1.- Arquitectura TCP/IP

Encaminamiento IP

Las capas IP en los ordenadores como sistemas finales y en los dispositivos de encaminamiento trabajan de forma conjunta para encaminar paquetes desde las redes IP origen a las de destino. La capa IP en cada ordenador y cada dispositivo de encaminamiento (router) mantiene una tabla de encaminamiento que se utiliza para determinar cómo tratar cada paquete IP. Considere la acción en el ordenador origen. Si la tabla de encaminamiento indica que el ordenador destino está conectada directamente al ordenador origen por un enlace o por una red LAN, el paquete se envía directamente al ordenador destino utilizando la interfaz física apropiada. En otro caso, la tabla de encaminamiento especifica normalmente que el paquete se debe enviar a un router por defecto que está conectado directamente al ordenador origen. Ahora considere la acción de un dispositivo de encaminamiento. Cuando un router recibe un paquete a través de una de sus interfaces de red, éste examina su tabla de encaminamiento para ver si el paquete va dirigido a él mismo, y si es así, pasarlo al protocolo de la capa superior apropiado. Si la dirección IP no es la del propio router, entonces determina el siguiente router en la ruta y la interfaz asociada.
Cada fila en la tabla de encaminamiento debe proporcionar la siguiente información: dirección IP destino, dirección IP del siguiente router en la ruta, varios campos de indicadores, y una interfaz salida. Hay que definir varios tipos de indicadores. Por ejemplo, el indicador H especifica si la ruta en la fila dada es hacia un ordenador (Host, H=1) o hacia una red (H=0). El indicador G especifica si la ruta en la fila dada es hacia un router (Gateway, G=1) o hacia un destino directamente conectado (G=0).
Cada vez que se va a encaminar un paquete, la búsqueda en la tabla de encaminamiento se realiza en el siguiente orden. Primero, se realiza una búsqueda en la primera columna para ver si la tabla de encaminamiento contiene una entrada con la dirección IP destino completa. Si es así, el paquete IP se reenvía de acuerdo con la entrada de siguiente salto y el indicador G. Segundo, si la tabla no contiene una dirección IP destino completa, se busca en la tabla de encaminamiento el identificador de red destino. Si se encuentra una entrada, el paquete IP se reenvía de acuerdo con la entrada de siguiente salto y el indicador G. Tercero, si la tabla no contiene el identificador de red destino, se busca en la tabla una entrada para un dispositivo de encaminamiento por defecto, y si se encuentra, el paquete se reenvía allí. Finalmente, si ninguna de las búsquedas anteriores tiene éxito, el paquete se declara como que no se puede entregar y se envía un paquete ICMP de "error de destino inalcanzable" al ordenador origen.
Ejemplo: encaminamiento con subredes
Suponga que el ordenador H5 desea enviar un paquete IP al ordenador H2 en la figura 4.1.1. H2 tiene la dirección IP 147.83.12.76, a continuación se analizará como se realiza esta tarea.
La tabla de encaminamiento en H5 sería la siguiente:

```
Destino        Siguiente salto     Banderas  Interfaz de
salida
127.0.0.1      127.0.0.2      H         lo0
147.83.14.0         147.83.14.4                   eth0
default        147.83.14.1         G         eth0
```

La primera entrada es la interfaz de lazo cerrado o loopback, el indicador H especifica una dirección de ordenador y lo0 es siempre por convención la interfaz de lazo cerrado. La segunda entrada no tiene puesto a 1 el indicador H, por lo que se trata de una

dirección de red; tampoco está puesto a 1 el indicador G, por lo que se indica una ruta directa y la entrada salto siguiente es la dirección IP de una interfaz de red de salida de la propia máquina. La tercera entrada es la ruta por defecto, con R2 (147.83.14.1) como dispositivo de encaminamiento, de ahí que G=1, y con una interfaz ethernet eth0.

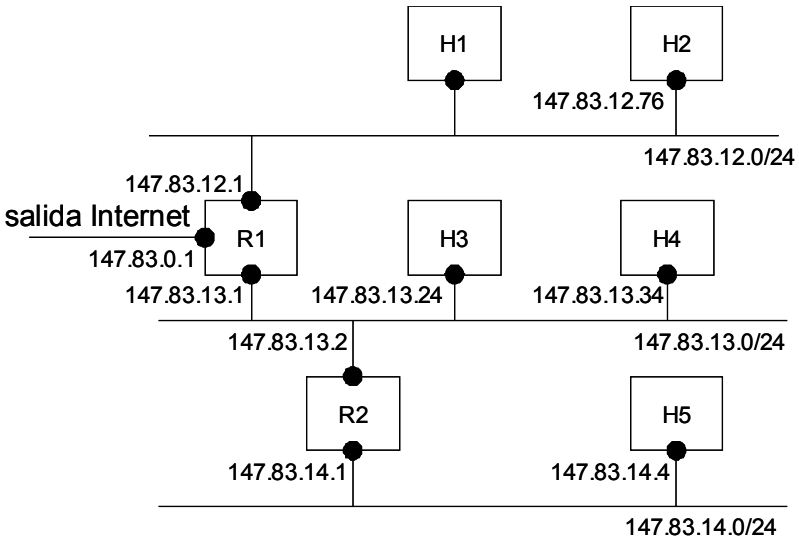

Figura 4.1.1. Ejemplo de red subdividida con una máscara de 255.255.255.0.

H5 busca primero es su tabla de encaminamiento la dirección IP destino del paquete 147.83.12.76 (H2). Cuando H5 no encuentra la entrada busca el identificador de red 147.83.12.0. Cómo éste tampoco lo encuentra busca la ruta por defecto, que sí está presente. En este caso se envía el paquete a la dirección del router R2 (147.83.14.1) a través de la red Ethernet.
La taba de encaminamiento de R2 podría ser algo parecido a lo siguiente:

```
Destino        Siguiente salto     Banderas  Interfaz de
salida
127.0.0.1      127.0.0.2      H         lo0
147.83.13.0         147.83.13.2                    eth0
147.83.14.0         147.83.14.1                    eth1
default        147.83.13.1         G         eth0
```

R2 realiza una búsqueda en su tabla de encaminamiento y envía el paquete IP al router R1, utilizando la ruta por defecto. R1 podría tener la siguiente tabla de encaminamiento:

```
Destino        Siguiente salto     Banderas  Interfaz de
salida
127.0.0.1      127.0.0.2      H         lo0
147.83.13.0         147.83.13.1                    eth0
147.83.12.0         147.83.12.1                    eth1
default        147.83.0.2          G         eth3
```

R1 realiza una búsqueda en su tabla de encaminamiento y encuentra una entrada para la dirección de de red 147.83.12.0, así enviará el paquete a través de su interfaz eth1 para que llegue al ordenador H2.
La orden netstat le permite mostrar la tabla de encaminamiento en su ordenador. Consulte el manual de su sistema para ver como se realiza esta orden.

Encaminamiento entre dominios sin clase

La división del espacio de direcciones IP en las clases A, B y C ha resultado ser inflexible. Mientras que, por una parte, la mayoría de las organizaciones utilizan ineficientemente la dirección de red de Clase B, por otra, normalmente la mayoría de als organizaciones necesitan más direcciones que las que proporciona una red de Clase C. Si se hubiera dado una dirección de Clase B a cada organización, se habría agotado fácilmente el espacio de direcciones IP, debido al rápido crecimiento de Internet. En 1993 se eliminó la restricción del espacio de direcciones con clase. En lugar del esquema con clase, se adoptó un esquema en el que se utiliza una longitud de prefijo arbitraria para indicar el número de red, conocido como encaminamiento entre dominios sin clase, CIDR (Classless InterDomain Routing). Utilizando la notación CIDR, un prefijo 147.83.12.0 de longitud 23 se escribe como 147.83.12.0/23. El rango de direcciones correspondientes a este prefijo abarca desde la 147.83.12.0 hasta la 147.83.13.255. La notación /23 indica que la máscara de red es de 23 bits o 255.255.254.0.

CIDR encamina paquetes de acuerdo con los bits de mayor orden de la dirección IP. Las entradas en la tabla de encaminamiento IP CIDR contienen una dirección IP de 32 bits y una máscara de 32 bits.

CIDR utiliza una técnica llamada creación de super-redes, de forma que una única entrada de encaminamiento cubre un bloque de direcciones sin clase. Por ejemplo, en lugar de tener cuatro entradas para un conjunto contiguo de direcciones clase C (por ejemplo: 147.83.0.0, 147.83.0.1, 147.83.0.2 y 147.83.0.3), CIDR permite anotarlas como una única entrada 147.83.0.0/22, es lo que se denomina agregación de direcciones. Para ver esta estructura hay que darse cuenta de lo siguiente:

```
147.83.0.0 = 1001 0011 . 0101 0011 . 0000 0000 . 0000 0000
147.83.0.1 = 1001 0011 . 0101 0011 . 0000 0001 . 0000 0000
147.83.0.2 = 1001 0011 . 0101 0011 . 0000 0010 . 0000 0000
147.83.0.3 = 1001 0011 . 0101 0011 . 0000 0011 . 0000 0000
máscara    = 1111 1111 . 1111 1111 . 1111 1100 . 0000 0000
```

De esta forma si una empresa requiere un rango de direcciones inferior a 254 entradas se le asigna una clase C que significa un /24, si requiere entre 255 i 510 se le asignan 2 clases C que significa un /23, si está entre 511 y 1022 se le asignan 4 clases C o un /22, etc. Debemos tener en cuenta que para que este esquema funcione las direcciones clase C que se le asignen deben ser siempre contiguas.

El RFC 1518 describe las políticas de asignación de direcciones para capitalizar la habilidad de CIDR para agregar rutas. Por ejemplo, la asignación de direcciones debería reflejar la topología física de la red; en este caso, los prefijos de direcciones IP debería corresponder a continentes o naciones. Esta técnica de agregación de rutas ha resultado en una reducción significativa en el crecimiento de las tablas de encaminamiento, observad después de la implementación CIDR. Sin la implementación de CIDR, el tamaño de la tabla de encaminamiento en el núcleo de Internet habría excedido fácilmente las 100.000 rutas en el 1996. En 1998, el tamaño de la tabla de encaminamiento utilizando el CIDR era de alrededor de 50.000 rutas.

Resolución de direcciones: protocolos ARP

En el punto anterior se supuso que un ordenador puede enviar paquetes a otro conociendo la dirección IP destino. En realidad, los paquetes IP se deben entregar finalmente por la tecnología de red subyacente, que utiliza un formato de dirección diferente. Como ejemplo concreto, suponga que la tecnología de red subyacente es Ethernet, que suele ser la situación más corriente. Recuerde que el hardware Ethernet sólo puede entender su propio formato de dirección MAC que es de 48 bits.
De esta forma, el ordenador origen debe conocer también la dirección MAC destino si quiere que el paquete llegue satisfactoriamente al destino.
¿Cómo puede un ordenador realizar la equivalencia de la dirección IP a la dirección MAC? Una solución elegante para encontrar la dirección MAC es utilizar el protocolo de resolución de direcciones ARP (Address Resolution Protocol). La principal idea se muestra en la figura 4.2.1. Suponga que H1 quiere enviar un paquete IP a H3 pero no conoce la dirección MAC de H3.

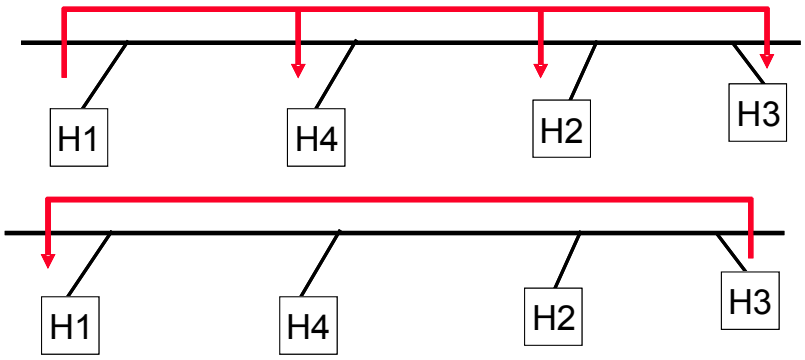

Figura 4.2.1. Ejemplo del protocolo ARP

Primero, H1 difunde un paquete de petición ARP solicitando al ordenador destino que se identifica con la dirección IP de H3 que responda. Este paquete se transmite utilizando la dirección de broadcast Etherenet (48 unos seguidos) por lo que todos los ordenadores de la red reciben el paquete. Sin embargo, solamente el ordenador referenciado, H3, responde a H1. El paquete de respuesta ARP contiene las direcciones IP y MAC de H3. A partir de ahora, H1 ya sabe cómo enviar paquetes a H3. Para evitar tener que enviar un paquete de solicitud ARP cada vez que H1 quiere enviar un paquete a H3, H1 guarda las direcciones MAC e IP de H3 en su tabla ARP almacenada en la memoria caché del ordenador. Las entradas en esta memoria están limitadas en el tiempo (entre 5 y 30 minutos), después de un periodo de no utilización se borran y si se quiere volver a enviar un paquete a la máquina cuya relación de direcciones IP y MAC ha sido borrada, deberá volver a aplicarse el protocolo ARP. Este procedimiento permite que se actualicen los cambios en las direcciones MAC de los ordenadores. La dirección MAC puede cambiar, por ejemplo, cuando la tarjeta Ethernet se rompe y hay que reemplazarla por una de nueva.

Ejercicios de autoevaluación

1. Una organización pequeña tiene una dirección de Clase C para siete redes con 24 computadoras cada una. ¿Cual es la máscara de red apropiada?

2. Se dispone del rango de direcciones 147.83.0.0/17 y se quiere subdividir la red de la empresa en 8 subredes. Indique la nueva máscara a utilizar y las

direcciones de red, de la primera máquina, de la última máquina y de multidifusión de cada una de las 8 subredes.

3. Realice una agregación CIDR de las siguientes direcciones IP /24: 128.56.25.0/24, 128.56.26.0/24, 128.56.27.0/24 y 128.56.28.0/24.

4. ¿Es posible agregar los 4 prefijos anteriores con 128.56.29.0/24 y 128.56.30.0/24?

5. Conéctese a Internet y ejecute la instrucción “netstat –r”, anote la tabla de encaminamiento presentada y analice sus campos.

Configuración remota de direcciones IP: DHCP e IP móvil

Un ordenador requiere tres elementos para conectarse a Internet: una dirección IP, una máscara de subred y la dirección de un router cercano. Cada vez que un usuario se desplaza o traslada, se tienen que reconfigurar estos elementos. En este apartado se discuten protocolos que se han desarrollado para automatizar el proceso de configuración.

Protocolo de configuración dinámica de computadoras

El protocolo de configuración dinámica de computadoras, DHCP (Dynamic Host Configuration Protocol), configura automáticamente los ordenadores que se conectan a una red TCP/IP. Un protocolo previo, el Bootstrap Protocol (BOOTP), permitía que las estaciones de trabajo sin disco arrancaran remotamente en una red. DHCP se construyó sobre la base de BOOTP y permite compatibilidad entre cliente un cliente BOOTP y un servidor DHCP. Ambos utilizan el puerto 67 de UDP para el servidor y el 68 para el cliente. DHCP tiene un uso extendido, ya que proporciona un mecanismo para asignar direcciones de red IP temporales a los ordenadores que lo solicitan. Esta capacidad se utiliza intensamente por los proveedores de servicios Internet (ISP) para maximizar el uso de sus espacios de direcciones IP limitados. Así no tienen que proveer una dirección para cada uno de sus clientes, si no sólo para aquellos que están conectados. Cada vez que un ordenador se conecta a un ISP, éste le asigna una dirección IP que tenga libre, por ello es muy usual que se nos asigne una dirección diferente en cada conexión que realicemos a nuestro ISP. El principal inconveniente es que solo pueden conectarse un determinado número de clientes, pero esto sería ya un problema de dimensionado.
Cuando un ordenador desea obtener una dirección IP, difunde un mensaje de descubrimiento de servidores DHCP en su red física. Los servidores de la red responden con un mensaje de ofrecimiento DHCP que proporciona la dirección IP y otra información de configuración como la máscara de subred o el router por defecto. Si responden varios servidores, el cliente debe seleccionar uno de los ofrecimientos y enviar al servidor seleccionado un mensaje de solicitud DHCP que sirve para indicar el servidor seleccionado. Éste enviará finalmente un paquete de confirmación (ACK) o de denegación (NACK). En el primer caso se asigna definitivamente la dirección IP que se ofreció al cliente en el primer mensaje.
Las direcciones IP se asignan por un cierto periodo de tiempo, cuando éste está a punto de expirar el cliente debe renovar la solicitud. De esta forma si una máquina no renueva su dirección se considera que se ha desconectado y el servidor recupera la dirección que le había asignado.

IP móvil

El trabajo en red móvil es una materia que está adquiriendo una importancia creciente conforme los dispositivos portátiles como los asistentes digitales personales, PDA (Personal Digital Assistant), y los ordenadores portátiles están siendo más potentes y menos caros, lo que se une a la necesidad de la gente de estar conectados en cualquier instante y en cualquier lugar en el que se hallen. El enlace entre los dispositivos portátiles y la red fija puede ser inalámbrico o fijo.
IP móvil permite que los dispositivos portátiles llamados ordenadores móviles (MH, Mobile Hosts), se muevan de un área a otra manteniendo las permitiendo la comunicación cómo si estuvieran en su propia red. Un requisito de IP móvil es que un ordenador fijo comunicándose con una MH y los dispositivos de encaminamiento intermedios no se modifiquen. Este requisito implica que una MH debe utilizar continuamente su dirección IP, incluso si se mueve a otra área. Las sesiones que estén

activas dejarán de funcionar cuando el MH salga de la red pero se restablecerán cuando entre en una de nueva.
El protocolo de IP móvil (figura 4.3.1) requiere de dos dispositivos, ubicados uno en la red origen del MH y otra en la red destino, además de un pequeño software ubicado en el propio MH:

- Home Agent (HA): Agente residente ubicado en la red origen.
- Remot Agent (RA): ubicado en la red destino.
- Mobile Agent (MA): ubicado en el MH.

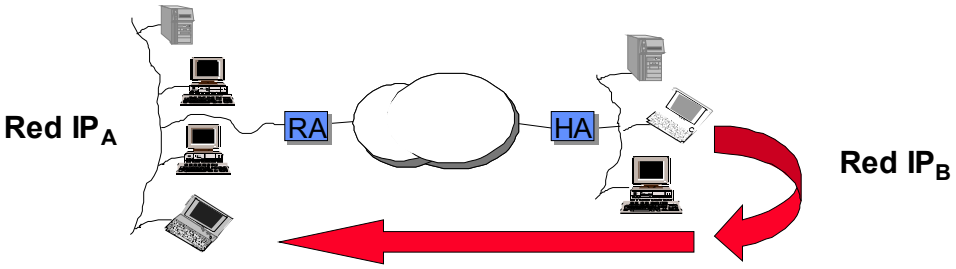

Figura 4.3.1. Elementos de IP móvil.

Cuando un ordenador (MH) sale de su red para entrar en otra, requerirá una nueva dirección para poder operar en ella. Esta dirección se denomina dirección de custodia o care-of-address, que se obtiene del RA una vez éste a validado al MH recién llegado. Para que el MH pueda recibir los paquetes que van destinados a su antigua dirección es necesario que el HA conozca su posición actual. Para ello, durante el periodo de validación, el RA se pone en contacto con el HA y le comunica la nueva posición del MH. Una vez se ha realizado esta operación, el MH ya puede empezar a recibir y enviar paquetes como si estuviera en su propia ubicación. El procedimiento esquematizado en la figura 4.3.2 es el siguiente:

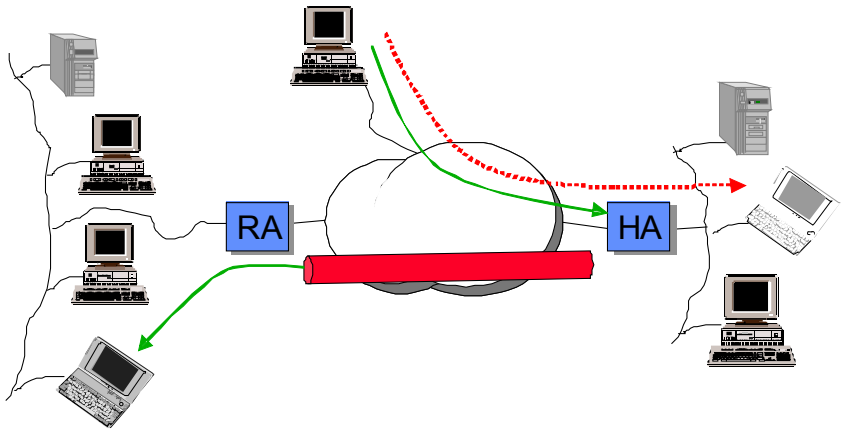

Figura 4.3.2. Funcionamiento de IP móvil.

- Cuando un ordenador cualquiera desea enviar un paquete a un MH, lo transmite a su dirección IP usual, ya que no tiene porque saber que el MH ha cambiado de posición. Este paquete es interceptado por el HA que normalmente está ubicado en el router de entrada de la red.

- A continuación este paquete debe ser enviado a la ubicación real del MH. Para ello el HA entunelará el paquete hasta el RA. Esto significa que el HA construirá un paquete IP con dirección IP destino del RA y como datos todo el paquete IP que iba dirigido al MH (es un paquete IP dentro de otro paquete IP).
- Cuando el RA reciba este paquete, quitará la cabecera IP donde aparece su dirección y lo ubicará como datos de un paquete Ethernet con dirección Ethernet destino, la del MH.
- El MH recibe un paquete Ethernet que transporta como datos el paquete IP que el ordenador origen generó, con la dirección IP del original del MH.

Si el MH desea enviar un paquete a otro ordenador, lo envía primero al RA y éste realiza el proceso inverso: lo entunela hasta el HA que lo envía como si fuera un paquete que saliera de su propia red.

IP sobre líneas serie: PPP

Una de las principales metas en el desarrollo de tecnologías de información y comunicaciones es proporcionar información remota a usuarios de una organización, manteniendo al mismo tiempo la seguridad corporativa y sin incrementar la carga del administrador de red.
El Acceso Remoto ha venido realizándose normalmente a través de emuladores de terminal o servidores de acceso. Estos dispositivos toman un flujo de bits, de por ejemplo un dispositivo RS232-C, y lo convierten en una sesión de red como el Telnet. Actualmente, un acceso simple a una máquina a través de un emulador de terminal virtual está lejos de las expectativas de los usuarios que precisan de la posibilidad de transferir ficheros, acceder a recursos a través de navegadores WWW (World Wide Web) y en definitiva, participar de las actividades de la red como si estuvieran conectados localmente. Por ello, aunque el dispositivo conectado al extremo de la línea telefónica continúa siendo un dispositivo serie, ahora requerirá inteligencia.
Necesitamos utilizar un protocolo de Nivel de Enlace que sea capaz de transportar datos de niveles superiores, y en particular que ofrezca al usuario la completa funcionalidad de la arquitectura de protocolos de Internet.
En el pasado, los fabricantes de Puentes o Routers, utilizaban protocolos propietarios para enlaces en Redes de Area Extensa. Hoy en día, esos fabricantes, en un esfuerzo para conseguir interoperabilidad entre ellos mismos, están volcándose a protocolos estandarizados como el Point-to-Point Protocol (PPP). El PPP es un estándar que permite a equipos de diferentes fabricantes, comunicarse a través de enlaces serie, líneas dedicadas, enlaces telefónicos utilizando módems o enlaces de la Red Digital de Servicios Integrados (RDSI). El PPP ha sido propuesto para reemplazar al protocolo más antiguo y "estándar de facto" conocido como SLIP (Serial Line Internet Protocol), mucho más simple pero con menos posibilidades.

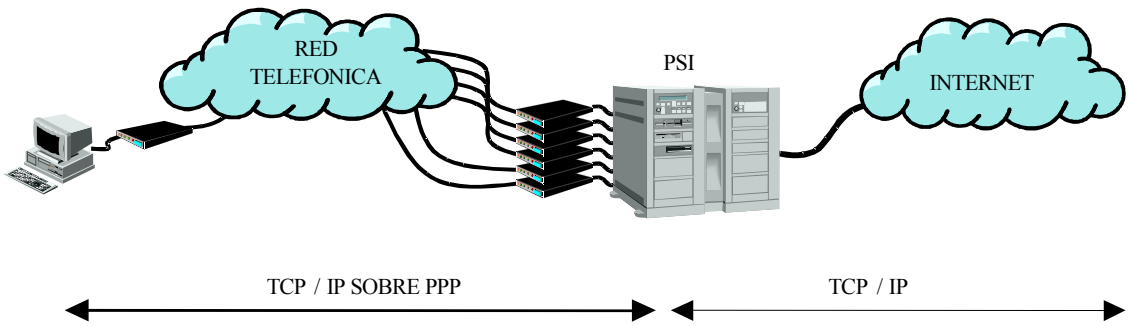

Figura 4 4.1. Utilización del PPP.

La aplicación más popular para el PPP es el acceso a Internet desde un ordenador ubicado en casa del usuario, utilizando un módem y a través de un Proveedor de Servicios Internet (PSI). En la figura 4.4.1 puede verse la situación descrita.
Este tipo de conexiones también se utilizan para conseguir acceso remoto corporativo. El hecho de llamar directamente a servidores de acceso remoto ubicados en la red de la empresa, causa un aumento de los gastos en llamadas a larga distancia y carga en la administración de la red. Asimismo, requiere que las empresas dispongan de la infraestructura de red de área extensa como módems y enlaces, y que deban velar por su seguridad.
Una forma de disminuir los costes por llamadas a larga distancia es la utilización de la Red Internet como mecanismo de transporte. De esta forma, los usuarios llaman a su Proveedor de Servicios Internet local y transmiten sus datos a través de Internet hasta su

red corporativa, tal y como ilustra la figura 4.4.2. Sin embargo, la utilización de Internet introduce algunos problemas:

- Aunque la red Internet está exclusivamente basada en la arquitectura de protocolos TCP/IP, el acceso remoto corporativo debe soportar múltiples protocolos (IPX, Apple Talk, NetBEUI, etc.). Una red Internet multiprotocolo no solucionaría este problema ya que no existe un organismo centralizado que proporcione direcciones únicas de protocolos como IPX o Apple Talk.
- Muchas empresas tienen direcciones IP que no son anunciadas en Internet, ya que no permiten acceso público. Algunas incluso utilizan el espacio de direcciones IP que no es único concebido en un principio para redes aisladas.
- Seguridad en los datos.

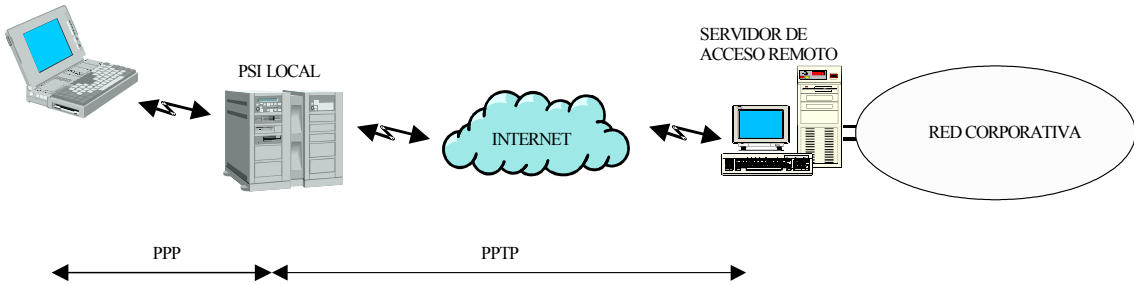

Figura 4.4.2. Acceso remoto a través de Internet.

Este problema puede resolverse entunelando el flujo de datos remoto a través de Internet. Los protocolos más utilizados para este fin son el Point-to-Point Tunneling Protocol (PPTP) y el L2TP (Layer 2 Tunneling Protocol). Estos son unos protocolos de entunelado que encapsulan el PPP. De esta forma se requieren dos conexiones: una desde el usuario remoto hasta su PSI utilizando el PPP, y otra desde el PSI hasta la red corporativa de destino utilizando el PPTP o el L2TP.
El ejemplo anterior es una de las aplicaciones de las denominadas Redes Privadas Virtuales (RPV). Una RPV conecta componentes y recursos de una red a través de otra red. Esto se consigue permitiendo al usuario entunelar sus datos a través de Internet u otra red pública de forma que los usuarios del túnel disponen de la misma seguridad y facilidades que tendrían si estuvieran en su red privada. Desde el punto de vista del usuario, la RPV es una conexión punto a punto entre su ordenador y el servidor de su red privada. La naturaleza del la red intermedia es irrelevante para el usuario ya que parece como si los datos se enviaran a través de un enlace dedicado.
Esta aplicación puede extenderse y utilizar la tecnología de las RPVs para permitir a una empresa conectar redes de varias sucursales entre sí, a través de una red pública, manteniendo las comunicaciones seguras.
Otra aplicación sería la conexión de ordenadores a través de una Intranet. En algunas redes corporativas, los datos de determinados departamentos pueden ser extremadamente confidenciales para ser transmitidos por la propia red privada. En este caso puede utilizarse una RPV para unir dos ordenadores de la misma Intranet de forma que los datos viajen encriptados por la misma

En todos los casos, la conexión segura a través de la red intermedia parece al usuario como si fuera una conexión a través de una red privada a pesar de que realmente no lo es, de aquí viene el nombre de Red Privada Virtual.
Para que una RPV sea eficiente debe permitir a los usuarios autorizados conectarse fácilmente, permitir el acceso a recursos remotos entre redes y todo ello en la más estricta seguridad. Para ello, una solución de RPV debe considerar como mínimo los siguientes puntos:
Autenticación de usuarios: la solución debe verificar la identidad de los usuarios y restringir el acceso a la RPV sólo a los autorizados. También es interesante el hecho de poder monitorizar y registrar quien se conecta y a que recursos accede.
Control de direcciones: la solución debe permitir asignar direcciones de la red privada a los clientes remotos.
Encriptación de datos: los datos que viajan por la red pública no deben ser leíbles por usuarios no autorizados.
Control de claves: la solución debe generar y refrescar claves de encriptación para el cliente y el servidor.
Soporte a múltiples protocolos: la solución debe ser capaz de soportar los protocolos más comunes como IP, IPX, NetBEUI, etc.

Conceptos de entunelado de paquetes

El entunelado es un método que utiliza la infraestructura de una red para transferir datos desde otra red a una tercera. Los datos transferidos pueden ser paquetes del mismo protocolo utilizado en la red de transporte u otro protocolo cualquiera. En lugar de transferir la trama tal y como ha sido generada en el nodo original, el protocolo de entunelado la encapsula con una cabecera adicional. Esta cabecera proporciona la información de encaminamiento necesaria para que los datos encapsulados puedan cruzar la red intermedia. Normalmente, la red intermedia suele ser la Internet aunque puede ser cualquier red pública, mientras que las redes origen y final suelen ser, o bien dos redes privadas, o un usuario remoto que accede a su red privada.
El camino lógico de la red intermedia por donde viajan los paquetes encapsulados se denomina túnel. Cuando los paquetes encapsulados llegan al nodo extremo del túnel, se desencapsulan y se redirigen a su destino final. El entunelado incluye el proceso de encapsulamiento, transmisión y desencapsulamiento de los paquetes.
Las tecnologías de entunelado ya vienen existiendo durante algún tiempo. Dos de bastante conocidas son:
Entunelado de paquetes SNA sobre redes IP: Cuando el tráfico de SNA (System Network Architecture) se envía a través de una red IP, los paquetes SNA se encapsulan en datagramas UDP (User Datagram Protocol).
Entunelado de IPX de Novel NetWare sobre redes IP: Los paquetes IPX enviados por redes IP también se encapsulan en datagramas UDP.
Las necesidades comentadas anteriormente han favorecido el desarrollo de nuevas tecnologías de entunelado en los últimos años. Estos nuevos protocolos son:
Point-to-Point Tunneling Protocol (PPTP): Desarrollado por el PPTP Fórum entre cuyos miembros se encuentran Microsoft Corporation, Ascend Communications, 3Com y ECI Telematics. Permite encriptar y encapsular tráfico IP, IPX y NetBEUI sobre datagramas IP que pueden ser enviados por Internet o cualquier otra red IP.
Layer 2 Forwarding (L2F): Protocolo propuesto por Cisco, que permite a servidores de acceso remoto enviar los datos de sus clientes telefónicos a servidores L2F atravesando redes de área extensa.
Layer 2 Tunneling Protocol (L2TP): Es una combinación de PPTP y L2F que permite encriptar y enviar trafico IP, IPX y NetBEUI sobre una red de conmutación de paquetes como IP, X.25, Frame Relay o ATM (Asynchronous Transfer Mode).

IP Security (IPSec) Tunnel Mode: Permite encriptar y encapsular datagramas IP sobre otro datagrama IP para ser enviados por Internet o cualquier otra red IP.
La tecnología de entunelado puede basarse en protocolos de entunelado de Nivel 2 o Nivel 3 del modelo de referencia OSI (Open Systems Interconnection). En los protocolos de entunelado de Nivel 2 (Nivel de Enlace) encontramos el PPTP, el L2TP y el L2F. Los tres encapsulan el paquete a transportar en una trama PPP y ésta se envía por la red de transporte. Como protocolos de entunelado de Nivel 3 (Nivel de Red) encontramos IP sobre IP e IPSec Tunnel Mode. Estos protocolos encapsulan directamente un datagrama IP sobre otro datagrama IP.
Para protocolos de entunelado de Nivel 2 como el PPTP un túnel es similar a una sesión; los dos extremos deben negociar las variables de configuración (asignación de direcciones, encriptación, compresión, ...). A lo largo de la conexión se utiliza un protocolo de mantenimiento para asegurar el correcto funcionamiento del túnel.
Las tecnologías de entunelado de Nivel 3, generalmente asumen que todas las cuestiones de configuración han sido establecidas fuera de banda, a menudo por procesos manuales. Para esos protocolos no existe la fase de mantenimiento del túnel. Una vez el túnel está establecido los datos de usuario pueden ser transmitidos utilizando el protocolo de transmisión.

PPP

El Point-to-Point Protocol es un estándar para la transmisión de paquetes sobre líneas serie. Como estándar universal, el PPP permite la interoperabilidad de equipos de diferentes fabricantes sobre enlaces serie, enlaces dedicados, enlaces que utilizan la Red Telefónica Conmutada (RTC) o la RDSI, y que pueden ser síncronos o asíncronos. El PPP fue propuesto por primera vez en 1990 para reemplazar al viejo “estándar defacto” SLIP (Serial Line Internet Protocol) y que no permitía establecer y liberar los enlaces de forma automática. A diferencia del SLIP, que sólo soportaba el IP, el PPP no está limitado en cuanto a transporte de protocolos, y puede transmitir varios protocolos simultáneamente por un solo enlace serie, eliminado la necesidad de tener un enlace separado para cada protocolo.
El PPP proporciona mecanismos para identificar el protocolo transportado, para testear el enlace y para negociar toda una serie de opciones. En el RFC 1661 se describen las tres partes que forman el PPP:

- Un método de encapsulamiento de datagramas de diferentes protocolos. El PPP utiliza una variante del HDLC (High Data Link Control) como base de su encapsulamieno.
- Un protocolo de control del enlace (LCP, Link Control Protocol), responsable de establecer, configurar y testear el enlace.
- Un grupo de protocolos de control de red (NCP, Network Control Protocols) utilizados para configurar el enlace para los protocolos de nivel de red:
    - Internet Protocol Control Protocol (IPCP)
    - OSI Network Layer Control Protocol (OSINLCP)
    - Internetwork Packet Exchange Control Protocol (IPXCP)
    - AppleTalk Control Protocol (ATCP)
    - Bridge Control Protocol (BCP)
    - DecNet Phase IV Control Protocol (DNCP)

- Banyan Vines (Vines IP) Control Protocol (BVCP)
- XNS Internet Datagram Control Protocol (XNSCP)

El PPP también dispone de facilidades para ir monitorizando el estado del enlace durante la conexión, para ello utiliza el Link Quality Monitoring Protocol (LQM) y de protocolos de autenticación, el PAP (Password Authentication Protocol) y el CHAP (Challenge Handshake Authentication Protocol). Además, permite a los fabricantes desarrollar sus propias extensiones del LCP, para tener encriptación propietaria o técnicas de autenticación y compresión no estándares.
En la figura 4.4.3 se pueden observar la relación que existe entre estos protocolos y los protocolos del nivel de red y el interfaz hardware.

Encapsulado del PPP

Para transmitir los datos del PPP se requiere de algún tipo de encapsulado que se adapte a la red de transporte. Los casos más típicos son los del PPP sobre enlaces serie utilizando un entramado del tipo de HDLC. Otros casos donde se utiliza el entramado específico de la red son el PPP sobre RDSI, X.25 o SONET/SDH.

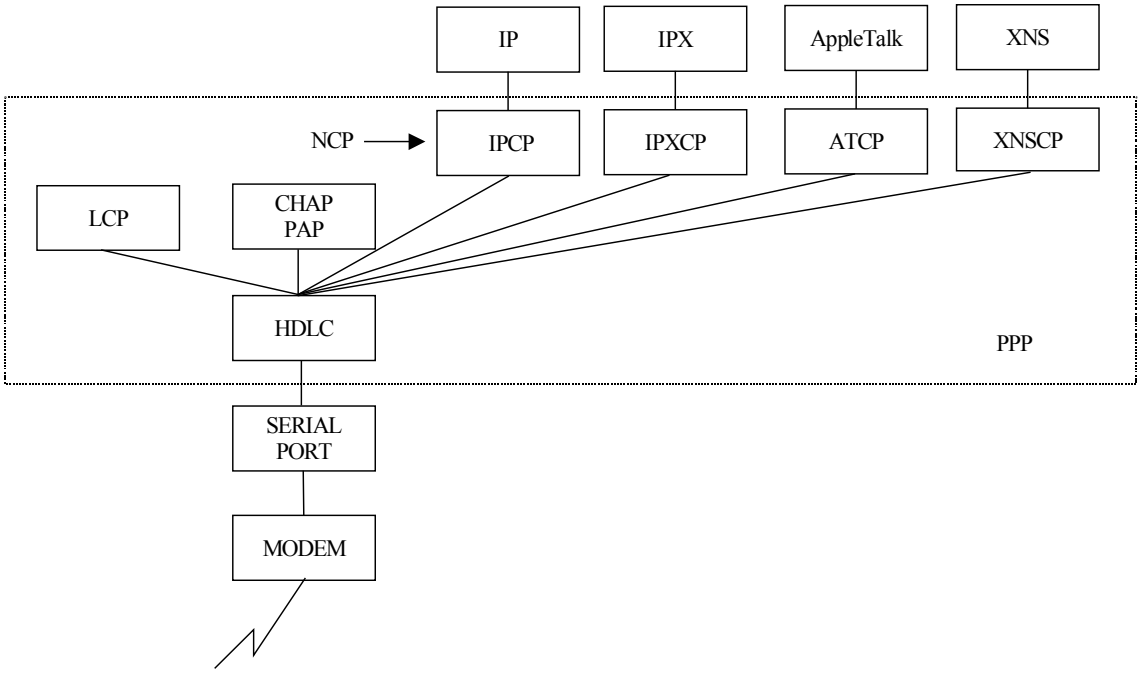

Figura 4.4.3. Protocolos en PPP.

Para realizar la práctica, utilizamos enlaces serie dedicados por lo que deberá utilizarse el entramado tipo HDLC representado en la figura 4.4.4.

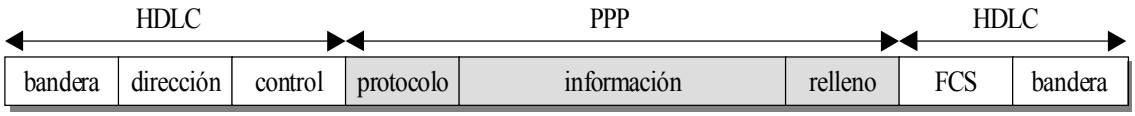

Figura 4.4.4. PPP en entramado tipo HDLC.

El **campo de bandera** es un carácter único de 8 bits (01111110), y como tal no puede utilizarse en ningún otro campo. Si aparece en algún otro campo se realiza una inserción de bit cero o "bit stuffing", que consiste en añadir un cero siempre que aparezcan 5 unos

consecutivos, el receptor siempre eliminará un cero después de 5 unos seguidos. Se utiliza para indicar el inicio y el final de cada trama, aunque sólo se necesita una bandera para separar dos tramas.
El **campo de dirección** es el carácter de 8 bits: 11111111. Esta dirección es equivalente a un broadcast, pero como sólo tenemos una máquina en el extremo opuesto del enlace serie se refiere únicamente a ella.
El **campo de control** es siempre el carácter 00000011. Finalmente, el **campo de control de errores** (Frame Check Sequence, FCS) puede ser de 16 o 32 bits, esta opción se negocia con el LCP. El FCS se calcula con todos los campos de la trama a excepción de las banderas.
En algunos casos deben transmitirse octetos que tienen un significado especial, para ello se ha definido un carácter de escape, el 7D. Por defecto los caracteres que deben transmitirse con el carácter de escape son todos los valores comprendidos entre 00 y 1F, además del propio 7D y la bandera de la trama, el 7E. Son opcionales los caracteres 7F, FF y del 80 al 9F. Para realizar la secuencia de escape de un carácter, primero se envía el carácter de escape 7D y a continuación el resultado de realizar una OR exclusiva con el carácter en cuestión y el valor fijo 20. Por ejemplo el valor 7E en el campo de datos se enviaría como 7D 5E.

Formato del paquete PPP

El PPP utiliza una técnica de encapsulación diseñada para identificar el protocolo transportado, para ello se utiliza el **campo de identificación de protocolo** que consta de 16 bits. En la tabla 4.4.1 pueden verse los identificadores de los protocolos más utilizados.
El **campo de información** contiene los datos propios del PPP. Su longitud está comprendida entre cero y "Maximum Receive Unit" (MRU) octetos, incluyendo el relleno. Por defecto el MRU es 1500 pero se puede negociar.

Internet Protocol Control Protocol (IPCP)	8021
Internetwork Packet Exchange Control Protocol (IPXCP)	802B
AppleTalk Control Protocol (ATCP)	8029
XNS Internet Datagram Control Protocol (XNSCP)	8025
Internet Protocol (IP)	0021
OSI Network Protocol	0023
AppleTalk	0029
Novell IPX	002B
Van Jacobson Compressed TCP/IP	002D
Link Control Protocol (LCP)	C021
Password Authentication Protocol (PAP)	C023
Link Quality Report (LQR)	C025
Challenge Handshake Authentication Protocol (CHAP)	C223

Tabla 4.4.1. Códigos de identificación de Protocolo.

Se ha considerado la posibilidad de que en una transmisión, el campo de información pueda ser rellenado (mediante el **campo de relleno**) hasta el MRU. Sin embargo, el PPP no indica como debe hacerse, es responsabilidad de cada protocolo de nivel de red el distinguir los bytes de relleno de los de información.

Operativa del enlace PPP

A diferencia del SLIP, en el PPP, antes de transferir datos, cada extremo manda una serie de paquetes para comprobar la operativa del enlace y, si ésta es correcta se utilizan los protocolos de control de red NCPs para configurarlo.
El procedimiento es el siguiente (figura 4.4.5): por defecto el PPP se encuentra en estado de "MUERTO", el PPP está inactivo esperando alguna señal del nivel físico para darse de alta ("ARRIBA"), un caso típico podría ser la detección de portadora en un enlace serie. Una vez se ha asegurado que el enlace está operativo, se pasa al estado de "ESTABLECIDO". En este estado debe establecerse la comunicación entre ambos extremos con el intercambio de una serie de paquetes de configuración del LCP. A continuación, si la autenticación ha sido habilitada, uno de los extremos habrá solicitado el uso de un protocolo de autenticación, el PAP o el CHAP. Si el proceso de autenticación ha sido correcto ("CORRECTO") o no ha sido solicitado ("NADA") se pasa al estado de "RED". En este estado se utilizarán los protocolos NCP para configurar el enlace con las características requeridas por los protocolos de nivel de red. En nuestro caso utilizaríamos el IPCP ya que deseamos transmitir datagramas IP por el enlace. Si el NCP utilizado ha podido configurarse correctamente se pasa al estado de "ABIERTO" donde se pueden transmitir los datos del protocolo de red. Para terminar la comunicación se pasa al estado de "TERMINAR" donde existe un intercambio de paquetes para cerrar el enlace adecuadamente. Además, en cualquier momento puede producirse un fallo que terminaría automáticamente la conexión.

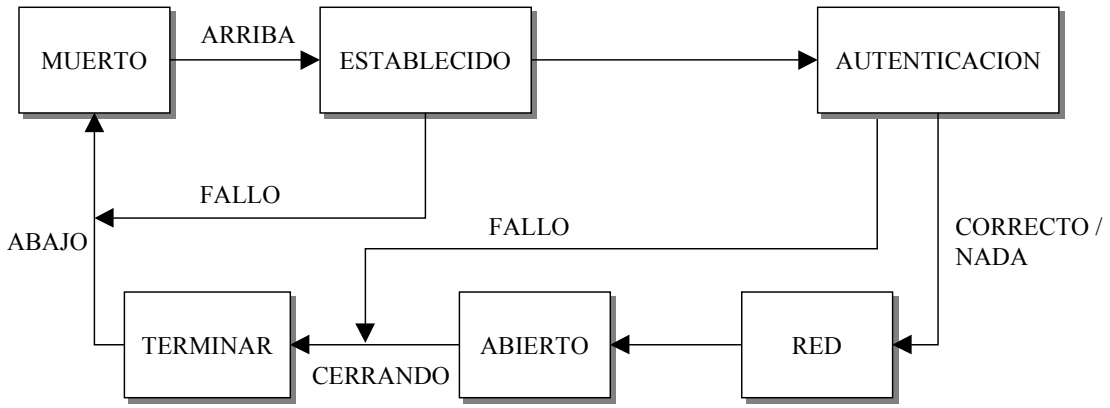

Figura 4.4.5. Diagrama de estados simplificado del PPP

Link Control Protocol (LCP)

El LCP tiene tres clases de paquetes:

- Paquetes de configuración del enlace, para establecer y configurar el enlace.
- Paquetes de terminación del enlace.

– Paquetes de mantenimiento del enlace

Los paquetes del LCP tienen el formato general mostrado en la figura 4.4.6, donde el **campo de código** de 8 bits identifica el tipo de paquete con los valores mostrados en la tabla 4.4.2. El **campo de identificador** (8 bits) se utiliza para poder relacionar los paquetes de solicitud con sus respectivas respuestas. El **campo de longitud**, que está formado por 16 bits, indica la longitud total del paquete LCP. Finalmente, el **campo de datos** es de longitud variable y depende del tipo de paquete.

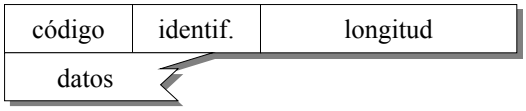

Figura 4.4.6. Formato general de los paquetes LCP.

Solicitud de configuración LCP (Configure Request)

Un paquete de solicitud de configuración (Configure Request) es enviado por las estaciones que desean cambiar algún parámetro del enlace. El campo de datos del paquete LCP tiene la estructura mostrada en la figura 4.4.7.

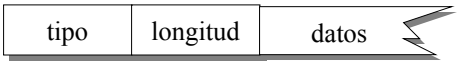

Figura 4.4.7. Campo de datos del paquete LCP con el código Configure Request.

El **campo de tipo** contiene uno de los valores presentados en la tabla 4.4.3 indicando el código del parámetro que se desea configurar. El **campo de longitud** indica la longitud total de la opción incluyendo el campo de tipo y el **campo de datos** contiene información específica de la opción negociada. Para cada opción negociada, la máquina remota debe enviar una respuesta.

Código	Descripción
1	Configure Request
2	Configure Positive Acknowledgement (ACK)
3	Configure Negative Acknowledgement (NACK)
4	Configure Reject (REJECT)
5	Terminate Request
6	Terminate Acknowledgement
7	Code Reject
8	Protocol Reject
9	Echo Request
10	Echo Reply
11	Discard Request
12	Identification
13	Time Remaining

Tabla 4.4.2. Códigos de los paquetes LCP.

Maximum Receive Unit (MRU): Indica el tamaño máximo de paquete que el receptor está dispuesto a recibir. La longitud total del paquete es de 4 bytes, 2 de los cuales

indican el valor del MRU. Aunque es posible indicar la longitud máxima del paquete, todas las implementaciones del PPP deben poder soportar una longitud mínima de 1500 bytes.

Código	Descripción
0	Reservado
1	Maximum Receive Unit (MRU)
3	Authentication Protocol
4	Quality Protocol
5	Magic Number
7	Protocol Field Compression
8	Address-and-Control Field Compression
9	FCS Alternatives
10	Self Describing Padding
13	Call Back
15	Compound Frames
17	Multi-Link MRRU
18	Multi-Link Short Sequence Number Header
19	Multi-Link Endpoint Discriminator

Tabla 4.4.3. Tipos más utilizados del paquete LCP Configure Request.

Protocolo de autenticación: Por defecto no se utiliza ningún mecanismo de autenticación para establecer la comunicación, si un extremo requiere autenticación debe notificarlo al extremo opuesto y éste tendrá la obligación de realizarlo. El PPP permite varios protocolos de autenticación. Los más usuales son el PAP (código C0 23) y el CHAP (código C2 23 05 para el estándar MD5 CHAP y C2 23 80 para el Microsoft CHAP), pero pueden utilizarse otros como el EAP (Extensible Authentication Protocol, código C2 27) o el SPAP (Shiva-PAP código C0 27). Cada extremo propone el que quiere utilizar y no es necesario que la autenticación en los dos sentidos sea la misma. Si un extremo requiere autenticación y el opuesto rechaza la opción, el primero termina la comunicación.
El formato del paquete se muestra en la figura 4.4.8. Si el protocolo propuesto requiere la transmisión de datos adicionales al código del protocolo, es posible añadirlos en el campo de datos de longitud variable.

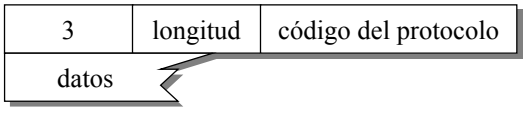

Figura 4.4.8. Campo de datos del paquete LCP con el código Configure Request y opción Authentication Protocol.

Protocolo de calidad: Igual que con la autenticación, el protocolo de monitorización de la calidad del enlace (LQM, Link Quality Monitoring) está deshabilitado por defecto. En algunos enlaces, particularmente los que tienen grandes tasas de error, puede ser interesante determinar la frecuencia en que el enlace se cae.
En la figura 4.4.9 se muestra el formato del paquete del protocolo de calidad de enlace del LCP. Para esta tarea pueden utilizarse diferentes protocolos, aunque el “Link Quality

Report protocol" está estandarizado como parte del PPP y se define en el RFC 1333. El código del protocolo se indica con los 16 bits que vienen a continuación de la longitud del paquete. Para el Link Quality Report protocol se utiliza el código C025. Después del código del protocolo viene un campo de longitud variable que depende del protocolo de calidad utilizado.

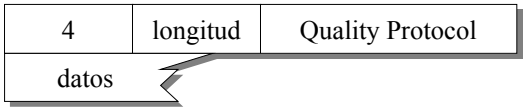

Figura 4.4.9. Campo de datos del paquete LCP con el código Configure Request y opción Quality Protocol.

Número Mágico: El número mágico es un identificador único para describir el puerto de comunicación del PPP, se utiliza para distinguir los dos extremos y detectar errores como lazos cerrados. Cada extremo de una conexión elegirá su propio número mágico de 32 bits que puede ser cualquiera siempre y cuando sea único en el enlace. En la figura 4.4.10 puede observarse la forma del paquete utilizado para negociarlo.

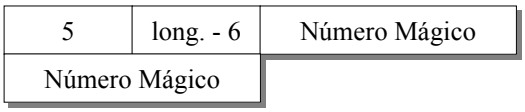

Figura 4.4.10. Campo de datos del paquete LCP con el código Configure Request y opción Magic Number.

Compresión de campo de protocolo y campos de dirección y control: En enlaces a baja velocidad es deseable transmitir los datos con la mínima carga de información de control. El LCP permite negociar dos tipos de compresión que consisten en no enviar ciertos campos que son siempre iguales.
El primer tipo de compresión es el de los campo de dirección y de control (Address-and-Control-Field Compression, ACFC) del entramado HDLC (figura 4.4.4). El segundo tipo es la compresión del campo de protocolo del entramado PPP (Protocol Field Compression, PFC). En ambos casos, la compresión siempre tiene lugar para paquetes normales de datos. En los paquetes de configuración de LCP nunca se utiliza compresión.
El formato de los paquetes de configuración de las compresiones pueden verse en la figura 4.4.11.

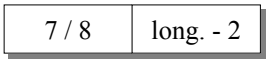

Figura 4.4.11. Campo de datos del paquete LCP con el código Configure Request y opción PFC o ACFC.

Alternativas de código de corrección de errores: En enero del 1994, el PPP fue mejorado por el RFC 1570 definiendo 4 extensiones a las opciones de configuración del LCP. El hecho de permitir diferentes tipos de códigos correctores o detectores de errores (Frame Check Sequence, FCS) es una de ellas.

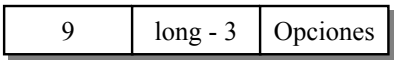

Figura 4.4.12. Campo de datos del paquete LCP con el código Configure Request y opción FCS Alternatives.

La negociación del FCS se realiza durante el establecimiento y el tipo de FCS negociado se utilizará durante las fases de autenticación y de transmisión de datos, pero durante la fase de negociación del LCP debe utilizarse el FCS estándar. El formato del paquete es el de la figura 4.4.12.
El campo de opciones sirve para indicar el tipo de FCS deseado. Su valor es una OR lógica de:

- 1: FCS nulo. Los FCS son considerados datos de relleno y se descartan.
- 2: FCS de 16 bits del CCITT. Es el FCS utilizado en la mayoría de enlaces HDLC.
- 4: FCS de 32 bits del CCITT. Representa un mecanismo opcional de FCS que utiliza secuencias de 32 bits.

Relleno autodescriptivo: En algunas ocasiones se requiere que un paquete tenga una longitud determinada, típicamente una potencia de dos. En estos casos se añaden los octetos de relleno 01 02 03 04 ... hasta la frontera natural del paquete. El receptor, si ha negociado esta opción, comprobará si el último octeto del paquete está dentro del rango 01 hasta el valor máximo de relleno (MPV, Maximum Pad Value), si se da esta circunstancia ira eliminando los octetos hasta llegar al 01 o a uno que esté fuera de rango, en este caso devolverá un error y descartará la trama. Si los datos terminan exactamente en la frontera natural del paquete y con un octeto comprendido entre 01 y MPV, se deberá añadir un relleno hasta la siguiente frontera posible del paquete.
La opción de Self Describing Padding del LCP sirve para negociar el MPV (figura 4.4.13).

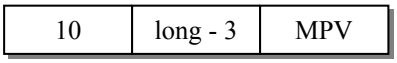

Figura 4.4.13. Campo de datos del paquete LCP con el código Configure Request y opción Self Describing Padding.

Call Back: Esta opción permite que un extremo solicite que el extremo opuesto le llame una vez concluida una primera conexión. Esta opción puede utilizarse como mecanismo de seguridad o para repercutir el coste de la llamada al extremo opuesto.
El formato de la opción se representa en la figura 4.4.14, donde el **campo de operación** se usa para indicar el contenido del **campo mensaje**, y puede tomar los siguientes valores:

- 0: La localización se determina a través del mecanismo de autenticación.
- 1: Número de teléfono a llamar
- 2: Identificador de localización. En este caso se consigue el número de teléfono de una base de datos.
- 3: Un número estandarizado que define la localización del llamante.
- 4: Un nombre que permite conocer la localización del llamante.

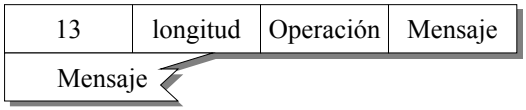

Figura 4.4.14. Campo de datos del paquete LCP con el código Configure Request y opción Call Back.

Tramas compuestas: Para mejorar la eficiencia del PPP, el RFC 1570 introdujo el concepto de tramas compuestas, permitiendo que varios paquetes PPP fueran encapsulados en una sola trama (en nuestro caso HDLC). La figura 4.4.15 muestra el tipo de paquete de configuración para negociar esta opción.

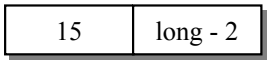

Figura 4.4.15. Campo de datos del paquete LCP con el código Configure Request y opción Compound Frames.

Multi-Link Maximum Receive Recontructed Unit (MRRU), Multi-Link Short Sequence Number Header Format, Multi-Link Endpoint Discriminator Option: Estas tres opciones, descritas en el RFC 1990, forman la base para el protocolo Multi-Link PPP, que permite el uso de varios enlaces físicos para una sola conexión PPP.

Confirmación de solicitud LCP (Configure ACK, Configure NACK y Configure Reject)

El formato de los paquetes de confirmación de configuración: Configure Positive Acknowledgement (ACK), Configure Negative Acknowledgement (NACK) y Configure Reject (Reject), es el mismo para todos (figura 4.4.16).
Un ACK se envía siempre que todas las opciones de un paquete Configure Request sean reconocidas y aceptadas. En este caso el **campo de código** contiene el valor 2 y el **campo de opciones** contiene la lista de las opciones reconocidas positivamente. El **campo identificador** contiene el mismo valor que el identificador del paquete Configure Request del cual estamos reconociendo las opciones. Finalmente, el **campo longitud** contiene la longitud total del paquete LCP.

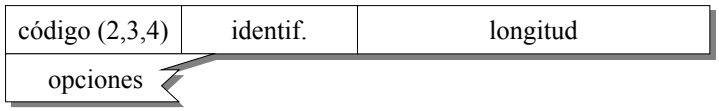

Figura 4.4.16. Formato de los paquetes LCP ACK, NACK y Reject.

Un NACK se envía cuando todas las opciones del paquete Configure Request son reconocidas pero una o más opciones no son aceptadas. El paquete Configure NACK utiliza el **código** 3 y en el **campo de opciones** se incluyen las opciones que no son aceptables. Los **campos de identificador y longitud** son iguales que en Configure ACK.
El paquete Configure Reject se envía cuando una o más opciones del paquete Configure Request no son reconocidas. También se utiliza para rechazar aquellas opciones que no contienen campo de datos, es decir son booleanas, se utilizan o no se utilizan (un ejemplo seria la opción de compresión de campo de protocolo, PFC). El **código** para el paquete Configure Reject es el 4 y en el **campo de opciones** se incluyen aquellas que son rechazadas. Los **campos de identificador y longitud** son iguales que en Configure ACK.
La recepción de un NACK o un Reject no implica que las opciones del paquete Configure Request original que no se hayan rechazado queden confirmadas por defecto.

Después de la recepción de un NACK o un Reject se deberá emitir otro Configure Request que no contenga las opciones rechazadas y esperar a un Configure ACK.

Terminación de una conexión

Un puerto puede solicitar la terminación de una conexión de forma ordenada mediante el envío de un paquete LCP Terminate Request. No existe negociación posible ante este paquete, el receptor debe enviar siempre un Terminate Ack como respuesta. Los puertos que no reciban un reconocimiento a su solicitud de terminación irán enviando Terminate Requests hasta que se reciba un reconocimiento o expire algún temporizador.
El formato general de estos paquetes es el de la figura 4.4.17, donde el **código** es 5 para el Terminate Request y 6 para el Terminate Ack. El **campo de identificador** se utiliza para poder relacionar los paquetes de solicitud con sus respectivas respuestas. El **campo longitud** indica la longitud total del paquete LCP. Finalmente, en algunas implementaciones del PPP se permite poner una cadena de caracteres ASCII (**campo de datos**) al final del paquete para indicar el motivo de la finalización de la conexión.

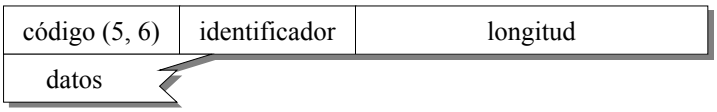

Figura 4.4.17. Formato de los paquetes LCP Terminate Request y Terminate Ack.

Rechazo de código LCP

En la mayoría de protocolos existe un campo que identifica la versión del protocolo utilizado a efectos de distinguir entre formatos de los paquetes. El PPP, para ahorrar información de control no dispone de ningún campo de este tipo, por lo que viejas implementaciones del PPP pueden no soportar algunos tipos de paquetes. En previsión de que esto ocurra se ha definido el paquete de Code Reject, que es utilizado para informar que el código del último paquete recibido no es reconocido.
La figura 4.4.18 nos muestra su formato. El **código** del paquete es 7, el **identificador** es un número único escogido por el puerto que manda el paquete, la **longitud** indica la longitud total del paquete LCP y a continuación se añade el paquete cuyo código es irreconocible.

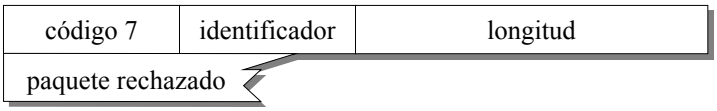

Figura 4.4.18. Formato paquete LCP Code Reject.

Rechazo de Protocolo

Si un puerto recibe un paquete PPP con un protocolo desconocido, lo rechazará con el paquete Protocol Reject. El campo de **código** del paquete mostrado en la figura 4.4.19, es en este caso 8. Los **campos de identificación y longitud** tienen el mismo significado que en los casos anteriores. Se incluye también un campo con el **código del protocolo rechazado** y una copia del paquete rechazado en el **campo de información de rechazo**.

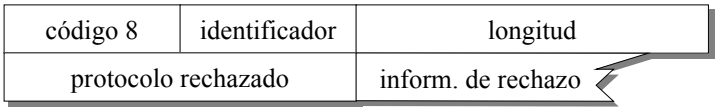

Figura 4.4.19. Formato del paquete LCP Protocol Reject.

Solicitud y respuesta de eco

El LCP tiene una operación de eco similar a la del ICMP (Internet Control Message Protocol). Estos paquetes se utilizan para realizar tests de los enlaces. Al igual que en los ICMP, cuando un puerto recibe un paquete de Echo Request (**código** 9) debe responder con un Echo Reply (**código** 10), en este caso el **identificador** del paquete debe ser el mismo que el recibido en el paquete de solicitud.
El **número mágico** se utiliza para identificar de forma única el puerto que emite el paquete y debe ser previamente negociado. En caso de que no se haya negociado, el campo se rellena con ceros. El **campo de datos** es utilizado por el emisor, el receptor no interpreta los datos, solamente los copia en el paquete Echo Reply.

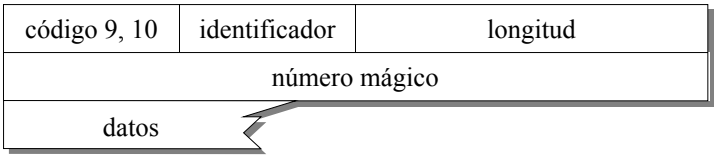

Figura 4.4.20. Formato de los paquetes LCP Echo Request y Echo Reply.

Solicitud de descarte

Este tipo de paquetes también se utilizan para sondear enlaces. Cuando se recibe un paquete de Discard Request es descartado inmediatamente, generalmente se utilizan para cargar enlaces con datos que no influyan en el resto de la red. Los campos del paquete (figura 4.4.21) tienen el mismo significado que en paquete de Echo Request.

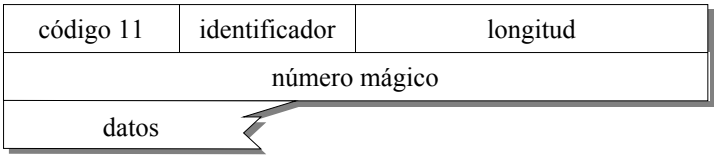

Figura 4.4.21. Formato del paquete LCP Discard Request.

Identificación de LCP

La identificación de LCP es otra de las nuevas opciones descritas en el RFC 1570, se utiliza para identificar un puerto PPP y normalmente se utiliza antes de que el PPP pase al estado de "Abierto". El formato del mensaje, figura 4.4.22 es similar al 4.4.21, pero el **campo de datos** transporta la información específica de la implementación de identificación.

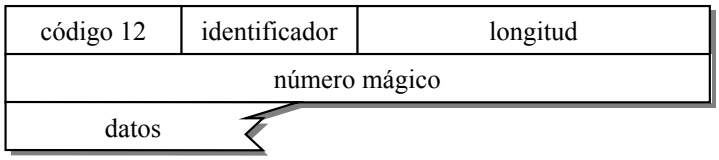

Figura 4.4.22. Formato del paquete LCP Identification.

Tiempo restante

Opción también descrita en el RFC 1570, no existe negociación para esta opción ni tampoco respuesta. El mensaje de LCP Time Remaining permite a un sistema PPP notificar al extremo opuesto que está sujeto a algún tipo de control administrativo y que va a finalizar la conexión dentro un intervalo de tiempo. Estos mensajes son tratados según la implementación del PPP, una opción es presentarlo al usuario.

El formato de paquete se representa en la figura 4.4.23 y tiene una estructura similar a los anteriores. cuatro octetos para el número mágico, cuatro octetos para definir un número entero representando el número de segundos que faltan para cerrar el enlace y un texto de longitud variable.
Cabe destacar que este paquete no cierra el enlace, una vez expirado el tiempo, el puerto que desee cerrar la conexión deberá enviar paquetes de solicitud de terminación.

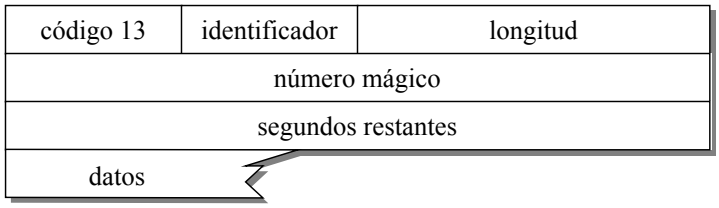

Figura 4.4.23. Formato del paquete LCP Time Remaining .

Protocolos de autenticacion del PPP

El RFC 1334 define dos protocolos de autenticación para utilizar en el PPP: el Password Authentication Protocol (PAP) y el Challenge Handshake Authentication Protocol (CHAP). De todas formas, aunque estos protocolos son los más utilizados, la naturaleza abierta del PPP permite el uso de otros protocolos.

Password Authentication Protocol (PAP)

El PAP es un método simple mediante el cual un puerto puede identificar el extremo opuesto de la comunicación. La autenticación se realiza cuando el proceso de establecimiento del enlace se ha completado satisfactoriamente y consiste en el envío de unos datos y la recepción de la confirmación positiva o negativa, en este último caso la conexión finalizaría. Por ello se requieren tres tipos de paquetes: el Authenticate Request, el Authenticate Ack y el Authenticate Nack. Con el PAP la contraseña viaja en claro por el enlace.
Authenticate Request: Es una solicitud de autenticación y se utiliza para iniciar el proceso. Un puerto envía un paquete PAP con su identificador y su contraseña, y lo va reenviando a intervalos regulares hasta que recibe confirmación o se corta el enlace. El formato de este paquete se representa en la figura 4.4.24.
Para este paquete el **código** es 1, el **identificador** un valor único para poder cotejar la solicitud con la respuesta, a continuación la **longitud total** del paquete, un octeto con la **longitud de la identificación** del puerto y un campo variable con esta **identificación**, otro octeto para indicar la **longitud de la contraseña** del puerto y el campo de longitud variable con la **contraseña**.

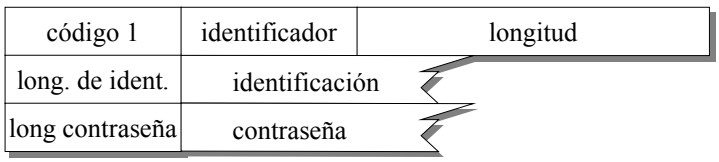

Figura 4.4.24. Paquete PAP de Authentication Request.

Authenticate Ack y Authenticate Nack: La respuesta a una solicitud de identificación puede ser positiva si la identificación y la contraseña se ha reconocido o negativa si ha fallado, en este caso el enlace se cerrará con un paquete LCP Terminate Request.
El formato para ambos paquetes es el representado en la figura 4.4.25. Para estos paquetes el **código** es 2 para un Ack y 3 para un Nack. Es posible añadir un **campo de texto** al paquete pero es una opción específica de la implementación del PPP.

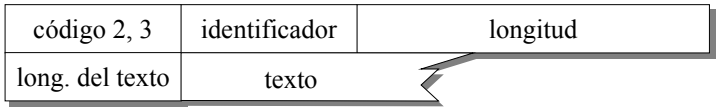

Figura 4.4.25. Paquete PAP de Authentication Ack y Authentication Nack.

Challenge Handshake Authentication Protocol (CHAP)

A diferencia del PAP que sólo permite un mecanismo simple de autenticación, el CHAP proporciona un sistema más seguro. El CHAP utiliza un mecanismo con un intercambio de tres mensajes, y emplea una contraseña conocida sólo por los puertos involucrados y que viaja encriptada por el enlace. Además, se pueden realizar comprobaciones en cualquier momento de la duración de la conexión.
El CHAP define 4 tipos de paquetes para realizar la autenticación:
Paquete Challenge: El CHAP empieza cuando un puerto empieza a enviar paquetes de Challenge repetidamente, hasta que recibe una respuesta o el enlace se cierra. Los paquetes de Challenge tienen el formato presentado en la figura 4.4.26. El **código** es en este caso el 1, el **identificador** se usa para relacionar comandos con respuestas y el **campo de longitud** para indicar la longitud total del paquete CHAP. A continuación viene un campo de 8 bits que indica la **longitud del valor** en octetos, y después el propio **valor** que tiene longitud variable. Finalmente, el **campo nombre** sirve para identificar el sistema que ha transmitido el paquete.

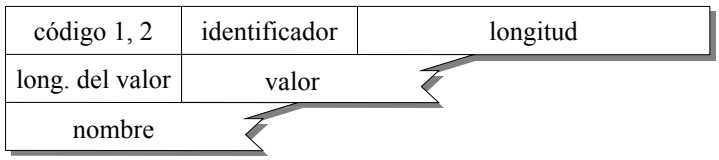

Figura 4.4.26. Paquete CHAP de Challenge y Response.

Paquete Response: Como respuesta a un paquete Challenge, un puerto debe enviar un paquete de Response. En este caso el formato es el mismo que el anterior pero el **código** es 2. Los campos tienen el mismo significado exceptuando el **campo valor** donde se incluye el resultado de realizar una operación de *hash* con el identificador concatenado con la contraseña y el valor del paquete Challenge recibido.
Paquetes de Success y Failure: Si el valor recibido como respuesta es el que el puerto esperaba debe enviarse una confirmación positiva (Success) y si es erróneo una confirmación negativa (Failure) y a continuación cerrar el enlace con un paquete LCP Terminate Request. El formato de estos paquetes está representado en la figura 4.4.27, el **código** es 3 para el Success y 4 para Failure, el **campo de mensaje** contiene información específica de la implementación.

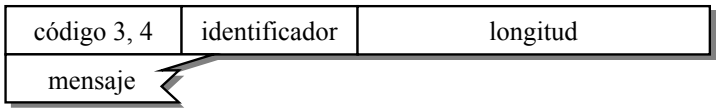

Figura 4.4.27. Paquete CHAP de Success y Failure.

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP).

El MS-CHAP es un mecanismo de autenticación encriptada muy similar al CHAP. Al igual que éste, el servidor de acceso envía una palabra al cliente remoto. El cliente remoto debe devolver el nombre de usuario y el resultado de codificar la palabra indicada por el servidor con la contraseña encriptada del usuario. Este sistema añade un mayor nivel de seguridad porque el servidor almacena las contraseñas de los usuarios

encriptadas en lugar de texto plano como hace el CHAP. El MS-CHAP también proporciona corrección de errores, expiración de contraseña y mensajes encriptados entre el cliente y el servidor que permiten a los usuarios modificar sus contraseñas.

PPP Link Quality Monitoring (LQM)

En algunos casos resulta interesante tener una idea de la tasa de errores que introduce el enlace. Para ello se desarrolló el protocolo de monitorización de la calidad del enlace (Link Quality Monitoring, LQM) definido en el RFC 1333. Este protocolo realiza un intercambio de información sobre los errores detectados en el enlace. Para ello necesitará una serie de contadores, tanto de paquetes transmitidos como de recibidos, correctos e incorrectos. La información se transmite en los denominados Quality Reports.
El hecho de medir la calidad del enlace, es opcional y se negocia con un Configure Request de código igual a 4, y si se utiliza el protocolo de informes de calidad (Quality Reports) se envía el código de protocolo de calidad C025. El campo de datos, de 32 bits de longitud, se rellena con el periodo máximo entre informes de calidad de enlace expresada en fracciones de 1/100 segundos.
Por supuesto, si el enlace funciona correctamente, los informes de calidad añaden una carga extra al mismo, pero cuando existe un problema pueden ayudar en gran medida a determinar su origen y corregirlo.
Link Quality Report (LQR): el informe de calidad viene encapsulado dentro de un paquete PPP, con número de protocolo C025. La parte de información contiene 12 campos diferentes de 32 bits cada uno de ellos, que informan sobre:

- El número mágico.
- PeerInLQR: Número de LQR recibidos por el puerto.
- PeerInPackets: Número de paquetes recibidos por el puerto.
- PeerInDiscards: Número de paquetes que deben descartarse (Discard Request) recibidos por el puerto.
- PeerInErrors: Número de errores recibidos por el puerto.
- PeerInOctets: Número de octetos recibidos por el puerto.
- PeerOutLQRs: Número de LQR enviados por el puerto.
- PeerOutPackets: Número de paquetes enviados por el puerto.
- PeerOutOctets: Número de octetos enviados por el puerto.
- LastOutLQR: Contiene el valor de PeerOutLQR contenido en último informe recibido del otro extremo.
- LastOutPackets: Contiene el valor de PeerOutPackets contenido en último informe recibido del otro extremo.
- LastOutOctets: Contiene el valor de PeerOutOctets contenido en último informe recibido del otro extremo.

Multilink PPP (MPPP)

Algunos tipos de redes como la RDSI permiten asignar ancho de banda bajo demanda, es decir utilizar varios enlaces simultáneamente según las necesidades del usuario. En el caso de la RDSI, un enlace básico proporciona 2 canales B de 64 Kbps cada uno y uno

primario, 30 canales B. El MPPP permite gestionar la utilización de varios de estos canales para una sola comunicación.
Cuando se dispone de varios enlaces, debemos asegurar una utilización óptima distribuyendo el tráfico equitativamente entre ellos. El problema radica en como se encaminan los diferentes paquetes por los enlaces, para ello hemos de tener en cuenta que los paquetes pueden ser de tamaño variable y que los enlaces pueden tener diferentes velocidades.
El RFC 1717 define un mecanismo de transmisión de paquetes por enlaces múltiples fragmentándolos en el emisor y reensamblándolos en el receptor. Cuando se utiliza el MPPP debe añadirse una cabecera adicional (figura 4.4.28) que controla este proceso de fragmentación y reensamblado de paquetes.
El primer campo del paquete MPPP es el **protocolo** utilizado, en este caso el mismo MPPP con el código 003D. Existen dos tipos de cabeceras una corta y otra larga que se diferencian únicamente por disponer, la versión larga, de 4 banderas más que hasta el momento no se utilizan, y un número de secuencia de 24 bits en lugar de uno de 12. Las banderas utilizadas son el **bit B** de inicio (beginning) y el **bit E** de final (ending), utilizadas para indicar el primer y último fragmentos de un paquete PPP. El **número de secuencia** sirve para indicar la posición del fragmento dentro del paquete original.
El protocolo LCP permite negociar la utilización de uno u otro tipo de paquetes MPPP. Por defecto se utiliza el paquete largo, si se desea utilizar el corto debe negociarse con la opción “Short Sequence Number Header Format”. Para notificar el deseo de un extremo de utilizar el MPPP al otro extremo se utiliza la opción “Multi-Link Maximum Receive Reconstructed Unit (MRRU)”. Esta opción negocia además, el tamaño máximo que puede tener un paquete reconstruido, el tamaño máximo de un fragmento viene impuesto por la Maximum Receive Unit (MRU) del enlace.

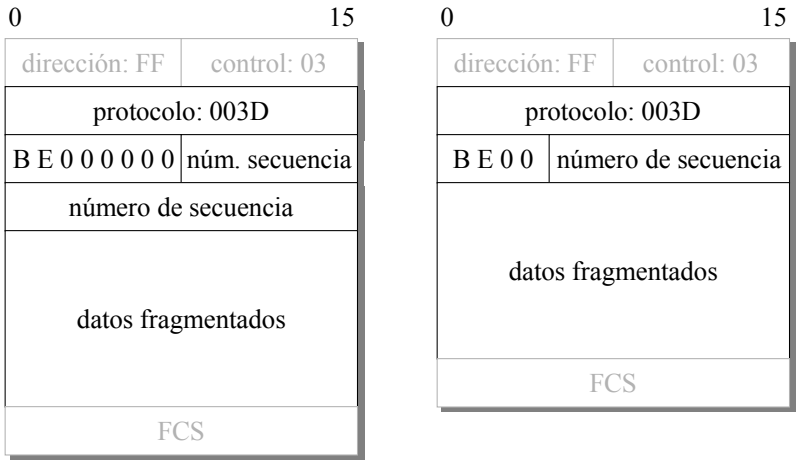

Figura 4.4.28. Formato de un paquete fragmentado MPPP.

La tercera opción del LCP relacionada con el MPPP es el “End-Point Discriminator”. Este es un valor adicional para identificar un puerto de PPP y puede utilizar direcciones IP, direcciones MAC, direcciones asignadas localmente, etc.

Internet Protocol Control Protocol (IPCP)

El PPP define varios protocolos de control de red (NCP) diseñados para configurar el funcionamiento del enlace que deberá transportar el protocolo de Nivel de Red. En esta sección describiremos el NCP utilizado para configurar el protocolo IP: el IPCP.

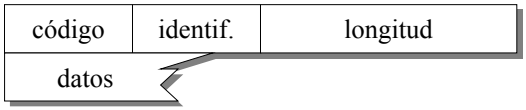

Figura 4.4.29. Formato general de los paquetes IPCP.

El IPCP estandarizado por el RFC 1332, utiliza los mismos mecanismos que el LCP, con los mismos tipos de paquetes. El código del protocolo IPCP que viaja en el campo de protocolo del encapsulamiento PPP es el 8021, y su formato es el que se presenta en la figura 4.4.29.
El **código** identifica el tipo de paquete y puede ser:

- 1: Configure Request
- 2: Configure ACK
- 3: Configure NACK
- 4: Configure Reject
- 5: Terminate Request
- 6: Terminate ACK
- 7: Code Reject

El **identificador, la longitud y los datos** funcionan exactamente igual que el LCP, solamente varían los tipos de opciones que deben negociarse mediante los paquetes de Configure Request. Una vez se han negociado con éxito todas las opciones, son los propios paquetes IP los que se encapsulan dentro del campo de datos del PPP, con el código del protocolo correspondiente al IP (0021).

Opciones de configuración del IPCP

Actualmente existen 3 opciones básicas de configuración del IP, aunque una de ellas es obsoleta y se desaconseja su uso. Asimismo, existen otras opciones específicas para equipos informáticos propietarios. En este punto vamos a describir las tres opciones generales.

- **IP-Addresses:** Esta opción utilizada para configurar las direcciones IP de los dos puertos de una conexión está actualmente obsoleta pero puede utilizarse por compatibilidad con algunos sistemas. En su lugar debe utilizarse la opción IP-Address.
- **IP-Compression-Protocol:** Por defecto el protocolo IP sobre el PPP no utiliza compresión. Cuando se requiere la compresión puede negociarse con el IPCP.

  El formato de la opción IPCP es el presentado en la figura 4.4.30. Como mínimo tiene 4 octetos de longitud: el **tipo** de opción negociada, en este caso 2, la **longitud** de la opción que depende del protocolo utilizado, el **código del protocolo de compresión** y finalmente un **campo de datos** que se utiliza sólo en aquellos casos que el protocolo de compresión requiere datos adicionales.

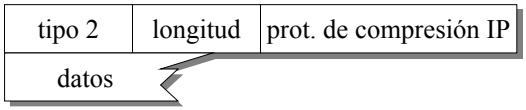

Figura 4.4.30. Campo de datos del paquete IPCP con el código Configure Request y negociación de compresión de protocolo IP.

El RFC 1332, sólo define en este momento la compresión Van Jacobson. Para este protocolo de compresión la longitud vale 6, el código del protocolo es 002D y el campo de datos contiene dos octetos. El primero es el "Max Slot ID" que identifica el número máximo de slots de conexión y el segundo es el "Comp Slot ID" que identifica si el número de Slot puede comprimirse o no. Una vez el PPP ha negociado con éxito la compresión del protocolo Van Jacobson, el protocolo IP viaja con uno de los siguientes códigos de protocolo:

- 0021: El protocolo IP no es TCP, el paquete es un fragmento o el paquete no puede comprimirse.
- 002D: Las cabeceras TCP / IP se han substituido por una cabecera comprimida.
- 002F: TCP no comprimido. El campo de protocolo IP ha sido substituido por el Slot.

– **IP-Address:** Esta opción permite negociar la dirección IP local de un puerto. Existen dos opciones, una el puerto propone la dirección IP que quiere utilizar y la otra solicita que sea el otro puerto quien le proponga la dirección a utilizar. El formato general del paquete es el presentado en la figura 4.4.31.

El campo de dirección puede contener la dirección IP que el puerto desea utilizar o todo ceros. En este último caso el puerto solicita que sea el extremo opuesto quien le asigne la dirección IP. Cuando la dirección no es aceptable por el extremo remoto, éste envía un Configure NACK con una dirección IP válida, que el otro extremo puede utilizar.

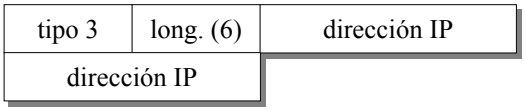

Figura 4.4.31. Campo de datos del paquete IPCP con el código Configure Request y negociación de dirección IP.

Ejercicios de autoevaluación

1. El sistema operativo LINUX permite configurar la mayoría de los parámetros del PPP, el proceso que ejecuta el PPP se denomina pppd. Conéctese al servidor LINUX de la asignatura y ejecute "man pppd". Liste los parámetros del LCP que pueden configurarse.

2. ¿Por que cree que es interesante poder configurar la longitud máxima del paquete a nivel de enlace?

Gestión de red

La gestión de red trata sobre la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste. Los objetivos principales de la gestión de red consisten en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.

Desde el momento en que las redes se consideran cada vez más una parte importante y estratégica de las empresas, industrias u otros tipos de instituciones y como resultado de las cada vez mayores dimensiones que están adoptando, resulta pues más importante su control y gestión con el fin de obtener la mejor calidad de servicio posible.

Tradicionalmente, en la gestión de las redes se ha partido de soluciones propietarias y cerradas con un ámbito de actuación limitado a la propia empresa o dominio de la institución. Con el tiempo, la evolución tecnológica ha permitido la entrada de múltiples fabricantes de equipos, de la misma forma que otros fabricantes de reputado nombre han desaparecido y, en consecuencia, también el apoyo que prestaban a sus soluciones de red. Por tanto, bien sea porque ha ocurrido la absorción de empresas o bien por diversificación de las fuentes de los equipos, las redes actuales son cada vez más heterogéneas en equipos.

Uno de los problemas más graves que tienen estas redes es que los equipos que las constituyen son de fabricantes distintos, con lo cual la única forma de gestionarlas es a partir de sistemas de gestión que utilicen estándares abiertos con el fin de compatibilizar protocolos e información. De esta forma, durante la década de los noventa, se han ido desarrollando diversas iniciativas con el objetivo de ofrecer recomendaciones y estándares abiertos para tratar de dar solución a estas nuevas problemáticas, como por ejemplo mediante el protocolo de gestión SNMP (Simple Network Management Protocol) o el CMIP (Common Management Information Protocol).

Para proporcionar una calidad de servicio adecuada mediante la gestión de redes, se parte de unos recursos humanos que mediante una serie de herramientas aplican unas determinadas metodologías a la red. Las recomendaciones sobre esta temática provienen de diversos grupos de estandarización. La más importante, la ITU–T, ha definido la red de gestión de las telecomunicaciones (TMN, *Telecommunications Management Network*). Estas recomendaciones definen cinco áreas funcionales para la gestión de red, las de supervisión y fallos, configuración, tarificación, prestaciones y seguridad.

Monitorización, control, gestión: Se utiliza el término *monitorización* para designar el tipo de acciones consistentes en obtener información de la red con el fin de detectar anomalías. Estas acciones son pasivas y su único objetivo es conocer el comportamiento respecto al tráfico del sistema. Una vez se conoce el sistema se puede proceder al control: para ello se establece una señalización o plano de control en toda red que se ocupa de regular activamente las comunicaciones y, en general, el tráfico de la red. Un ejemplo de red de control es el sistema de señalización nº 7. Finalmente, la gestión se define a partir del plano de gestión que integran las redes más avanzadas como RDSI, GSM, etc. Como ejemplo de red de gestión se puede citar la TMN definida por la ITU-T.

Según las áreas funcionales de gestión definidas por la ITU-T, la monitorización de red se utiliza para proporcionar información en la gestión de las funciones de prestaciones, fallos, contabilidad y en determinados aspectos de configuración, mientras que el control de red se aplica a las funciones de configuración y seguridad.

En el proceso de monitorización de la red se consideran una serie de aspectos como son: en primer lugar, una definición de la información de gestión que se monitoriza, una forma de acceso a la información de monitorización, un diseño de los mecanismos de monitorización y, finalmente, un procesado de la información de monitorización

obtenida. Por otra parte, la información de monitorización puede clasificarse según su naturaleza temporal en: información estática que se almacena en los elementos monitorizados (por ejemplo inventario); información dinámica que se almacena en los propios elementos o en equipos especializados (por ejemplo cambios de estado o fallos) e información estadística que se genera a partir de la información dinámica y que puede residir en cualquier lugar que tenga acceso a la información dinámica (por ejemplo rendimientos). Los mecanismos de monitorización se basan fundamentalmente en un sondeo o *polling* por parte de la estación gestora, esto es, en un acceso periódico a la información de gestión almacenada en los nodos gestionados. Este método tiene la ventaja de que los objetos que se gestionan únicamente deben estar preparados para responder, con lo que es más simple. Otros mecanismos que se emplean, desde el punto de vista del agente gestionado, se denominan *event reporting* o notificaciones, donde son los propios recursos quienes envían mensajes bajo ciertas condiciones; de esta forma tienen como ventaja el hecho que se minimiza el tráfico de gestión por la red. Otros métodos son mixtos, se basan en proxies, sondas, etc, y combinan los dos mecanismos anteriores.

Evolución de gestión de las redes de telecomunicaciones

Las redes de telecomunicaciones dentro del ámbito informático han evolucionado a partir de la necesidad de compartir información y procesos con usuarios remotos. En una primera fase se desarrollaron los grandes ordenadores: éstos eran extremadamente engorrosos de utilizar y caros. Estos primeros ordenadores tenían un uso local y eran manejados por una única persona o interfaz. Posteriormente, los sistemas operativos permitieron el acceso de múltiples usuarios que interactuaban en principio también en un modo local. La gestión de los equipos, cuando existía, era pues necesariamente local, y los mecanismos específicos de cada fabricante de ordenador.

Más adelante, el uso de redes de telecomunicaciones permitió el acceso remoto de equipos terminales a los grandes ordenadores. Las redes de tecnología conmutada y el uso de módems eran más baratos de utilizar que el coste que comportaba la disposición de múltiples ordenadores. El único ordenador era de tipo multiacceso y se accedía a éste de modo local, o remotamente mediante el uso de módems y equipos terminales (inicialmente teletipos). La gestión de red seguía siendo básicamente de tipo centralizado y basada en métodos del fabricante del mismo ordenador. Si bien esa gestión ya no cubría todos los elementos que entraban en la red de comunicaciones.

A medida que creció el uso del ordenador y aumentó el número de conexiones de equipos terminales a éste, fue necesario reducir la cantidad de módems utilizados debido a sus elevados costes. La solución fue la introducción del multiplexor que permitía integrar múltiples conexiones de equipos terminales en una sola línea de comunicación con lo que aumentaba el rendimiento. De esta forma, no eran necesarios tantos módems y se reducía el coste de las telecomunicaciones.

A medida que el progreso tecnológico abarataba los costes de la introducción de ordenadores en la empresa, las redes pasaron de tener configuraciones centralizadas a configuraciones de tipo distribuido con múltiples ordenadores. De esta forma, si bien en un principio se seguían utilizando redes RTC con módems, eran los ordenadores multiacceso quienes se interconectaban de forma interna. La gestión de red empezó a pasar de modelos centralizados a plantearse de modo distribuido o jerárquicamente distribuido en función del rango de los ordenadores en la red.

Conforme la interacción mutua del sistema distribuido de ordenadores iba aumentando fue haciéndose más necesario el uso de líneas dedicadas que permitieran reducir el coste debido al tráfico de información por las redes. Las empresas alquilaban líneas a los operadores de redes y eso permitía ofrecer costes menores en comunicaciones. La gestión de red se plantea de forma distribuida.

A raíz del crecimiento del tráfico telefónico en las redes de ordenadores se hace cada vez más necesario el empleo de líneas telefónicas privadas en las grandes corporaciones. A medida que la tecnología avance, se introducirán, además, líneas digitales que se adecuen mejor al tráfico generado por las comunicaciones entre ordenadores.
La entrada de las comunicaciones de tipo digital permitió optimizar la transferencia de información entre ordenadores. Nacieron redes como RDSI de conmutación de circuitos para terminales multimedia y otras redes basadas en conmutación de paquetes como la que utiliza la norma X.25.
Más adelante, con el empleo masivo de terminales tipo PC en las grandes corporaciones, se desarrollaron redes locales en conexión con redes de área extendida para poder cubrir las distancias correspondientes a campus o ciudades. Otros estándares como Frame Relay o ATM se han desarrollado para permitir esa interconexión de redes locales que pueden estar situadas de forma remota. En estos casos la proliferación de múltiples fabricantes distintos en el desarrollo de los terminales y dispositivos de interconexión de red hace complicada la gestión de este tipo de redes heterogéneas. Es por ello que a partir de esos momentos, resulta evidente la necesidad de diseñar mecanismos de estandarización para poder gestionar la creciente complejidad de los sistemas de redes.
De esta forma, surgieron diversos organismos de estandarización que trataron de solucionar el problema de la gestión en redes heterogéneas, como IETF que definió el protocolo SNMP o como ISO, que hizo lo propio con el protocolo CMIP.
Se puede, pues, hablar de distintos tipos de gestión según las configuraciones de los escenarios, es decir, una gestión autónoma donde las redes tienen gestión local en cada nodo; una gestión homogénea con redes homogéneas con un único nodo de gestión centralizado; finalmente, una gestión heterogénea, con la ampliación de las redes con la interconexión de productos heterogéneos. Este sería el caso del siguiente ejemplo: una organización que interconecta sus sistemas de información con diferentes redes de comunicaciones.
El caso de utilizar sistemas de gestión de red propietarios trae consigo las siguientes consecuencias: un plano de usuario (operador de red) con una multiplicidad de interfaces de usuario; un plano de aplicación (de gestión) con distintos programas de aplicación con funcionalidad similar; y, finalmente, un plano de información (de gestión): con una duplicidad y posible inconsistencia de la información almacenada en las bases de datos. Todo ello, dificulta el cumplimiento de que la gestión de red sea efectiva desde el punto de vista del coste.

Como solución se plantea una gestión integrada, en la que se normalizan las comunicaciones con la especificación de un protocolo entre elemento de red y centro de gestión, y la normalización de la información donde el centro de gestión debe poder conocer a los elementos de red mediante su nombre y sus propiedades visibles. Por tanto, debe haber también una definición sintácticamente uniforme de los elementos de red.

Clases de productos de gestión

Se pueden distinguir las siguientes clases de productos de gestión para LANs:

- Productos *standalone*, dirigidos especialmente a monitorización, análisis de test, seguridad y necesidades de tarificación.
- Plataformas de gestión de red que proporcionan un entorno en el cual las aplicaciones pueden ser desarrolladas, mejoradas e intercambiadas.
- Herramientas de gestión de LANs de PCs, que incluyen soluciones de propósito especial como una combinación de funciones de sistemas operativos en LANs y añadidos especiales.

- Sistemas de gestión de elementos LAN basados en estándares abiertos o *de facto* que ofrecen una aceptable funcionalidad a elementos LAN, tales como segmentos LAN, *hubs* cableados, dispositivos de interconexión LAN, FDDI, PBXs y conexión a integradores de gestores de red.
- Integradores que probablemente soportan elementos de gestión de sistemas LAN, MAN, y WAN en la misma plataforma.

Plataformas de gestión

Las plataformas de gestión utilizan una integración de aplicaciones para poder adaptarse al entorno cambiante y complejo de los elementos de red que se quieran gestionar. Entre las aplicaciones más usuales que se incorporan, destacan los *MIB browser* (navegadores u hojeadores de MIB) como interfaces de usuario del protocolo SNMP; el *discover*, que permite autodescubrir equipos y topologías de la red; la programación de sondeos de variables de la MIB; la programación de acciones ante alarmas; y, finalmente, los visualizadores gráficos de valores de variables de MIB.
Dentro de la categoría de sistemas basados en UNIX podemos encontrar los siguientes:

- Enterprise Management Architecture de Digital (PolyCenter)
- OpenView Network Management server de HP
- SunNet Manager de Sun Microsystems (Solstice)
- Spectrum de Cabletron
- DualManager de Netlabs (OverLord)
- NMC 3000 de Network Managers
- NetExpert de Objective Systems Integrators
- NMS/Core de Teknekron Communications Systems
- Network Knowledge Systems de Applied Computing Devices
- IBM Netview/6000 para AIX
- TME 10 de Tivoli.

Las plataformas de gestión posibilitan mayor grado de integración multifabricante que el esquema gestor de gestores. Las interacciones con otros sistemas de gestión de diferentes fabricantes se realizan a través de un interfaz de programación de aplicaciones estándares (API) y un conjunto estándar de definiciones de datos de gestión.

Modelos de gestión

Existen una serie de modelos de gestión normalizados, en los cuales es posible el acceso uniforme a los recursos gestionados. Se normaliza el protocolo de comunicaciones, el modelo de información de gestión y las definiciones de información de gestión. Los modelos de gestión de red tradicionales más importantes son la arquitectura TMN (Telecommunications Management Network) de la ITU-T (International Telecommunications Union, telecommunications sector), el modelo de gestión OSI (Open Systems Interconnection) de la ISO (International Standards Organization) basado en el protocolo CMIP (Common Management Information Protocol), y el modelo de gestión Internet del IETF (Internet Engineering Task Force) basado en el protocolo SNMP (Simple Network Management Protocol). Más recientemente, han adquirido importancia el modelo DMI (Desktop Management Interface), la gestión por agentes inteligentes y la gestión por webs.

Red de gestión de las telecomunicaciones (TMN)

La TMN proporciona funciones de gestión y comunicaciones para la operación, la administración y el mantenimiento de una red de telecomunicaciones y sus servicios en un entorno de múltiples fabricantes [SLO1].
Existieron dos motivaciones básicas para el desarrollo de la arquitectura TMN: una es la creciente heterogeneidad en la tecnología para la construcción de redes de telecomunicación, y la coexistencia de redes analógico-digitales; otra se deriva de las mayores demandas sobre: posibilidad de introducir nuevos servicios, alta calidad de servicios, posibilidad de reorganizar las redes. métodos eficientes de trabajo para operar las redes y competencia entre empresas operadoras privadas.
La TMN define la relación entre los bloques funcionales básicos constituyentes de la red (sistemas de operación (OS), red de comunicaciones de datos, elementos de red (NE)) a través de interfaces estándares. Introduce el concepto de control de subred (conjunto de elementos de red agrupados según un determinado criterio (por ejemplo función, proveedor,…) y es tratada como una sola entidad por la aplicación de gestión. El dispositivo que implementa la funcionalidad OAM&P de subred, el elemento gestor (EM), simplifica la comunicación entre OSs y NEs. Desde el punto de vista de la arquitectura, el EM es un punto de gestión flexible que une la realización del fabricante con los sistemas de gestión de la red, utilizando las interfaces y modelos de información definidos en la TMN.
Las recomendaciones que regulan la TMN son las de la serie M.3XXX de la ITU-T. En estas recomendaciones se definen los siguientes modelos y arquitecturas:

- Arquitectura física: estructura y entidades de la red.
- Modelo organizativo: niveles de gestión.
- Modelo funcional: servicios, componentes y funciones de gestión.
- Modelo de información: definición de recursos gestionados.

Los servicios de gestión que se definen son del siguiente tipo:

- Administración de abonados. Administración de encaminamiento y análisis de digitos. Administración de medidas y análisis de tráfico. Administración de la tarificación.
- Gestión de la seguridad de la TMN. Gestión de tráfico. Gestión del acceso de abonado. Gestión de circuitos entre centrales y equipo asociado. Gestión de la red de conmutación. Gestión de equipos en la instalación del usuario. Gestión del servicio controlado por el abonado. Gestión del sistema de señalización por canal común. Gestión de redes inteligentes. Gestión de la TMN.
- Administración de instalación del sistema. Administración de calidad de servicio y funcionamiento de la red
- Restablecimiento y recuperación.
- Gestión de materiales.
- Programa de trabajo del personal.

Las recomendaciones para la red TMN son las siguientes:

- M.3000. Introducción a la recomendación TMN.
- M.3010. Principios para una red de gestión de telecomunicaciones.
- M.3020. Metodología para la especificación de la interfaz TMN.
- M.3100. Modelo de información de elementos de red genéricos.
- M.3101. Requerimientos para conformar objetos gestionados en TMN M.3100.

- M.3180. Catálogo de información de gestión TMN.
- M.3200. Introducción a los servicios de gestión TMN.
- M.3300. Capacidades de gestión TMN presentadas en la interfaz F.
- M.3400. Funciones de gestión TMN.
- M.xfunc. Servicios de gestión TMN y funciones para la interfaz X.
- M.xinfo. Identificación de la información que se intercambia vía la interfaz X para diferentes casos de acceso.

Gestión según OSI

El fundamento del sistema de gestión OSI es la base de datos que contiene información relativa a los recursos y elementos que deben ser gestionados (MIB, Management Information Base). La estructura de gestión de información (SMI, Structure Management Information) identifica los tipos de datos que pueden ser usados en la MIB y cómo se representan y nombran los recursos dentro de la MIB.
Una MIB es un conjunto de definiciones de uno o varios recursos formado por clases de objetos gestionados, acciones, notificaciones, atributos, sintaxis, etc, y los *name bindings*. Actualmente hay una gran variedad de MIBs definidas y normalizadas. Una MIB no tiene por qué ser autocontenida, ya que permite referencias a otras MIBs. La sintaxis de MIBs se basa en la notación GDMO *(Guidelines for Definition of Managed Objects)*. Existen una serie de criterios para implementar una MIB, como son el uso de herencias de definiciones ya existentes y el establecer ligaduras de nombrado siempre que sea posible.
Cada recurso que se monitoriza y controla por el sistema de gestión OSI se representa por un objeto gestionado, como por ejemplo: conmutadores, estaciones de trabajo, PBX, programas en cola, algoritmos de encaminamiento, etc.
En este caso de gestión, la complejidad de la gestión se traslada al agente (que reside en un ordenador). Los protocolos de gestión permiten realizar funciones más complejas dado que el modelo de información también es complejo. La evolución de este tipo de gestión permitirá realizar una gestión integrada en entornos heterogéneos (por ejemplo TMN).
Las recomendaciones de la serie X.700 permiten hablar de una serie de modelos de gestión de sistemas. Son los siguientes:

- Modelo de comunicaciones: se detalla el protocolo de gestión y el servicio que proporciona.
- Modelo de información: se definen los recursos de red usando una sintaxis abstracta.
- Modelo funcional: se definen las funciones de gestión que proporcionan una interfaz a la aplicación de gestión.
- Modelo de organización: se exponen las posibles subdivisiones de la red en dominios de gestión.

Modelo de comunicaciones en el modelo de gestión OSI: CMIP

El Common Management Information Protocol (CMIP) se define en el estándar 9596 de OSI. Este protocolo ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para capas OSI. Una parte de la especificación del protocolo CMIP es la definición de la *Abstract Syntax Notation* (ASN.1) para codificación y decodificación de unidades de datos del protocolo CMIP (PDUs, Protocol Data Unit).
A lo largo de la evolución del protocolo CMIP han surgido variantes del protocolo para diferentes entornos. Por ejemplo, existe una versión de CMIP sobre protocolos TCP/IP

denominada CMOT, o bien el caso de una versión de CMIP sobre protocolos IEEE de LANs denominada CMOL.
Entre las características más importantes del protocolo CMIP se pueden destacar las siguientes:

- Requiere de gran cantidad de memoria y capacidad de CPU.
- Se generan largas cabeceras en los mensajes de los protocolos.
- Las especificaciones son difíciles de realizar y tediosas de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- Permite una jerarquía de sistemas de operación.
- El protocolo asegura que los mensajes llegan a su destino.

El hecho de que se trate de una gestión conducida por eventos se traduce en que:

- El agente notifica al gestor de sucesos la información concerniente a los recursos gestionados.
- El agente es responsable de monitorizar los recursos.
- Presenta la ventaja de que existe menor gestión de tráfico.
- Presenta la desventaja de tener agentes más complejos.

Servicios ofrecidos por CMIP: A través de CMISE (Common Management Information Service Element), CMIP proporciona tres tipos de servicios:

- Manejo de datos: usado por el gestor para solicitar y alterar información de los recursos del agente.
- Informe de sucesos: usado por el agente para informar al gestor sobre diversos sucesos de interés.
- Control directo: usado por el gestor para solicitar la ejecución de diversas acciones en el agente.

Actualmente las plataformas de gestión con protocolo CMIP de diferentes fabricantes presentan información que es propietaria, de forma que existe una cierta incompatibilidad si se quieren utilizar conjuntamente en la gestión de una red. En la figura adjunta se describe esta situación.
Finalmente, y más recientemente, se ha presentado el interfaz XOM/XOP, definido por la asociación X/Open para la coexistencia de protocolos SNMP con CMIP. A partir de unos *proxies* se permite la complementariedad de gestión de ambos protocolos en redes grandes. En entornos locales se utiliza SNMP y, a nivel de red de área extensa, se suele hacer uso del protocolo CMIP.

Modelo de gestión de Internet

Los protocolos SNMP (Simple Network Management Protocol) están normalizados por el IETF y constituyen el núcleo central de la gestión en Internet. El SNMP es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos Internet. SNMP define una arquitectura basada en cliente-servidor. El programa cliente (llamado el gestor de red) realiza conexiones virtuales a un programa servidor (llamado el agente SNMP) ejecutando en un dispositivo de red remoto. La base de datos controlada por el agente SNMP se denomina Management Information Base (MIB), y es

un conjunto estándar de valores estadísticos y de control de status. SNMP permite también extensiones de esta MIB a agentes particulares para el uso de MIB privadas. Este modelo será estudiado con más detalle en un punto posterior del presente capítulo.

Modelo de gestión DMI

Actualmente son las plataformas abiertas de gestión de red las que constituyen la base común para que a través de APIs (interfaces de programación de aplicaciones) las aplicaciones de gestión puedan realizar la recogida de datos de los elementos de red. Estas aplicaciones son accesibles normalmente por medio de lenguaje C y permiten que una aplicación pueda invocar una función de otra.

DMI (Desktop Management Interface) fue el primer API de gestión de PCs independiente de protocolos y sistemas operativos (abril 1994). Es uno de los principales componentes de la solución de gestión de DMTF (Desktop Management Task Force), consorcio industrial que persigue proveer una plataforma PC susceptible de ser gestionada en modo flexible. Los ficheros MIF (Management Information Format) provistos con cada producto gestionable definen, por su parte, los atributos gestionables del estándar en categorías tales como sistemas PC, servidores, impresoras, adaptadores LAN, módems y aplicaciones software. La arquitectura DMI incluye el nivel de servicio, un programa local que recoge información de los productos, gestiona esa información en bases de datos MIF, y la pasa a las aplicaciones de gestión cuando es solicitada. Controla, además, su comunicación con las aplicaciones de gestión de MI (Management Interface) y con los productos gestionables a través de CI (Component Interface).

Arquitecturas propietarias

Desde siempre los fabricantes líderes en sistemas de gestión han tratado de imponer estándares *de facto*. Actualmente se trata de una tendencia que está cayendo en desuso. Las razones principales se basan en la cada vez menor cuota de mercado de estos fabricantes líderes y de la cada vez mayor complejidad de los entornos de red, formados por extensas interconexiones de redes y servicios que dificultan su control y gestión por parte de unos pocos fabricantes.
Entre las arquitecturas de red más importantes se encuentran:

- IBM network management architecture: Open network management (ONA) es el marco de trabajo para los sistemas de gestión IBM. Las plataformas de gestión que utilizan la arquitectura de red IBM pueden ser: Netview para la gestión de redes SNA (System Network Architecture), LAN Network Manager para la gestión de redes Token Ring y Netview/6000 para la gestión SNMP (Karat).
- Novell: Novell utiliza un sistema operativo de red, basado en una evolución del Netware. Recientemente Novell ha introducido CMISE (Common Management Information Service Element) y CMIP en sus sistemas de gestión de red. Actualmente Novell está migrando su torre de protocolos IPX al estándar IP.
- AT&T: La arquitectura del sistema de gestión múltiple de red, *UNMA (Unified Network Management Architecture)* de AT&T está basada en OSI. UNMA consiste de una arquitectura en tres capas ligadas. El nivel más bajo está formado por los elementos de la red, es decir, componentes físicos y lógicos que comprende la red que se quiere gestionar. El segundo nivel lo forman Element Management Systems (EMS), que administran y gestionan elementos de red. El tercer nivel consiste de sistemas de gestión integrados que unen conjuntamente los EMSs de los tres niveles.

Gestión de red en Internet

Tal y como se ha dicho anteriormente se utiliza el protocolo SNMP que define una arquitectura basada en cliente-servidor con el programa gestor de red (cliente) y el agente (servidor). Los mensajes enviados por el gestor de red a los agentes SNMP están formados de identificadores de objetos MIB, junto con instrucciones a fin de cambiar u obtener un valor.
A pesar de la fácil integración de SNMP en los protocolos UDP/IP, es posible montar SNMP sobre otras torres de comunicación (Ethernet, IPX, OSI, CLNS). Sin embargo, a la hora de elegir una infraestructura de comunicaciones, hay que tener en cuenta la interoperabilidad, el nivel de transporte y el uso de un servicio orientado o no a conexión.
Entre las características principales del protocolo SNMP se puede destacar el hecho de que es un protocolo de gran flexibilidad y que permite una gran extensibilidad a todo tipo de redes. A pesar de definirse como un protocolo simple resulta ser un protocolo difícil de implementar para el diseño de aplicaciones, dada la complejidad intrínseca de las aplicaciones que debe diseñar. Por otra parte, en cuanto a rendimiento, la eficiencia del protocolo para la transmisión de información es baja, ya que se trata de una arquitectura basada en polling de acuerdo con una estructura de funcionamiento centralizada. El hecho de que se trate de una gestión conducida por polling determina que el gestor pregunte periódicamente a la información del agente sobre los recursos gestionados, de forma que es el gestor el responsable de monitorizar los recursos. Ello presenta la ventaja de que el gestor puede ser simple, pero presenta la desventaja de que la gestión de tráfico puede ser importante.
SNMP, si bien es un protocolo abierto, también puede utilizar un agente proxy para gestionar sistemas propietarios. Cabe destacar también que en SNMP la comunicación con los agentes no está orientada a conexión y que al ser un protocolo basado en UDP/IP no garantiza la llegada de los mensajes TRAP a destino, con lo que tienen que integrarse mecanismos especiales en capas superiores para evitar estas deficiencias.
El protocolo SNMP es eminentemente un protocolo simple y de monitorización. A continuación, se definen los tipos de operaciones permisibles con sus objetos:

- GetRequest: petición de valores específicos de la MIB.
- GetNextRequest: proporciona un medio para moverse por la MIB. Petición del objeto siguiente a uno dado de la MIB (orden lexicográfico).
- GetResponse: devuelve los valores solicitados por las operaciones anteriores.
- SetRequest: permite asignar un valor a una variable. Debido a posibles problemas de seguridad esta función suele estar desactivada.
- Traps: permite a los agentes informar de sucesos inusuales. (p.e. ColdStart, WarmStart, LinkDown, LinkUp, AuthenticationFailure, EGPNeighborLoss, EnterpriseSpecific).

En la figura 4.5.1 se muestran las relaciones que existen entre los diversos tipos de primitivas y los nodos de comunicaciones, es decir, los papeles de gestor (lado de la izquierda) y agentes (lado derecho). Junto a los mensajes anteriores destacan las Traps como mensajes especiales que especifican alarmas o sucesos inusuales. Estas Traps suelen variar mucho en cada entorno, dependiendo de la implementación que realice el fabricante.
El uso de MIBs privadas junto con mensajes tipo Trap permite la respuesta del sistema a alarmas específicas de los equipos de cada fabricante. Además, se posibilita la integración de agentes en multitud de dispositivos para su gestión, tales como puentes, encaminadores, pasarelas, etc. Las definiciones de las variables MIB soportadas por un agente en particular se incorporan en ficheros descritos en una notación especial

denominada Abstract Syntax Notation (ASN.1) a fin de que puedan ser utilizables por programas cliente de gestión de red de otros fabricantes.

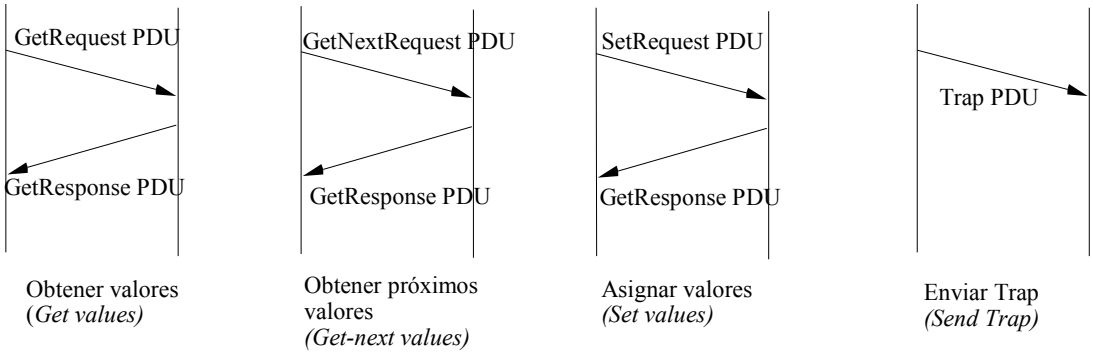

Figura 4.5.1 Secuencias de PDUs en el protocolo SNMP

Codificación para la transferencia de la información de gestión: BER

La información de gestión se define a partir de la ASN.1. Ésta establece que para la codificación se utilizarán las BER (Basic Encoding Rules). Las BER permiten traducir una estructura de datos cualquiera en una secuencia de bytes y viceversa. Las BER no son más que un algoritmo recursivo que puede producir una secuencia de bytes a partir de cualquier valor ASN.1. El protocolo SNMP sólo utiliza un subconjunto de estas reglas.
Las BER codifican los tipos utilizando los siguientes tres campos de longitud arbitraria:

- Tag: indica el tipo de ASN.1
- Length: indica el tamaño de la codificación del valor que sigue
- Value: indica propiamente la codificación del valor.

Configuración y rendimiento de una red gestionada por el protocolo SNMP

La gestión de redes se basa en la gestión de nodos, entendiendo como tales abstracciones de una entidad de red física como routers, hubs, ordenadores personales, impresoras, etc. Sin embargo, para analizar más en detalle la configuración y el rendimiento en la gestión, se tienen que determinar las dimensiones de los correspondientes parámetros:

- Número de estaciones
- Número de redes
- Número de segmentos
- Número de nodos
- Número de interfaces
- Número de gateways
- Número de nodos gestionados.

De hecho, cada nodo tiene una o más interfaces que se registran en la base de datos. La carga de gestión puede determinarse a partir del número de nodos gestionados más el número de interfaces gestionadas para cada nodo. A partir de ahí, considerando el número de redes y de segmentos se determina finalmente el número de objetos que se deben gestionar.

Para calcular el número de objetos que se deben gestionar, se tiene en cuenta que el número de interfaces por nodo suele ser único, y que experimentalmente puede considerarse un promedio de 2.4 objetos por nodo.
Los requerimientos de recursos del sistema de gestión pasan por cubrir las funcionalidades de monitorización y de descubrimiento básicas (Discover); las funcionalidades de presentación (display); las funcionalidades de eventos de acción y de colección de datos; finalmente, funcionalidades relativas a gestión distribuida y de bases de datos específicas. Todas estas funciones requieren de espacio de memoria estándar, memoria swap, espacio de disco y potencia de cálculo. Se suele estimar a menudo que el espacio de memoria swap sea como dos veces el de la memoria estándar.
El uso del protocolo SNMPv2 permite diversas configuraciones de gestión, y puede integrar estaciones de gestión con estaciones de sondeo de datos y con cónsolas de gestión (sesiones del programa de gestión). El proceso de sincronización de la información puede ser por ejemplo, de unos 3 min. para configuraciones de una estación de gestión, hasta unos 15 min. para configuraciones de 5 estaciones.
El uso de filtros para los procesos de obtención de información, de descubrimiento de los nodos (Discovery), la topología y los mapas, permite reducir mucho las necesidades de memoria y la carga del sistema de gestión, cosa que repercute en una mayor concentración de recursos para los objetos que realmente interesa gestionar.

Marco administrativo

Para una gestión con SNMP adecuada se define un nombre de comunidad (community) que afecta tanto al agente como al conjunto de gestores que lo administran, y un perfil de comunidad que delimita las propiedades así como el modo de acceso al sistema. De esta forma, la comunidad puede ser pública (public), es decir, de libre acceso. Esta información se almacena en cada MIB. De esta forma, una comunidad es una relación entre un agente y gestores y el nombre de comunidad es una cadena de octetos transmitida en los mensajes SNMP.
Para la determinación de políticas de autentificación y autorización se trabaja con autentificación simple, en la que el nombre de comunidad se transmite en claro; de ahí la necesidad de ampliar la seguridad del entorno de gestión mediante otros servicios de seguridad. En cuanto a la autorización, cada comunidad tiene asociado una vista (conjunto de objetos), de forma que para cada objeto se define un modo de acceso: read-only, read-write. Finalmente, el nombre de comunidad junto al perfil de comunidad marca la política de acceso al sistema.

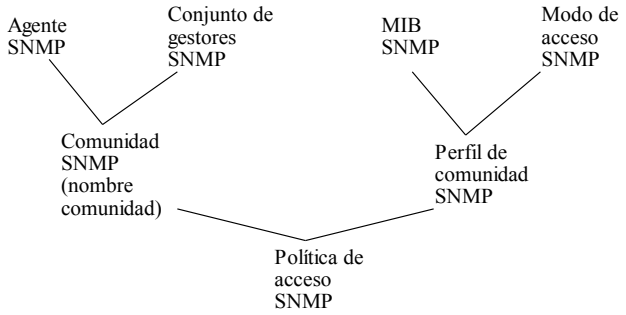

Figura 4.5.2 Conceptos administrativos

Conclusiones sobre el SNMP

Entre las ventajas del protocolo SNMP se pueden considerar las siguientes:

- Es un estándar de mercado.
- Es simple, fácil de usar.

- Modelo útil para el acceso a datos de gestión de la red.
- Acceso y organización eficientes de los datos gestionados.
- Independencia del entorno de comunicaciones.
- Capacidades generales de monitorización y control.

Respecto a los inconvenientes más importantes se pueden enumerar los siguientes:

- Limitaciones en el mecanismo de obtención de información: Falta de obtención selectiva de información.
- No dispone de controles de gestión.

A pesar de ser las MIBs unas bases de datos para gestión de red muy utilizadas y de fácil uso, presentan diversos problemas respecto a otros entornos de gestión más evolucionados. Entre los aspectos negativos considerados figuran los siguientes:

- Las comunicaciones datagrama son ineficientes para la obtención de grandes cantidades de información de las bases de datos.
- No existen mecanismos para la obtención agregada de datos de las MIB.
- No existen mecanismos de compresión de la información en la fuente.
- No existen mecanismos de correlación de la información en la fuente (por ejemplo la unión de tablas SNMP).
- No existe control de acceso a MIB.
- La estructura estática de la información en las MIB limita la manipulación y la reconfiguración dinámica, aunque se puede hacer uso de MIBs con información aportada por fabricantes,...
- Existe gran heterogeneidad en el modelo sintáctico/semántico.
- No hay modelo explícito de control (por ejemplo en invocaciones remotas).
- No hay mecanismos para representar y manipular relaciones.

El protocolo SNMPv2

Este protocolo de gestión que se definió en 1993, es una versión más avanzada del SNMP. SNMPv2 aporta una serie de ventajas respecto a la primera versión, entre las cuales pueden destacarse:

- Permite una mayor eficiencia en la transferencia de información.
- Admite mecanismos de seguridad como la autentificación y el cifrado frente al SNMP (no implementados).
- Permite la comunicación entre estaciones de gestión.
- Parte de un modelo de comunicaciones extendido considerablemente.
- Permite una señalización extendida de errores.
- Permite el uso de varios servicios de transporte.

El sistema basado en SNMPv2 soluciona muchos de los problemas de su anterior versión, SNMP; sin embargo, su incompatibilidad con la versión SNMP y su mayor complejidad está coartando su desarrollo.
El desacuerdo en el consorcio sobre las recomendaciones acerca de seguridad propuestas en SNMPv2 ha propiciado finalmente su incorporación en una nueva versión SNMPv3.

El protocolo SNMPv3

El protocolo SNMPv3 es una evolución de la serie de modelos de gestión vistos anteriormente. SNMPv3 está aún en fase de especificación; sin embargo, se pueden describir algunas de las características en las que se está trabajando. Las áreas a las que SNMPv3 va enfocado son, primordialmente, mejorar la seguridad y la administración respecto a SNMPv2.
Respecto a la estructura de la información de gestión, la SMI está dividida en tres partes: definiciones de módulos, definiciones de objetos y definiciones de notificaciones. Las definiciones de módulos (macros ASN.1: MODULE-IDENTITY) se utilizan para describir semánticamente los módulos de información. Para las definiciones sintácticas y semánticas de objetos se usan macros ASN.1: OBJECT-TYPE. Las definiciones de notificaciones usan macros NOTIFICATION-TYPE y describen transmisiones no solicitadas de información de gestión.
En SNMPv3 se prevé también aumentar el mapeo de mensajes tipo SNMP a otros tipos de protocolos de transporte. Desde el punto de vista de arquitectura de gestión se extiende el nombrado de:

- Motores y aplicaciones.
- Entidades (proveedores de servicio tales como motores en agentes y gestores).
- Identidades (usuarios de servicio).
- Información de gestión, incluido soporte para múltiples contextos lógicos.

Los cinco tipos de aplicaciones que se prevé asociar con un motor SNMP son: generadores de comandos, receptores de comandos (generadores de respuestas), originadores de notificaciones, receptores de notificaciones y envío de proxies.
Respecto a las mejoras en seguridad, SNMPv3 utilizará MD5 y algoritmos de Hash para firma digital y proteger contra la modificación de la información proporcionando integridad de datos, autentificación de origen y de usuario.

Voz sobre IP (VoIP)

Los sistemas de comunicación han evolucionado muy rápidamente en los últimos tiempos; sin embargo, el servicio de telefonía sigue siendo fundamental en todo tipo de entornos cotidianos. Recientemente la integración de tecnologías de la computación con los servicios de voz está posibilitando que las empresas dispongan de centros de atención de llamadas que permiten la incorporación de multitud de facilidades frente a los sistemas más convencionales basados en centralitas telefónicas. Estos nuevos entornos de red están constituidos por pasarelas a determinadas redes y gatekeepers (guardianes de puerta) que pueden realizar funciones de centro de control de llamadas en entornos más avanzados (Recs. H.32X).

Los protocolos de red utilizados se basan en el IP usado en redes internet. En principio el soporte de la aplicación de voz sobre IP (VoIP) puede tener como base las redes LAN privadas en las cuales, si bien la calidad de servicio no suele estar garantizada, normalmente no presentan mayores problemas para la calidad de servicio demandada habitualmente para el servicio de voz (Rec. H.323). Otro entorno de posible funcionamiento es la conexión a redes públicas (RDSI, RTC). En este caso la calidad de servicio suele ser también bastante aceptable.

Finalmente, otro caso de entorno de interconexión es el uso de internet. El empleo de VoIP sobre este tipo de redes se beneficia de la propia estructura del protocolo y del bajo coste de las comunicaciones; sin embargo, la calidad de servicio, bien sea debida a los retardos, bloqueos e incluso pérdidas de información, la hacen poco viable actualmente para comunicaciones telefónicas.

Recomendaciones relacionadas con VoIP

Existen una serie de recomendaciones básicas para la realización del gatekeeper como son H.323, H.225 y H.245 de la ITU. Junto a éstas pueden utilizarse otras muchas relacionadas a menudo con servicios más avanzados.

Recomendación H.323: Sistemas de comunicación multimedia basados en paquetes

En enero de 1998 el UIT-T aprobó una segunda versión para la recomendación H.323 relativa a Sistemas de Comunicación Multimedia basada en Conmutación de Paquetes. En este documento se define un entorno para comunicaciones de videotelefonía en un entorno formado por una Red de Área Local con acceso a otro tipo de redes como, por ejemplo, RDSI-BA, RDSI-BE y la Red Telefónica Conmutada (RTC).

La recomendación H.323 describe los componentes de un sistema formado por terminales, pasarelas o gateways, guardianes de puerta o gatekeepers, controladores multipunto o MCUs, procesadores multipunto y unidades de control multipunto. Los mensajes y procedimientos de control de esta recomendación definen la manera de comunicar de estos componentes.

Los terminales H.323 proporcionan capacidad de comunicaciones de audio y opcionalmente de vídeo y datos en conferencias punto a punto o multipunto.

El interfuncionamiento con otros terminales de la serie H, terminales vocales de la RTC o la RDSI, o terminales de datos de la RTC o la RDSI se realiza utilizando gateways. Concretamente el gateway actúa como pasarela hacia las demás redes adaptando tanto la señalización propia de cada sistema como la codificación del servicio (voz, vídeo o datos) para que puedan ser traspasados hacia la red de transporte.

El gatekeeper aparece como elemento de control del sistema H.323, sus funciones básicas consisten en realizar tareas de traducción de direcciones, control de admisión, gestión del ancho de banda y control de los demás elementos H.323.

Aunque la recomendación H.323 no define como imprescindibles a los elementos gateway y gatekeeper, éstos son básicos para poder extender los servicios prestados por el sistema local hacia otras redes.

Recomendación H.225.0: Empaquetación y sincronización de trenes de medios en redes de área local con calidad de servicio no garantizada

Esta recomendación describe los métodos por los que se asocian, codifican y paquetizan las señales de audio, vídeo, datos y control para su transporte entre terminales H.323 por una LAN con calidad de servicio no garantizada, o entre terminales H.323 y una cabecera H.323, que a su vez pueden conectarse a terminales de RDSI de banda estrecha, RTC o RDSI de banda ancha. Esta cabecera, las descripciones de terminales, y los procedimientos se describen en la recomendación H.323, mientras que la recomendación H.225.0 trata los protocolos y formatos de mensaje. Es también posible la comunicación a través de una cabecera H.323 hacia una cabecera H.322 para las LAN con calidad de servicio (QOS) garantizada, y por tanto a puntos extremos H.322.
La recomendación H.225.0 está destinada a operar con una amplia variedad de LAN diferentes, inclusive IEEE 802.3, Token Ring, etc. De este modo, la recomendación H.225.0 se define como algo que está por encima de la capa de transporte tal como los protocolos TCP/IP/UDP, SPX/IPX, etc. Así, el alcance de la comunicación H.225.0 se halla entre terminales H.323 y cabeceras H.323 en la misma LAN, utilizando el mismo protocolo de transporte. Esta LAN puede ser un único segmento o anillo, o podría lógicamente ser una red de datos empresarial que comprenda múltiples LAN interconectadas.
La recomendación H.225.0 hace uso del RTP/RTPC (protocolo en tiempo real/protocolo de control en tiempo real) para la empaquetación y sincronización de medios de todas las LAN subyacentes. Adviértase que la utilización de los protocolos RTP/RTCP especificada en la recomendación H.225.0 no está vinculada en modo alguno a la utilización de la familia TCP/IP/UDP.
Los protocolos utilizados dentro de la recomendación H225.0 son:

- RAS (Registration, Admissions and Status): Los mensajes RAS controlan las funciones de registro en los gatekeepers, admisión de llamadas, control de ancho de banda y control de estado.
- Q.931: Es el sistema de señalización utilizado para el establecimiento, mantenimiento y liberación de las llamadas.
- RTP/RTCP: Permite la transmisión y control de los paquetes de voz en tiempo real.

Recomendación H.245: Protocolo de control para comunicación multimedia

Esta recomendación especifica la sintaxis y la semántica de los mensajes de información de terminal, así como los procedimientos para utilizarlos en la negociación en banda al comienzo de la comunicación o durante ésta. Los mensajes comprenden capacidades de recepción y transmisión, así como preferencia de modos desde el extremo de recepción, la señalización de canal lógico y la indicación y control. Se especifican procedimientos de señalización con acuse de recibo para garantizar comunicaciones fiables audiovisuales y de datos.
Esta recomendación abarca una amplia gama de aplicaciones que incluyen servicios de voz así como los de almacenamiento/recuperación, mensajería y distribución. Los distintos sistemas que utiliza pueden especificar el empleo de protocolos de transporte diferentes. Sin embargo, se ha previsto su utilización con una capa de transporte fiable, es decir, que proporciona una entrega garantizada de datos correctos.

MCU: Multicast Control Unit

Dentro de las funciones definidas en H.323 relacionadas con el control de las comunicaciones, destaca el apartado de las conexiones *multicast*, concretándose en la definición de una unidad de control específica.
La función MCU se encarga del control de las conexiones *multicast* dentro de los entornos de red H.323. Los servicios avanzados requieren no sólo de conexiones punto a punto, como sucede con los servicios telefónicos convencionales, sino que requerirán de conexiones punto a multipunto o multipunto a multipunto. De esta manera, los usuarios podrán conectarse entre sí simultáneamente, ya sea con conexiones unidireccionales o bidireccionales.

Gateway o pasarela

El gateway o pasarela es un dispositivo lógico que tiene conectividad IP y conectividad a alguna otra red, usualmente una red pública o privada. La función del gateway es traducir las medias y protocolos de señalización desde la tecnología de una red a otra, consiguiendo una conexión transparente para los usuarios del sistema. Entre los atributos que tiene está el rango de números telefónicos, el volumen y tipo de servicios que proporciona incluyendo el número de puertos, número de llamadas simultáneas, velocidad de las líneas, protocolos de señalización soportados, funcionalidades telefónicas, seguridad, etc.

Gatekeeper o guardian de puerta

El diseño de un gatekeeper, o en modo más amplio llamado también centro de llamadas, en su estructura más básica, parte de las especificaciones funcionales de un guardián de puerta (gatekeeper). En ese sentido hay que decir que el gatekeeper es un dispositivo que, aunque sea opcional en un sistema H.323, presta servicios de control de llamada básicos a los puntos extremos H.323. Aunque puede estar presente más de un gatekeeper y comunicar con cada uno de los demás de una manera no especificada, la recomendación determina que debe haber uno por zona. El guardián de puerta está separado lógicamente de los puntos extremos. Sin embargo, su implementación física puede coexistir con un terminal, MCU, pasarela, MC u otro dispositivo de red no H.323. Cuando esté presente en un sistema, el guardián de puerta deberá prestar los siguientes servicios:

- Conversión de dirección: El guardián de puerta efectuará la conversión de dirección de alias a dirección de transporte. Esto se debe hacer utilizando un cuadro de conversión que se actualiza mediante mensajes de registro. También son posibles otros métodos de actualización.
- Control de admisiones: El guardián de puerta autorizará el acceso a la red. La autorización del acceso puede basarse en la autorización de la llamada, en la anchura de banda o en algún otro criterio que se deja a decisión del fabricante. También puede ser una función nula que admita todas las peticiones.
- Control de ancho de banda: El guardián de puerta realizará la gestión del ancho de banda. También puede ser una función nula que acepte todas las peticiones de cambio de anchura de banda.
- Gestión de zona: El guardián de puerta proporcionará las funciones anteriores para terminales, MCU y pasarelas que se hayan registrado en él.

El guardián de puerta también puede efectuar otras funciones opcionales, tales como:

- Señalización de control de llamada: El guardián de puerta puede optar por completar la señalización de la llamada con los puntos extremos y puede procesar él mismo la señalización de la llamada. De manera alternativa, el guardián de puerta puede encaminar los puntos extremos para que conecten el canal de señalización de llamada directamente el uno al otro. De esta manera, el guardián de puerta puede evitar el tratamiento de señales de control de llamada H.225.0. Es posible que tenga que actuar como la red para sustentar servicios suplementarios.
- Autorización de llamada: Utilizando la señalización H.225.0, el guardián de puerta puede rechazar llamadas procedentes de un terminal por ausencia de autorización. Pueden ser motivos de rechazo, entre otros, el acceso restringido hacia/desde terminales o pasarelas particulares y el acceso restringido durante determinados periodos de tiempo.
- Gestión del ancho de banda: Control del número de terminales H.323 a los que se permite el acceso simultáneo a la red. Utilizando la señalización H.225.0, el guardián de puerta puede rechazar llamadas procedentes de un terminal debido a limitaciones del ancho de banda. Tal cosa puede ocurrir si el guardián de puerta determina que no hay suficiente ancho de banda disponible en la red para soportar la llamada. Esta función puede ser una función nula, es decir, que a todos los terminales se les permita el acceso. Esta función actúa también durante una llamada activa, cuando un terminal pide ancho de banda adicional.
- Gestión de llamada: Por ejemplo, el guardián de puerta puede mantener una lista de llamadas H.323 en curso. Esta información puede ser necesaria para indicar que un terminal llamado está ocupado y proporcionar información para la función de gestión de anchura de banda.
- Estructura de datos de información de gestión del guardián de puerta.
- Reserva de ancho de banda para terminales que no pueden efectuar esta función.
- Servicio de directorio.

Proceso de llamada utilizando el H.323

Antes de dar paso a una comunicación H.323 se requiere del registro de los terminales en el gatekeeper. Para ello se envían los siguientes mensajes utilizando un canal RAS identificado por una dirección IP y un puerto UDP:

- Registration Request (RRQ).
- Registration Confirmation (RCF).

En el momento de iniciar una comunicación los terminales deben pedir autorización al gatekeeper utilizando los mensajes:

- Admission Request (ARQ). El ARQ contiene parámetros de alias de destino, número telefónico o nombre del usuario que el grupo llamante quiere contactar.
- Admission Confirm (ACF): El gatekeeper otorga permiso para la llamada enviando un mensaje de conteniendo la dirección de transporte actual asociada al alias del grupo llamado enviada en el mensaje ARQ.
- Admission Reject (ARJ): El gatekeeper podría tambien rechazar la petición enviando este mensaje donde se incluyen las razones de la denegación, tales como falta de ancho de banda, problemas de seguridad, etc.

A partir de la confirmación se inicia una comunicación H.323 que incluye cuatro fases:

- Establecimiento de llamada.

- Comunicación inicial e intercambio de capacidades: una vez se ha establecido una comunicación entre los terminales, se establece un canal de control H.245 para negociar las capacidades multimedia de la comunicación. Este canal de control H.245 se identifica por una dirección IP y un puerto TCP. Los mensajes que se intercambian los terminales se denominan TerminalCapabilitySet. El mensaje describe las capacidades del terminal tales como la capacidad de recibir audio codificado por G.711 o vídeo codificado en H.261.
- Establecimiento de la comunicación audiovisual: Una vez se han establecido las capacidades de los terminales, los extremos establecen un canal de datos para llevar audio, vídeo, o tráfico de datos entre los extremos de la comunicación
- Terminación de la llamada

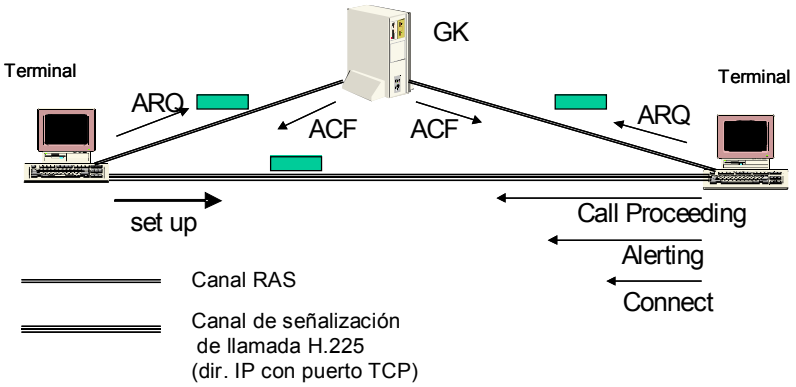

Figura 4.6.1 Establecimiento de llamada

Estándares IETF. Telefonía IP

El IETF a su vez ha desarrollado nuevas alternativas al control y gestión de las comunicaciones de voz sobre IP, en este caso utiliza los siguientes protocolos:

- Session Initiation Protocol (SIP)
- Session Description Protocol (SDP)
- Gateway Location Protocol (GLP)
- Media Gateway Control Protocol (MGCP)
- Service Location Protocol (LSP)

Session Initiation Protocol (SIP)

El SIP es un protocolo cliente-servidor con sintaxis y semántica parecida al HTTP que se utiliza para iniciar una sesión entre usuarios y es una alternativa más descentralizada al H.323. Permite realizar las siguientes funciones:

- Servicios de búsqueda de usuarios
- Establecimiento de llamada
- Gestión de participantes en una llamada
- Invocación de determinadas funcionalidades

El SIP CGI es un interfaz basado en CGI que sirve para programar servicios. Se basa en las mismas características que los CGI utilizados en webs, sin embargo aporta nuevas funcionalidades para mantener interacciones prolongadas de información respecto a clientes o servidores. Los agentes de la llamada se invocan cuando una llamada llega a

un servidor SIP. Estos agentes ejecutan las instrucciones contenidas en el script CGI. Con ello, permite disponer de inteligencia a la red.

Session Description Protocol (SDP)

El SDP se utiliza para describir las sesiones multimedia tanto para telefonía como para aplicaciones distribuidas como, por ejemplo, radio por internet. El protocolo incluye información relacionada con:

- Flujos de los medias
- Direcciones (pueden ser distintas para distintos medias!)
- Puertos
- Tipos de los trayectos
- Tiempos de inicio y pausas
- Originante

SDP es más bien un formato descriptivo de los parámetros de una sesión. Por ejemplo, tenemos:

- v: identificador de versión de la sesión
- u: dirección URL
- e: dirección email
- c: dirección de la sesión
- b: ancho de banda de la sesión
- t: tiempos de inicio y final
- m: tipos de medias

Gateway Location Protocol (GLP)

El GLP permite realizar llamadas entre usuarios de internet a usuarios de otras redes como telefonía. Para ello se requiere de una pasarela entre una red de telefonía e internet. El GLP permite minimizar la distancia entre la RTC y la pasarela correspondiente de acceso a internet. Cada dominio de la red dispone de servidores de posición (location servers, LS) con un protocolo intradominio SLP (Service Location Protocol).
El servidor de posición (Location Server, LS) es la entidad funcional principal del Telephony Routing over IP (TRIP). El LS es un dispositivo lógico que tiene acceso a una base de datos de gateways (pasarelas) llamada la Telephony Routing Information Base (TRIB). El LS también exporta información de pasarelas a otros LS de otros Internet Telephony Administrative Domain (ITAD). El LDAP (Lightweight Directory Access Protocol), como protocolo intradominio, también podría utilizarse para acceder a los LS.
El Telephony Routing over IP (TRIP) se ocupa del descubrimiento (discovery) e intercambio de tablas de encaminamiento entre pasarelas de telefonía IP de distintos proveedores. Los servidores de posición (LS) son entidades lógicas con conectividad IP que tienen conocimiento de pasarelas que pueden utilizarse para terminación de llamadas hacia la RTC. El LS es la principal entidad que participa en el encaminamiento de telefonía sobre IP. Un LS podría responsabilizarse del envío de información de pasarela a otros LS's, GK's o servidores SIP. TRIP funciona a nivel de aplicación.

El *Internet Telephony Administrative Domain (ITAD)* es el conjunto de recursos (pasarelas, servidores de posición,..) bajo el control de una única autoridad administrativa. Los usuarios son clientes de un ITAD.

Media Gateway Control Protocol (MGCP)

El *Media Gateway Control Protocol* (MGCP), publicado como RFC 2705, es un protocolo de control que permite a un coordinador central monitorizar eventos en pasarelas y teléfonos IP y configurarlos para enviar medias a direcciones específicas. EL MGCP integra al *Simple Gateway Control Protocol (SGMP)* y el *Internet Protocol Device Control (IPDC)*
MGMP describe un interfaz de programación de aplicaciones (API) y un protocolo complementario, el MGCP. Su propósito es definir las operaciones de pasarelas de telefonía como dirigidas por un controlador, conocidas como *agentes de llamada*, o bien, *Media Gateway Controllers* (MGC).
La pasarela de telefonía proporciona operaciones de conexión e interfuncionamiento entre las señales de audio utilizadas en circuitos telefónicos y los paquetes de datos utilizadas en internet u otros tipos de redes orientadas a paquetes. El agente de llamada dirige las operaciones del *gateway* o pasarela.
Existen diversos tipos de pasarelas para conectar una red de voz sobre IP con redes de telefonía básica, de acceso, ATM, centralitas PABX, etc.

Service Location Protoco (LSP)

El protocolo de localización de servicios (*Service Location Protocol*, LSP) proporciona un marco de funcionamiento escalable para el descubrimiento (*discovery*) y selección de servicios de red. Usando este protocolo, los ordenadores en redes IP apenas necesitan configuración estática de servicios de red para aplicaciones basadas en la red. Esto es especialmente importante en equipos portables o en equipos no gestionables por el administrador de la red. Aplicable a inteligencia de red.
El posicionador de recursos uniforme (URL) especifica la posición de un terminal en la red telefónica y los tipos de conexión (modos de operación: tel, fax y módem) que pueden utilizarse para conectarse a esta entidad. El URL especifica las llamadas de voz (llamadas telefónicas normales, máquinas de respuesta automática y sistemas de mensajería de voz), llamadas de fax y llamadas de datos, tanto para abonados de telefonía fija (POTS) como digitales / móviles.

Codificadores de voz

En la recomendación H.323 se utilizan varios codificadores de voz. Actualmente el Forum VoIP está recomendando la especificación G.723.1 para su uso en telefonía y audioconferencia en Internet. Otras recomendaciones como la G.729 (algoritmo ACELP) son más apropiadas para redes WAN. En este caso, se llega a compresiones de hasta 8 Kbps a partir de flujos de 64 Kbps, utilizados frecuentemente en los canales PCM. En el caso del codec G.728 (algoritmo LD-CELP) se baja el flujo de voz hasta los 16 Kbps.
El codificador de G.723 alcanza los 5.3 Kbps y la versión G.723.1 comprime hasta los 6.3 Kbps. Aunque la calidad de la voz no es muy buena, permite la comunicación con intranets y a través de la RTC punto a punto mediante un simple módem a 14.4 Kbps.
Estándares de compresión de voz y sus retardos:

- PCM (G.711) 0.75 ms
- 32K ADPCM (G.726) 1 ms
- 16K LD-CELP (G.728) 3-5 ms

- 8K CS-ACELP (G.729) 10 ms
- 8K CS-ACELP (G.729a) 10 ms
- 6.3K MPMLQ (G.723.1) 30 ms
- 5.3K ACELP (G.723.1) 30 ms

Conclusiones sobre VOIP

- La fiabilidad y la calidad de los servicios (QoS) de telefonía basados en IP no están todavía a la altura de las redes de telefonía pública tradicionales.
- La disponibilidad de servicios suplementarios en el entorno de la red IP no es comparable todavía a los servicios en RTC.
- Los trabajos de estandarización aún no están terminados provocando la aparición de soluciones propietarias incompatibles.
- La falta de coordinación de los foros de estandarización, en algunos aspectos (IETF-SIP y ETSI/ITU-H.323), provoca que la incompatibilidad de los equipos sea aún mayor.
- Los procedimientos de interfuncionamiento SS7-SCTP, SS7-H.323 o SS7-SIP no están aún resueltos.
- Existen problemas de direccionamiento IP entre redes distintas como la RTC y la red IP.
- Actualmente, la telefonía IP se puede utilizar en redes Intranet de empresas dejando para las comunicaciones exteriores, por ejemplo con los clientes, el uso de redes RTC, RDSI, etc. de mayor calidad que disponen de una reserva de recursos.
- Permite ciertas economías de escala con el uso de un único cableado.
- La integración de equipos y con las redes IP reduce costes a largo plazo.
- Los terminales de telefonía IP de voz en general son más caros y complejos que los terminales convencionales.
- Necesaria adaptación de las redes basadas en el SS7, generalmente en manos de operadores tradicionales, a las redes basadas en protocolos tipo IP.