)
- submandatos [43](#)

**buzón del sistema** [11](#)
**buzón personal** [11](#)
**buzón secreto**

- submandatos [45](#)

## C

**CacheFS**

- sistema de archivos de antememoria [594](#)

**cambiar a otro buzón** [20](#)
**cambio de mensaje, submandatos** [44](#)
**campo cc** [28](#)
**campo subject** [28](#)
**campos**

- bcc [27, 28](#)
- cabecera [27](#)
- cc [27, 28](#)
- subject [27, 28](#)
- to [27, 28](#)

**campos de cabecera**

- añadir a [27](#)
- cambiar [27](#)
- listar ignorados [40](#)
- listar retenidos [41](#)
- restablecer [40](#)

**cancelar**

- correo reenviado [32](#)
- mensajes de vacaciones [33](#)
- trabajos remotos [547](#)

**CAPTURE\_KEY, secuencia de teclas de control** [727](#)
**cd, mandato** [121, 122](#)
**cd, submandato** [43](#)
**chauthent, mandato** [113](#)
**chmod, mandato** [114](#)
**CIO (Concurrent Input/Output - Entrada/Salida simultánea)** [605](#)
**client** [108](#)
**clsnmp** [561](#)
**comprobar número de mensajes del buzón** [15](#)
**comprobar ortografía de correo** [29](#)
**comunicación**

- asíncrona [667](#)
- métodos [670](#)
- parámetros [668](#)
- serie [665](#)
- síncrona [666](#)

**comunicar**

- entre sistemas locales y remotos [538](#)
- por cable o módem [538](#)

comunicar (*continuación*)  
    por módem 539  
    utilizar BNU 538  
        utilizar Programas de utilidad básicos de red 538  
con un valor, opciones de correo 36  
Conceptos de red 1  
conexión  
    BNU 537  
    UUCP 536  
conexión de administración  
    BNU 537  
conexiones de sistema principal  
    local a remoto 116  
        telnet, tn o tn3270, mandato 116  
conexiones directas  
    configuración de BNU  
        ejemplo 529  
Conexiones físicas  
    archivos de dispositivos para 522  
conexiones mediante autodialers  
    archivos de dispositivos 523  
conexiones remotas  
    BNU  
        supervisión 543  
configuración  
    DCE 114  
    nativa 114  
    TCP/IP 109  
configuración de BNU  
    archivos 514  
    general 517  
configuración de los módems  
    automatizada 713  
configuración estática 143  
configuración estática de tiempo de ejecución 143  
configurar  
    ate.def 729  
    EIA 232 764  
    ISA de 8 puertos 763  
connect, submandato 726, 727, 738  
consideraciones sobre los módems 711  
control de enlace de datos (DLC)  
    entorno del gestor de dispositivos  
        componentes 749  
        estructura 749  
    genérico 749  
control de flujo 670  
control genérico de enlace de datos 749  
control, submandatos 43, 44  
Controlador Serial over Ethernet 745  
Controlador SoE 745  
conversación en tiempo real 120  
Correo  
    alias 46  
    archivo de registro cronológico, gestionar 54  
    archivos  
        /etc/mail/aliases 46  
        /etc/mail/sendmail.cf 55  
        /etc/mail/statistics 55  
        /etc/netsvc.conf 47  
        /var/spool/mqueue 48  
        /var/spool/mqueue/log 53  
    archivos y directorios, lista de 105  
    base de datos de alias 47

Correo (*continuación*)  
cola  
    archivos 48  
    determinar intervalos de proceso 51  
    especificar intervalos de proceso 51  
    forzado 51  
    gestión 48  
        impresión 48  
depuración 100  
estadísticas  
    estadísticas 55  
filtrar 55  
IMAP (Internet Message Access Protocol) 101  
instalación 7  
interfaces de usuario 7  
mandatos  
    mailq 48  
mandatos, lista de  
    IMAP y POP 107  
POP (Post Office Protocol) 101  
programa de direccionamiento de mensajes 7  
programas de acceso a mensajes 101  
programas de correo  
    bellmail 7  
    BNU 7  
        SMTP (Simple Mail Transfer Protocol - Protocolo simple de transferencia de correo) 7  
registro 53  
tareas de gestión 45  
tráfico, registro cronológico 54  
visión general de gestión del sistema 7  
correo secreto  
    enviar y recibir 33  
    submandatos 45  
correo, cabeceras  
    control de la visualización 40  
crear  
    .forward, archivo 32  
    .netrc, archivo 114  
    alias 37  
    carpetas predeterminadas 41  
    correo secreto 33  
    listas de distribución 37  
    mail 20  
    mensaje nuevo 31  
criterios para la selección de un producto 662  
crt, opción 38  
ct, mandato 538, 539  
cu, mandato  
    utilización de la programación manual del módem 712  
cuenta de saltos 434  
cuestionario  
    SLIP 722  
cumplimiento de los estándares 768, 774

## D

d, submandato 16, 41, 43, 45  
Daemon de capa de negociación de imagen de arranque (Boot Image Negotiation Layer daemon - BINLD) 390  
Daemon portmap  
    NFS (Network File System - Sistema de archivos de red) 601  
daemon talkd 120

Daemon uucpd 536  
Daemon uusched 535  
daemons  
    NFS seguro 649  
    servicios de red 649  
    SRC 602  
    talkd 120  
    TCP/IP 431  
    uucico 542, 545  
    uutx 542  
    uuxqt 542  
Daemons  
    sendmail  
        detener 53  
        inicio 52  
    syslogd 53  
DCE, configuración 114  
DDN 443  
dead.letter, archivo  
    guardar el mensaje en 25  
    recuperación y adición 27  
depuración  
    BNU  
        anomalías de inicio de sesión 551  
desactivación temporal de SLIP 717  
Descubrimiento de MTU de vía de acceso 486  
deshacer la supresión de mensajes 17  
desplazarse por el buzón 14  
devolución de llamada xxfi\_abort 94  
DIO (Entrada/Salida directa) 605  
Dirección IP virtual (VIPA) 446  
direcccionadores  
    TCP/IP 434  
direccionar  
    TCP/IP 433  
direcccionar correo  
    a más de un usuario 21  
    a través de un enlace BNU o UUCP 22  
    a usuarios de la red 21  
    a usuarios de una red diferente 22  
    a usuarios del sistema local 21  
direcciones  
    TCP/IP 179  
directorio de marcación  
    ATE 733  
    formato de archivo 739  
directorio público  
    BNU 514  
directorios  
    estructura en BNU 514  
directorios ocultos  
    BNU 516  
directory, submandato 726, 738  
disciplina de línea 672  
DLC (control de enlace de datos) 749  
DNS (Servicio de nombres de dominio) 184  
dp, submandato 16  
dt, submandato 16  
DTR/DSR  
    definición 671  
duplicación NFS  
    espacio de nombres global 606

## E

e, editor 42  
e, submandato 24, 25, 43  
editar información de cabecera 27  
editor de correo  
    comprobación ortográfica 29  
    editar un mensaje 24  
    iniciar desde el indicador del buzón 24  
    iniciar desde la línea de mandatos 24  
    inicio 24  
    reformatear un mensaje 28  
    salida 25  
    salir sin guardar 25  
    seleccionar un editor 42  
    submandatos 44  
    visualizar líneas de un mensaje 25  
    visualizar un mensaje 25  
editor, opción 42  
editores  
    e 42  
    vi 24, 42  
EIA 232  
    descripción 765  
    señal de la interfaz 769, 774  
EIA 422A  
    señal de la interfaz 769, 775  
ejemplos  
    clientes 664  
ejemplos de BNU  
    conexión directa 529  
    conexión por módem 526–528  
    conexión TCP/IP 524  
ejemplos de clientes 664  
emulación  
    aplicaciones 5  
emulación de sistema principal 5  
emuladores  
    impresora 5  
    modalidad bidireccional 5  
    terminal 5  
emuladores de impresora 5  
emuladores de terminal 5  
enlace  
    NFS (Network File System - Sistema de archivos de red)  
        598  
enlaces  
    prueba 754  
    rastreo 754  
enq, mandato 125, 126, 511  
enroll, mandato 33  
enviar  
    archivos 540  
    correo secreto 33  
    mail 20, 29  
EOT, submandato 44  
equipo de terminal de datos 4  
ESCDELAY 502  
escribir macros ftp 115  
estación de enlace 754  
estadísticas  
    consulta  
        SAP 755  
estado

estado (*continuación*)  
de intercambios de mandatos y archivos 541  
de la cola de trabajos BNU 541  
de operaciones BNU 542  
de sistemas conectados mediante BNU 541  
mail 12  
mandato 124  
estándar EIA 232D 669  
EtherChannel  
    configurar 451  
    gestión  
        eliminación 463  
        listado de EtherChannels 460  
        modificación de adaptadores 461  
        modificación de la dirección alternativa 460  
    modalidad a prueba de fallos sin pérdidas 454  
    recuperación automática 455  
    recuperación sin pérdidas 454  
    recuperación tras error forzada 455  
    resolución de problemas 470  
Ethernet Versión 2 174  
ex, submandato 17  
exportar  
    NFS (Network File System - Sistema de archivos de red)  
    592  
exports, archivo 599  
extensión de kernel  
    NFS 647

## F

f, mandato 127, 511  
f, submandato 14, 43  
file, submandato 20  
finger, mandato 127, 128, 511  
fmt, mandato 28  
folder, opción 41  
folder, submandato 15, 19, 20, 43  
formatos de archivo  
    ate.def 739  
    directorio de marcación 739  
ftp, mandato 112, 113, 121–123, 510  
Funciones constantes 98  
Funciones de control de la biblioteca 57  
Funciones de devolución de llamada 83  
Funciones de manejo de mensajes 81  
Funciones de modificación del mensaje 71  
Funciones del acceso de datos 65  
Funciones varias 98

## G

GDLC (control genérico de enlace de datos)  
    controles  
        instalación 752  
    criterios 751  
    interfaz  
        implementación 751  
    operaciones ioctl 752  
    servicios del kernel 755  
    visión general 749  
gestión de dispositivos de TTY 672  
Gestión de red 552

gestor de bloqueos de red 635  
get\_auth\_methods, subrutina 113  
get, submandato 124  
guardar  
    mensajes con cabeceras 18  
    mensajes sin cabeceras 19

## H

h, submandato 13, 38, 43  
habilitar opciones de correo 36  
hebras biod 602  
help, submandato 726, 727, 738  
host, mandato 127, 511

## I

identificar sistemas compatibles 545  
idiomas nacionales  
    BNU, soporte 514  
IEEE 802.3ad  
    gestión  
        listado de agregaciones de enlaces 460  
        modificación de la dirección alternativa 460  
ignorar  
    cabecera de fecha 40  
    en cabecera 40  
ignore, submandato 37, 40, 43  
IMAP (Internet Message Access Protocol)  
    configurar 102  
    visión general 101  
impresión  
    archivos 125, 544  
    desde sistemas remotos 126  
incluir archivos en un mensaje 26  
inetd, daemon  
    depuración 501  
info, mandato 34  
información de cabecera  
    añadir o cambiar 27  
inhabilitar opciones de correo 36, 37  
iniciadores de software iSCSI 477  
inicio  
    ATE 726  
    Connected Main Menu de ATE 727  
    editor de correo 24  
    programa de correo (mail) 12  
    Unconnected Main Menu de ATE 726  
instalación  
    8 puertos 765  
    TCP/IP 109  
intercambio de archivos  
    BNU 539  
interfaces  
    TCP/IP 173  
interfaces de red  
    TCP/IP 173  
IPv6  
    vean también Protocolo Internet Versión 6 130  
IPv6 (Protocolo Internet versión 6)  
    actualización a IPv6 con IPv4 configurado 138  
    actualizar a IPv6 con IPv4 no configurado 141

## K

Kerberos V.5  
autentificación [112, 116](#)  
validación de usuario [113](#)  
kvalid\_user, subrutina [113](#)

## L

LAN (Local Area Network - Red de área local), descripción [3](#)  
leer  
mail [12, 15](#)  
mensaje anterior [16](#)  
mensaje siguiente [16](#)  
mensajes [15](#)  
libauthm.a, biblioteca [113](#)  
libvaliduser.a, biblioteca [113](#)  
list, mandato [34](#)  
listar  
alias [37](#)  
campos de cabecera ignorados [40](#)  
campos de cabecera retenidos [41](#)  
listas de distribución [37](#)  
listas de control de accesos [593](#)  
listas de distribución  
crear [37](#)  
listar [37](#)  
LS (estación de enlace)  
definición [754](#)  
estadísticas  
consulta [755](#)  
lsauthent, mandato [113](#)  
lsdev, mandato [720](#)  
luces del módem [720](#)

## M

m, opción [541](#)  
m, submandato [24, 31, 44](#)  
macdef, submandato [115](#)  
macros  
ftp, escribir [115](#)  
mail  
a través de un enlace BNU o UUCP [22](#)  
almacenar [11](#)  
añadir a campos de cabecera [27](#)  
añadir contenido de dead.letter al mensaje [27](#)  
añadir información a un mensaje [25](#)  
aplicaciones [11](#)  
avisos de mensaje de ausencia por vacaciones [33](#)  
bcc, campo [28](#)  
buscar buzón actual [19](#)  
buscar carpeta actual [19](#)  
buzón personal [11](#)  
cambiar a otro buzón [20](#)  
cambiar cambios de cabecera [27](#)  
cambiar el mensaje actual [25](#)  
campo cc [37](#)  
campo subject [28, 37](#)  
cancelar mensajes de ausencia por vacaciones [33](#)  
cancelar reenviado [32](#)  
carpetas [11, 17](#)  
cc, campo [28](#)

mail (*continuación*)

cola  
Archivo de control q [49](#)  
combinar los submandatos delete y print [41](#)  
comprobar buzón del sistema [12](#)  
comprobar en buzón personal [13](#)  
comprobar en carpeta de correo [13](#)  
comprobar número de mensajes del buzón [15](#)  
correo secreto [33](#)  
crear [20](#)  
crear carpetas [41](#)  
crear correo secreto [33](#)  
crear un mensaje nuevo [31](#)  
dead.letter, archivo [11](#)  
deshacer la supresión de mensajes [17](#)  
desplazarse por el buzón [14](#)  
direcciónamiento [20](#)  
direccionar a más de un usuario [21](#)  
direccionar a usuarios de la red [21](#)  
direccionar a usuarios de una red diferente [22](#)  
direccionar a usuarios del sistema local [21](#)  
editar un mensaje [24](#)  
editores de texto [42](#)  
enviar [20, 29](#)  
enviar correo secreto [33](#)  
estado [12](#)  
filtro, configuraciones [56](#)  
guardar mensajes con cabeceras [18](#)  
guardar mensajes sin cabeceras [19](#)  
habilitar opciones [36](#)  
help [34](#)  
ignorar en cabecera [40](#)  
ignorar mensaje de fecha [40](#)  
incluir archivos con mensaje [26](#)  
inhabilitar opciones [36, 37](#)  
inicio [12](#)  
leer mensaje anterior [16](#)  
leer mensaje siguiente [16](#)  
leer mensajes [12, 15](#)  
líneas superiores de mensajes [39](#)  
lista de mensajes [38](#)  
mandatos del sistema [42](#)  
mensaje de cabecera [41](#)  
mensajes enviados [41](#)  
mensajes incompletos [11](#)  
mensajes largos [38](#)  
organización [17](#)  
personalización [35](#)  
rangos de mensajes [13](#)  
recepción [12](#)  
recibir correo secreto [33](#)  
reenviar mensajes [31](#)  
reenviar mensajes seleccionados [31](#)  
reenviar todo [32](#)  
requisitos de filtro [55](#)  
responder a [30](#)  
salida [17](#)  
submandatos [42](#)  
suprimir [16](#)  
suprimir mensajes [16](#)  
to, campo [28](#)  
ver opciones habilitadas [36](#)  
visión general [8](#)  
visualizar cabecera [40](#)

mail (*continuación*)  
  visualizar contenido de buzón 13  
  visualizar información de cabecera de correo 14  
  visualizar mensaje de cabecera 40  
  visualizar número de mensaje actual 15  
mail, mandato 12, 13, 20–22, 24, 29, 39, 41, 42, 120  
MAIL, variable de entorno 12  
MAILCHECK, variable de entorno 12  
MAILMSG, variable de entorno 12  
MAINMENU\_KEY, secuencia de teclas de control 727  
man, mandato 34  
mandato  
  ifconfig 719  
  lsdev 720  
  netstat 719  
  pdisable 720  
  ping 720  
  ps 720  
Mandato bellmail 10  
Mandato ifconfig 719  
Mandato netstat 719  
Mandato ps 720  
mandatos  
  ? 34  
  ate 726, 738  
  bellmail 10  
  bterm 5  
  cd 121, 122  
  chauthent 113  
  chmod 114  
  ct 538, 539  
  cu 538  
  enq 125, 126, 511  
  enroll 33  
  estado 124  
  f 127, 511  
  finger 127, 128, 511  
  fmt 28  
  ftp 112, 113, 121–123, 510  
  info 34  
  l 34  
  lsauthent 113  
  mail 12, 13, 20–22, 24, 29, 39, 41, 42, 120  
  man 34  
  mkdir 41  
  pg 36, 38  
  ping 120, 127, 511  
  rcp 112, 113, 121, 510  
  refresh 125, 511  
  remsh 116, 511  
  rexec 116, 511  
  rlogin 112, 113, 116, 126, 511  
  rm 32, 33  
  rsh 112, 113, 116, 511  
  rwho 127, 511  
  securetcpip 114  
  sistema principal 127, 511  
  smit 126, 511  
  solicitar ejecución de 542  
  spell 29  
  talk 120, 511  
  telnet 112, 113, 116, 119, 126, 502, 511  
  tftp 121, 123, 124, 510  
  tic 502

mandatos (*continuación*)  
  tip 538  
  tn 116, 511  
  tn3270 116, 511  
  touch 501  
  utftp 123  
  uucp 539  
  udecode 539–541  
  uuencode 539–541  
  uname 545  
  upick 539–541  
  upoll 542, 545  
  uuq 541  
  uusend 539  
  uusnap 541  
  uustat 541, 542, 547  
  uuto 539, 540  
  uux 542  
  vacation -I 33  
  whois 127, 511  
  xget 45  
  xmodem 738  
  xsend 33, 45  
Mandatos  
  /usr/sbin/mailstats 55  
  bugfiler 105  
  comsat 105  
  mail 7  
  mailq 48, 105  
  mailstats 105  
  mhmail 7  
  newaliases 47, 105  
  sendbug 105  
  sendmail 48, 53, 105  
  smmdemon.cleanu 105  
Mandatos de BNU  
  comprobación del estado 532  
  ejecución remota 536  
  mantenimiento 532  
mandatos de comunicaciones remotas 511  
mandatos de impresión 511  
mandatos de inicio de sesión remoto 511  
mandatos de transferencia de archivos 510  
mandatos del sistema  
  enviar correo secreto 45  
Mandatos NFS  
  lista de 648  
manejador de archivos  
  NFS (Network File System - Sistema de archivos de red) 598  
manejo de mensajes, submandatos 43  
marcación  
  hasta establecer una conexión 539  
  múltiples números 539  
mbox 11  
mensaje de cabecera  
  control de la visualización 41  
mensajes de error  
  NFS 640  
métodos  
  TCP/IP 513  
métodos de autentificación  
  Kerberos V.4 113  
  Kerberos V.5 112, 113, 116

métodos de autentificación (*continuación*)

Standard AIX [113](#)

métrica [434](#)

mh, programa [9](#)

MIB (Base de información de gestión)

variables [576](#)

MIL-STD

señal de la interfaz [767](#)

MIL-STD 188

nivel de voltaje de señal [768](#)

Milter [55](#)

mkdir, mandato [41](#)

mMail

cola

mover [52](#)

modalidad de local ocupado [754](#)

modalidad de retención corta [754](#)

módems

cableado [687](#)

conexión de un módem [688](#)

conexiones

ejemplo de configuración de BNU [526–528](#)

configurar [689](#)

consideraciones [685](#)

estándares

ITU-TSS [683](#)

Microcom Networking Protocol (MNP) [683](#)

estándares para las telecomunicaciones [683](#)

hayes y compatibles con hayes [691](#)

mandatos

envío de mandatos AT [689, 690](#)

resolución de problemas [692](#)

resumen de mandatos AT

modificadores de marcación [698](#)

resumen de códigos de resultados [698](#)

resumen de los registros S [696](#)

visión general [682](#)

modify, submandato [726, 727](#)

mount, mandato

NFS (Network File System - Sistema de archivos de red)

sistemas de archivos [623](#)

MTU

Descubrimiento de MTU de vía de acceso [486](#)

## N

n, submandato [16, 43, 45](#)

nativa, configuración [114](#)

negociación de terminal [116](#)

NFS

servicio de proxy [596](#)

NFS (Network File System - Sistema de archivos de red)

ACL (Access Control Lists - Lista de control de accesos) [593](#)

Archivo /etc/exports [599](#)

Archivo /etc/xtab [600](#)

archivos correlacionados [595](#)

arranque del sistema

cómo iniciar [615](#)

automount, daemon [624](#)

clientes

cómo configurarlas [616](#)

controlar [601](#)

NFS (Network File System - Sistema de archivos de red) (*continuación*)

Daemon portmap [601](#)

determinación de problemas

archivos de montaje fijo [638](#)

archivos de montaje flexible [638](#)

esquemas de autentificación [643](#)

lista de mandatos [638](#)

permissions [643](#)

programas colgados [643](#)

directory [592](#)

enlace [598](#)

exportar [592](#)

extensión de kernel [647](#)

gestor de bloqueos de red

arquitectura [635](#)

cómo iniciar [636](#)

periodo de gracia [635](#)

proceso de bloqueo de archivos de red [635](#)

proceso de recuperación de detención anormal [635](#)

resolución de problemas [636](#)

grupos [645](#)

hebras biod

cómo cambiar el número de [602](#)

implementación [601](#)

lista de comprobación para configurar [615](#)

manejador de archivos [598](#)

mensajes de error

mount [640](#)

nfs\_server [640](#)

montajes

predefinidos [631](#)

tipos de [596](#)

NFS seguro

daemons de red [649](#)

programas de utilidad de red [649](#)

nfsd, daemons

cómo cambiar el número de [602](#)

PC-NFS

servicios de autentificación [632](#)

servicios de spooling de impresión [632](#)

periodo de gracia [604](#)

proceso de montaje [598](#)

puntos de montaje [616](#)

RPC [601](#)

rpc.

cómo configurarlas [632](#)

rpc.pcnfsd

cómo iniciar [633](#)

cómo verificar la accesibilidad [633](#)

servicios de red

lista de [592](#)

servidores

cómo configurarlas [616](#)

servidores sin estado [592](#)

sistema de archivos [592](#)

sistema de archivos de antememoria [594](#)

sistemas de archivos

cómo desmontar [631](#)

cómo eliminar la exportación [621](#)

cómo exportar [617](#)

cómo habilitar el acceso de root [622](#)

cómo montar automáticamente [624](#)

cómo montar explícitamente [623](#)

exportados, cómo cambiar [622](#)

NFS (Network File System - Sistema de archivos de red) (*continuación*)

- supervisor de estado de red [635](#)
- tiempos de acceso [642](#)
- visión general [592](#)
- XDR [601](#)

NFS, daemons

- argumentos de línea de mandatos
  - cómo cambiar [602](#)
- bloquear
  - lista de [649](#)
- cómo detener [603](#)
- cómo iniciar [603](#)
- cómo obtener el estado actual [603](#)
- controlar [601](#)
- NFS seguro [649](#)

NFS, servidores

- determinación de problemas
  - resolución de nombres [644](#)
- programas colgados [643](#)

nfsd, daemons

- NFS (Network File System - Sistema de archivos de red)
  - [602](#)

NIC [787](#)

NIC (Network Information Center) [443](#)

no header, opción [41](#)

nombre\_sistema!, nombres de vía de acceso [534](#)

nombre\_sistema!nombre\_sistema!, nombres de vía de acceso [534](#)

nombres de vía de acceso

- BNU [533](#)
- completos [533](#)
- directorio inicial de usuario [534](#)
- identificar a través de varios sistemas [534](#)
- identificar en otro sistema [534](#)
- nombre\_sistema!, [534](#)
- nombre\_sistema!nombre\_sistema!, [534](#)
- ~[opción] [534](#)
- que empiezan con un tilde [534](#)
- relativos [534](#)

nombres de vía de acceso relativos [534](#)

nombres de vías de acceso completos [533](#)

número de mensaje

- visualización [15](#)

números asignados [169](#)

## O

opción de exportación de referencia

- opción de exportación de réplica [606](#)

opción escape [24](#)

opciones

- ask [37](#)
- askcc [37](#)
- autoprint [41](#)
- crt [38](#)
- editor [42](#)
- escape [24](#)
- folder [41](#)
- m [541](#)
- no header [41](#)
- p [541](#)
- pantalla [38](#)
- q [541](#)
- quiet [41](#)

opciones (continuación)

- record [41](#)
- set folder [11](#)
- toplines [39](#)
- visual [42](#)
- opciones de correo
  - binary [36](#)
  - con un valor [36](#)

operaciones de impresión en TCP/IP

- sistemas remotos [125](#)

organización del correo [17](#)

## P

p, opción [541](#)

p, submandato [15, 41](#)

P, submandato [40](#)

pantalla, opción [38](#)

paquete [108](#)

paquetes [128](#)

parámetros

- bits de marca [669](#)
- bits por carácter [668](#)
- bits por segundo [668](#)
- inicio [669](#)
- parada [669](#)
- paridad [668](#)
- velocidad en baudios [668](#)

pasarelas

- TCP/IP [434](#)

PC-NFS [631, 632](#)

pdisable, mandato [720](#)

perform, submandato [726, 727, 738](#)

permissions, archivos [538](#)

personalización

- mail [35](#)
- TCP/IP [114](#)

Personalización de TCP/IP

- escribir macros FTP [115](#)

- modificación de la asignación de un grupo de teclas [115](#)

personalizar ATE [728](#)

pg, mandato [36, 38](#)

ping, mandato [120, 127, 511, 720](#)

pipe, submandato [28, 44](#)

planificación de la comunicación asíncrona [658](#)

planificación de red

- TCP/IP [108](#)

poner en cola trabajos utilizando smit [126](#)

POP (Post Office Protocol)

- configurar [102](#)

- visión general [101](#)

por omisión

- buzón personal [11](#)

- carpetas [41](#)

PPP (Point-to-Point Protocol)

- procesos a nivel de usuario [707](#)

pre, submandato [43](#)

preparado para enviar/borrar para enviar [671](#)

PREVIOUS\_KEY, secuencia de teclas de control [727](#)

prioridad de las comunicaciones [767](#)

problemas [721](#)

procedimientos del shell

- BNU [533](#)

proceso [108](#)

proceso de montaje  
     NFS (Network File System - Sistema de archivos de red) 598  
 programa de correo (mail) 9, 11  
 programa de utilidad de varias pantallas 739  
 programa manejador de mensajes 9  
 programación manual del módem 712  
 programas  
     mail 9  
     manejador de mensajes 9  
     mh 9  
     sendmail 8  
 Programas de correo  
     bellmail 7  
     BNU 7  
 programas de utilidad  
     NFS  
         seguro 649  
         servicios de red 649  
 Programas de utilidad básicos de red (Basic Networking Utilities)  
     cancelación de trabajos remotos 547  
     cola de trabajos 541  
     comunicación entre locales y remotos 538  
     estado de intercambios 541  
     estado de operaciones 542  
     identificar sistemas compatibles 545  
     imprimir archivos 544  
     intercambiar mandatos 542  
     intercambio de archivos 539  
     marcar hasta establecer una conexión 539  
     marcar varios números 539  
     nombre\_sistema!, nombres de vía de acceso 534  
     nombre\_sistema!nombre\_sistema!, nombres de vía de acceso 534  
     nombres de vía de acceso 533  
     nombres de vía de acceso relativos 534  
     nombres de vías de acceso completos 533  
     ~[option] nombres de vía de acceso 534  
     sistemas conectados 541  
     TCP/IP 107  
 protocolo 108  
 Protocolo de configuración dinámica de sistemas  
     principales (Dynamic Host Configuration Protocol - DHCP)  
     asignaciones de parámetros  
         TCP/IP 218  
     daemon proxy 347  
     direcciones  
         TCP/IP 218  
 Protocolo de control de transmisiones (Transmission Control Protocol) 161  
 Protocolo de control de transmisiones/Protocolo Internet (Transmission Control Protocol/Internet Protocol) 108  
 Protocolo de mensajes de control de Internet (Internet Control Message Protocol) 151  
 Protocolo Internet (Internet protocol) 152  
 Protocolo Internet Versión 6 130  
 protocolo Point-to-point protocol asíncrono  
     procesos a nivel de usuario 707  
 protocolo PPP asíncrono  
     configuración 708  
 protocolos  
     pasarela 435  
 puerto 108  
 puertos  
     serie frente a del sistema 666  
 puertos del sistema  
     distinción de los puertos serie 666  
 puertos serie  
     distinción de los puertos del sistema 666  
 punto de acceso de servicio (SAP) 753  
 puntos de montaje  
     NFS (Network File System - Sistema de archivos de red) 616  
 put, submandato 124

## Q

q, opción 541  
 q, submandato 17, 43, 45  
 quiet, opción 41  
 quit, submandato 726, 727, 738

## R

r, submandato 30, 44  
 R, submandato 30, 44  
 rcmds seguros  
     configuración del sistema 113  
 rcp, mandato 112, 113, 121, 510  
 RDMA 789  
 receive, submandato 727, 738  
 recepción  
     archivos 541  
     correo secreto 33  
     mail 12  
 recepción de un archivo con ATE 736  
 record, opción 41  
 red 108  
 Red  
     física 3  
     LAN (Local Area Network - Red de área local) 3  
     MAN (Metropolitan Area Network - Red de área metropolitana) 3  
     sistemas y protocolos 4  
     WAN (Wide Area Network - Red de área amplia) 3  
 Red en Anillo 175  
 red jerárquica 108  
 red plana 108  
 red, direcciones 179  
 reenviar  
     mensajes de correo 31  
     mensajes seleccionados 31  
     todo el correo 32  
 reformatear un mensaje 28  
 refresh, mandato 125, 511  
 remote.unknown, archivo 537  
 remsh, mandato 116, 511  
 resolución de nombres  
     TCP/IP 184  
 resolución de nombres NIS\_LDAP 217  
 resolución de problemas  
     ATE 737  
     EtherChannel 470  
     SNMPv1 589  
     SNMPv3 569

resolución de problemas (*continuación*)
   
     TTY 674

responder al correo 30

restablecer campos de cabecera 40

retain, submandato 40, 41

rexec, mandato 116, 511

RFC 1010 150

RFC 1100 150

RFC 1155 552

RFC 1157 552

RFC 1213 552

RFC 1227 552

RFC 1229 552

RFC 1231 552

RFC 1398 552

RFC 1512 552

RFC 1514 552

RFC 1592 552

RFC 1905 552

RFC 1907 552

RFC 2572 552

RFC 2573 552

RFC 2574 552

RFC 2575 552

RFC 791 152

rlogin, mandato 112, 113, 116, 126, 511

rm, mandato 32, 33

rmail 105

RoCE 787, 789

RPC
 

- NFS 601

rpcinfo, mandato
 

- configuración de NFS 633

rsh, mandato 112, 113, 116, 511

RTS/CTS
 

- definición 671

ruta
 

- definición de 433

ruta de red 433

ruta de sistema principal 433

ruta predeterminada 433

rwho, mandato 127, 511

**S**

s, submandato 17, 18, 43, 45

salida
 

- editor de correo 25
- mail 17

SAP (punto de acceso de servicio)
 

- definición 753
- estadísticas
  - consulta 755

Scripts
 

- /usr/lib/smddemon.cleanu 54

secuencias de teclas de control
 

- ATE 727
- CAPTURE\_KEY 727
- MAINMENU\_KEY 727
- PREVIOUS\_KEY 727

securetcpip, mandato 114

seguridad
 

- BNU 536
- seguridad de TCP/IP

seguridad de TCP/IP (*continuación*)
 

- archivos de configuración 114
- seleccionar un editor de correo 42
- send, submandato 727, 738
- sendmail
  - filtrar 55
- Sendmail
  - detener 53
  - inicio 52
- sendmail, programa 8
- serial line internet protocol 710
- serie
  - comunicación 665
  - transmisión 665
- servicios de autentificación
  - PC-NFS 632
- servicios de red
  - daemons
    - lista de 649
  - programas de utilidad
    - lista de 649
- servidor
  - TCP/IP 112
- servidores
  - configuración de IMAP 102
  - configuración de POP 102
  - NFS (Network File System - Sistema de archivos de red)
    - sin estado 592
- set folder, opción 11
- set folder, submandato 18
- set\_auth\_methods, subrutina 113
- set, submandato 18, 36, 43
- síncrona, comunicación 666
- sincronización 666
- Sistema de archivos cliente SMB 653
- sistema de archivos de antememoria, soporte
  - NFS (Network File System - Sistema de archivos de red) 594
- Sistema de archivos de red (Network File System - NFS) 592
- sistema principal 108
- sistema principal, direcciones 179
- sistemas de archivos 592
- sistemas remotos
  - BNU
    - sondeo 521
    - copia de archivos 121, 123
    - impresión desde 126
    - impresión en 125
    - iniciar la sesión en 119
    - iniciar sesión directamente 121
    - iniciar sesión indirectamente 122
    - visualizar usuarios conectados 127, 128
- SLIP
  - activación de una conexión 718
  - configuración 711
  - cuestionario 722
  - depuración de problemas 718
  - desactivación de una conexión
    - temporal 717
  - eliminación de una interfaz 718
- SMB 653
- SMBCFS 653
- smfi\_addheader 72

smfi\_addrcpt 78  
smfi\_addrcpt\_par 78  
smfi\_chgfrom 77  
smfi\_chgheader 74  
smfi\_delrcpt 79  
smfi\_getpriv 67  
smfi\_getsymval 66  
smfi\_insheader 75  
smfi\_main 65  
smfi\_opensocket 57  
smfi\_progress 81  
smfi\_quarantine 82  
smfi\_register 58  
smfi\_replacebody 80  
smfi\_setbacklog 63  
smfi\_setconn 61  
smfi\_setdbg 63  
smfi\_setmlreply 70  
smfi\_setpriv 68  
smfi\_setreply 68  
smfi\_setsymlist 99  
smfi\_settimeout 62  
smfi\_stop 64  
smfi\_version 99  
smit, mandato 126, 511  
SMTP (Simple Mail Transfer Protocol - Protocolo simple de transferencia de correo) 7  
SNMP  
    introducción 552  
    SNMPv1  
        configurar 571  
        daemon 571  
        políticas de acceso 571  
        procesar 572  
        resolución de problemas 589  
    SNMPv3  
        emitir peticiones 561  
        introducción 553  
        resolución de problemas 569  
SNMP (protocolo simple de gestión de red)  
    SNMPv1  
        migrar hasta SNMPv3 562  
    SNMPv3  
        actualizar dinámicamente claves en 558  
        crear usuarios en 565  
        migrar desde SNMPv1 562  
SNMP, daemon  
    MIB, soporte de variables 576  
solicitar ejecución de un mandato 542  
sondeo  
    BNU  
        sistemas remotos 521  
soporte de archivos correlacionados  
    NFS (Network File System - Sistema de archivos de red)  
        595  
Soporte DIO y CIO de NFS 605  
soporte sin disco  
    NFS  
        SUN 649  
soporte sin disco NFS  
    SUN  
        clientes 649  
source, submandato 36  
spell, mandato 29  
spooling, directorio  
    BNU 516  
SRC (System Resource Controller - Controlador de recursos del sistema)  
    NFS (Network File System - Sistema de archivos de red)  
        daemons 603  
submandatos  
    - 16  
    ! 43, 45  
    ? 34  
    . 29, 44  
    + 16  
    = 15  
    ~: 44  
    ~! 29, 44  
    ~? 34  
    ~b 28  
    ~c 28  
    ~d 27, 44  
    ~e 25, 42, 44  
    ~f 26, 31, 32, 44  
    ~h 27  
    ~m 26, 31, 32, 44  
    ~p 25, 44  
    ~q 25, 44  
    ~r 26, 44  
    ~s 28  
    ~t 28  
    ~v 25, 42, 44  
    ~w 44  
    a 37, 44  
    alias 37  
    alter 726, 727  
    añadir a cabecera 44  
    añadir a mensaje 44  
    archivo 20  
    break 727, 738  
    buzón secreto 45  
    cambiar mensaje 44  
    cd 43  
    connect 726, 727, 738  
    control 43, 44  
    correo secreto 45  
    crear correo nuevo 44  
    d 16, 41, 43, 45  
    directory 726, 738  
    dp 16  
    dt 16  
    e 24, 25, 43  
    EOT 44  
    ex 17  
    f 14, 43  
    folder 15, 19, 20, 43  
    get 124  
    h 38, 43  
    help 726, 727, 738  
    ignore 37, 40, 43  
    m 24, 31, 44  
    macdef 115  
    manejo de mensajes 43  
    modify 726, 727  
    n 16, 43, 45  
    p 15, 41

submandatos (*continuación*)

- P 40
- perform 726, [727](#), [738](#)
- pipe 28, [44](#)
- pre 43
- put [124](#)
- q [17](#), [43](#), [45](#)
- quit 726, [727](#), [738](#)
- r [30](#), [44](#)
- R [30](#), [44](#)
- receive 727, [738](#)
- retain [40](#), [41](#)
- s [17](#), [18](#), [43](#), [45](#)
- send 727, [738](#)
- set [18](#), [36](#), [43](#)
- set folder [18](#)
- source [36](#)
- t [15](#), [38](#), [40](#), [43](#)
- T [40](#)
- Tecla de retorno 45
- terminate 727, [738](#)
- top [39](#), [40](#), [43](#)
- u [17](#), [43](#)
- unalias [37](#)
- unset [36](#), [37](#)
- v [24](#), [25](#)
- visualización [43](#)
- w [17](#), [19](#), [43](#), [45](#)
- x [17](#), [43](#)
- z [13](#), [14](#), [38](#)

submandatos para crear correo nuevo [44](#)

subrutinas

- get\_auth\_methods [113](#)
- kvalid\_user [113](#)
- set\_auth\_methods [113](#)

subservidores

- TCP/IP [431](#), [511](#)

subsistemas

- TCP/IP [431](#), [511](#)

supervisión

- BNU
  - automática [521](#)
  - conexión remota [543](#)
  - transferencia de archivos [544](#)
- supervisor de estado de red [635](#)
- suprimir
  - .forward, archivo [32](#), [33](#)
  - mail [16](#)
  - mensajes [16](#)
- SYSLOG, recurso [104](#)

**T**

t, submandato [15](#), [38](#), [40](#), [43](#)

T, submandato [40](#)

tabla de direccionamiento [433](#)

talk, mandato [120](#), [511](#)

tarjetas de adaptadores de red

- TCP/IP [170](#)

TCP/IP

- /etc/gated.conf [440](#)
- /etc/gateways [440](#), [499](#)
- /etc/hosts [108](#), [111](#), [184](#), [186](#), [189](#), [191](#), [498](#)
- /etc/named.boot [192](#)

TCP/IP (*continuación*)

- /etc/named.ca [192](#)
- /etc/named.data [192](#)
- /etc/named.local [192](#)
- /etc/named.rev [192](#)
- /etc/networks [440](#), [499](#)
- /etc/protocols [169](#)
- /etc/rc.net [109](#)
- /etc/rc.tcpip [431](#), [440](#)
- /etc/resolv.conf [189](#), [192](#), [498](#)
- /etc/sendmail.cf [189](#), [201](#)
- /etc/services [169](#)
- /etc/syslog.conf [498](#)
- /usr/lib/sendmail.cf [201](#)
- asignaciones de parámetros
- DHCP [218](#)
- BINLD [390](#)
- BNU
  - archivos de dispositivos [524](#)
  - client [108](#)
  - conexiones BNU [536](#)
  - conexiones de sistema principal [116](#)
  - configuración [109](#)
  - conversación en tiempo real [120](#)
  - copia de archivos [121](#), [123](#)
  - daemons
    - cómo configurar gated [440](#)
    - cómo configurar routed [440](#)
    - inetd [431](#)
    - SRC (System Resource Controller - Controlador de recursos del sistema) [501](#)
    - subservidores [511](#)
    - subsistemas [511](#)
  - denominación
  - autorización [185](#)
  - cómo elegir nombres [186](#)
  - convenios [186](#)
  - DNS (Servicio de nombres de dominio) [184](#)
  - dominio [185](#)
  - red jerárquica [108](#), [184](#)
  - red plana [108](#), [184](#)
  - direccionalar
    - cómo configurar gated [440](#)
    - cómo configurar routed [440](#)
    - cómo obtener un número de sistema autónomo [443](#)
    - cuenta de saltos [434](#)
    - dinámico [434](#), [436](#)
    - direcciónadores [434](#)
    - estático [434](#), [436](#)
    - gated [434](#)
    - métrica [434](#)
    - pasarelas [111](#), [434](#)–[437](#)
    - protocolos [435](#)
    - resolución de problemas [499](#)
    - routed [434](#)
  - direcciones
    - bucle de retorno local [184](#)
    - ceros [181](#)
    - clase A [179](#)
    - clase B [180](#)
    - clase C [180](#)
    - comparación [183](#)
    - daemon de proxy DHCP [347](#)
    - DHCP [218](#)

TCP/IP (*continuación*)  
direcciones (*continuación*)  
difusión 184  
locales 179  
máscaras de subred 182  
red 179  
sistema principal 179  
subred 181  
ejemplos  
  configuración de BNU 524  
File Transfer Protocol (FTP) 121  
grupo de teclas 115  
grupo de teclas de instalación y configuración 115  
imprimir desde sistemas remotos 126  
instalación 109  
interfaces 173  
interfaces de red  
  802.3 175  
  configuración automática 174  
  configuración de SLIP 176  
  creación automática 174  
  creación manual 174  
  Ethernet Versión 2 174  
  gestión 176  
  óptica serie 176  
  Red en Anillo 175  
  resolución de problemas 504  
  varias 176  
lista de daemons 511  
lista de mandatos 507  
mail, mandato 107  
mandato sendmail 107  
mandatos  
  lista de 111  
  transferencia de archivos 121  
mandatos de comunicaciones remotas 511  
mandatos de estado 127, 511  
mandatos de impresión 511  
mandatos de inicio de sesión remoto 511  
mandatos de Manejo de mensajes 107  
mandatos de transferencia de archivos 121, 123, 510  
métodos 513  
paquete 108  
paquetes  
  cabeceras 147–149  
  definición 128  
  rastreo 147  
  resolución de problemas 507  
planificación de red 108  
poner en cola trabajos utilizando smit 126  
poner en cola un trabajo con el mandato enq 125  
PPP (Point-to-Point Protocol)  
  procesos a nivel de usuario 707  
  utilizado como alternativa a SLIP 707  
proceso 108  
protocolo 108  
Protocolo Internet Versión 6 130  
protocolos  
  nivel de aplicación 164  
  nivel de red 150–152  
  nivel de transporte 155–157, 161  
  números asignados 169  
puerto 108  
red 108

TCP/IP (*continuación*)  
resolución de nombres  
  local, cómo realizar 191  
  planificar para dominio 192  
  proceso 189  
  resolución de problemas 498  
resolución de problemas  
  comunicación 498  
  direccionar 499  
  entrega de paquete 507  
  ESCDELAY 502  
  interfaz de red 504, 505  
  resolución de nombres 498  
  SRC 501  
  telnet o rlogin 502  
  TERM 502  
RFC  
  RFC 1010 150  
  RFC 1100 150  
  RFC 791 152  
  soportadas 513  
ruta  
  definición de 433  
  por omisión 433  
  red 433  
  sistema principal 433  
servicios de red de cliente 432  
servicios de red de servidor 433  
servidor 108  
servidor de correo 201  
servidor de nombres  
  archivos de configuración 192  
  cómo configurar el servidor de correo 201  
  cómo configurar el sistema principal para que lo utilice 206  
  cómo configurar esclavo 194  
  cómo configurar intermedio 194  
  cómo configurar maestro 194  
  esclavo 186  
  maestro 186  
  remitente/cliente 186  
  remoto 186  
  sólo almacenamiento en antememoria 186  
  zona de autorización 186  
servidor de nombres DNS  
  configuración de zonas dinámicas 208  
servidores 111  
sistema principal 108  
sistemas principales 111  
SLIP  
  /usr/lib/uucp/Devices 714, 715  
  cómo configurar a través de un módem 714  
  cómo configurar a través de un módem nulo 715  
  desactivación de una conexión SLIP 717  
tabla de direccionamiento 433  
tarjetas de adaptadores de red  
  cómo configurarlas 170  
  cómo instalarlas 170  
tramas  
  definición 128  
Trivial File Transfer Protocol (TFTP) 121  
TTY  
  utilizado para SLIP a través de un módem 714  
  utilizado para SLIP a través de un módem nulo 715

TCP/IP (*continuación*)  
valores predeterminados 174  
visión general 107  
visualizar usuarios conectados 127, 128

Tecla de retorno, submandato 45

telnet, conexión  
depuración 502

telnet, mandato 112, 113, 116, 119, 126, 502, 511

telnetd, daemon  
depuración 502

TERM  
TCP/IP  
TERM 502

TERM, variable de entorno 672

termcap, conversión 672

terminal 671

terminal de datos preparado/conjunto de datos preparado 671

terminate, submandato 727, 738

terminfo, base de datos 672

tftp, mandato 121, 123, 124, 510

tic, mandato 502

tiempos de acceso  
NFS 642

tip, mandato  
configurar 546  
variables  
orden de utilización 545  
visión general 545

tn, mandato 116, 511

tn3270, mandato 116, 511

to, campo 28

top, submandato 39, 40, 43

toplines, opción 39

topología  
visión general 665

touch, mandato 501

trabajos  
iniciar la transmisión 545

tramas 128

transferencia  
archivos 121  
trabajos en spool 545

transferencia de archivos  
TCP/IP 121

transferencia de un archivo con ATE 736

transferencias de archivos  
BNU  
supervisión 544

transmisor activado/transmisor desactivado 671

Trivial File Transfer Protocol 123

TTY  
configuración de SLIP a través de un cable de módem nulo 715  
configuración de SLIP a través de un módem 714  
definición 671  
ejemplos 671  
gestión 672  
resolución de problemas  
identificadores del registro de tty 676  
información del registro de errores 676

tareas  
establecimiento de las características del tty 672

TTY (*continuación*)  
tareas (*continuación*)  
utilizando el programa de utilidad de varias pantallas 739

## U

u, submandato 17, 43

umount, mandato  
NFS (Network File System - Sistema de archivos de red)  
sistemas de archivos 631

unalias, submandato 37

UNIX-to-UNIX Copy Program 513

unset, submandato 36, 37

User Datagram Protocol 156, 157

usuarios  
añadir a campos de cabecera de mensaje 28

utftp, mandato 123

uucico, daemon 535, 542, 545

uuclean, mandato 532

uucleanup, mandato 532

UUCP 538

UUCP (UNIX-to-UNIX Copy Program) 513, 536

uucp, mandato 539

uudecode, mandato 539–541

uudemon.admin, mandato 533

uudemon.cleanu, mandato 532

uuencode, mandato 539–541

uuname, mandato 545

uupick, mandato 539–541

uupoll, mandato 532, 542, 545

uuq, mandato 532, 541

uusend, mandato 539

uusnap, mandato 532, 541

uustat, mandato 532, 541, 542, 547

uuto, mandato 539, 540

Uutry, mandato 543, 544

uutx, daemon 542

uux, mandato 542

uuxqt, daemon 536, 542

## V

v, submandato 24, 25

vacation-I, mandato 33

vacation.def, archivo 33

validación de usuario  
Kerberos V.5 113

variables  
tip, mandato  
orden de utilización 545

variables de entorno  
MAIL 12  
MAILCHECK 12  
MAILMSG 12

ver opciones de correo habilitadas 36

vi, editor 24, 42

VIPA (Dirección IP virtual) 446

visión general asíncrona 658

visual, opción 42

visualización  
cabecera de correo 40

visualización (*continuación*)

Connected Main Menu de ATE [727](#)  
contenido del buzón [13](#)  
información de cabecera de correo [14](#)  
mensaje de cabecera de correo [40](#)  
número del mensaje actual [15](#)  
Unconnected Main Menu de ATE [726](#)  
usuarios conectados [127, 128](#)  
visualización, submandatos [43](#)

## W

w, submando [17, 19, 43, 45](#)  
WAN (Wide Area Network - Red de área amplia), descripción  
[3](#)  
whois, mandato [127, 511](#)

## X

x, submando [17, 43](#)  
XDR  
NFS (Network File System - Sistema de archivos de red)  
[601](#)  
xmodem, protocolo [738](#)  
XON/XOFF  
definición [671](#)  
xsend, mandato [33](#)  
xtab, archivo [600](#)  
xxfi\_body [92](#)  
xxfi\_close [95](#)  
xxfi\_connect [86](#)  
xxfi\_data [90](#)  
xxfi\_envfrom [87](#)  
xxfi\_envrcpt [88](#)  
xxfi\_eoh [92](#)  
xxfi\_eom [93](#)  
xxfi\_header [91](#)  
xxfi\_helo [87](#)  
xxfi\_negotiate [96](#)  
xxfi\_unknown [90](#)

## Z

z, submando [14, 38](#)





**IBM.**<sup>®</sup>