CONFIGURACIÓN Y PRUEBA DE LA RED

INTRODUCCIÓN AL CAPITULO

Se analizara el proceso para conectar y configurar computadoras, switches y routers en una LAN Ethernet.

Presentaremos los procedimientos básicos de configuración para dispositivos de red. Estos procedimientos requieren la utilización del Sistema operativo Internetwork (IOS) y de los archivos de configuración relacionados para los dispositivos intermediarios.

Resulta esencial la comprensión del proceso de configuración con IOS por parte de los administradores de red y de los técnicos de red.

Objetivos

- Definir la función del Sistema operativo Internetwork (IOS).
- Definir el propósito de un archivo de configuración.
- Identificar las diversas clases de dispositivos que tienen IOS incorporado.
- Identificar los factores que contribuyen al conjunto de comandos IOS disponible para un dispositivo.
- Identificar los modos de operación de IOS.
- Identificar los comandos básicos de IOS.
- Comparar y contrastar los comandos show básicos.

Configuración y prueba de la red

CONFIGURACIÓN DE DISPOSITIVO

Sistema Operativo Internetwork (IOS)

Al igual que una computadora personal, un router o switch no puede funcionar sin un sistema operativo. Sin un sistema operativo, el hardware no puede realizar ninguna función. El sistema operativo Internetwork (IOS) es el software del sistema en dispositivos. El IOS se utiliza en la mayoría de los dispositivos, independientemente del tamaño o tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbricos, grandes routers con decenas de interfaces y muchos otros dispositivos.

El IOS proporciona a los dispositivos los siguientes servicios de red:

- Funciones básicas de enrutamiento y conmutación
- Acceso confiable y seguro a recursos en red
- Escalabilidad de la red

Los detalles operativos de IOS varían de acuerdo con los diferentes dispositivos de internetworking, según el propósito y el conjunto de características del dispositivo.

Por lo general, se tiene acceso a los servicios que proporciona el IOS de Cisco mediante una interfaz de línea de comandos (CLI). Las funciones accesibles a través de la CLI varían según la versión de IOS y el tipo de dispositivo.

El archivo IOS en sí tiene un tamaño de varios megabytes y se encuentra almacenado en un área de memoria semipermanente llamada flash. La memoria flash provee almacenamiento no volátil. Esto significa que los contenidos de la memoria no se pierden cuando el dispositivo se apaga. Aunque los contenidos no se pierden, pueden modificarse o sobreescribirse si es necesario.

El uso de memoria flash permite que se actualice el IOS a versiones más nuevas o que se incorporen nuevas funciones. En muchas arquitecturas de router, el IOS se copia en la RAM cuando se enciende el dispositivo y el IOS se ejecuta desde la RAM cuando el dispositivo está funcionando. Esta función mejora el rendimiento del dispositivo.

Métodos de acceso

Existen varias formas de acceder al entorno de la CLI. Los métodos más comunes son:

- Consola
- Telnet o SSH
- Puerto auxiliar

Consola: Se puede tener acceso a la CLI a través de una sesión de consola, también denominada línea CTY. La consola usa una conexión serial de baja velocidad para conectar directamente un equipo o un terminal al puerto de consola en el router o switch.

El puerto de consola es un puerto de administración que proporciona acceso al router fuera de banda. Es posible acceder al puerto de consola aunque no se hayan configurado servicios de networking en el dispositivo. El puerto de consola se suele utilizar para tener acceso a un dispositivo cuando no se han iniciado o han fallado los servicios de networking.

Los siguientes son algunos ejemplos del uso de la consola:

- La configuración de inicio del dispositivo de red
- Procedimientos de recuperación de desastres y resolución de problemas donde no es posible el acceso remoto
- Procedimientos de recuperación de contraseña

Cuando un router se pone en funcionamiento por primera vez, no se han configurado los parámetros de networking. Por lo tanto, el router no puede comunicarse a través de una red. Para preparar la puesta en marcha y configuración iniciales, se conecta un equipo que ejecuta un software de emulación de terminal al puerto de consola del dispositivo. En el equipo conectado pueden ingresarse los comandos de configuración para iniciar el router.

Durante el funcionamiento, si no se puede acceder a un router en forma remota, una conexión a la consola puede permitir a una computadora determinar el estado del dispositivo. En forma predeterminada, la consola comunica el inicio del dispositivo, la depuración y los mensajes de error.

Para muchos dispositivos IOS, el acceso de consola no requiere ningún tipo de seguridad, en forma predeterminada. Sin embargo, la consola debe estar configurada con contraseñas para evitar el acceso no autorizado al dispositivo. En caso de que se pierda una contraseña, existe un conjunto especial de procedimientos para eludir la contraseña y acceder al dispositivo. Debe colocarse el dispositivo en un cuarto cerrado con llave o en un bastidor de equipos para impedir el acceso físico.

Telnet y SSH

Un método que sirve para acceder en forma remota a la sesión CLI es hacer telnet al router. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de networking activos en el dispositivo. El dispositivo de red debe tener configurada por lo menos una interfaz activa con una dirección de Capa 3, como por ejemplo una dirección IPv4. Los dispositivos incluyen un proceso de servidor Telnet que se activa cuando se inicia el dispositivo. El IOS también contiene un cliente Telnet.

Un host con un cliente Telnet puede acceder a las sesiones vty que se ejecutan en el dispositivo. Por razones de seguridad, el IOS requiere que la sesión Telnet use una contraseña, como método mínimo de autenticación.

El protocolo Shell seguro (Secure Shell, SSH) es un método que ofrece más seguridad en el acceso al dispositivo remoto. Este protocolo provee la estructura para una conexión remota similar a Telnet, salvo que utiliza servicios de red más seguros.

El SSH proporciona autenticación de contraseña más potente que Telnet y usa encriptación cuando transporta datos de la sesión. La sesión SSH encripta todas las comunicaciones entre el cliente y el dispositivo IOS. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Como una mejor práctica, siempre utilice SSH en lugar de Telnet, cuando sea posible.

Las versiones más recientes del IOS contienen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren la activación del servidor SSH.

Los dispositivos IOS también incluyen un cliente SSH que puede utilizarse para establecer sesiones SSH con otros dispositivos. De manera similar, puede utilizarse un equipo remoto con un cliente SSH para iniciar una sesión de CLI segura. No se provee el software de cliente SSH de manera predeterminada en los sistemas operativos de todos los equipos. Es posible que deba adquirir, instalar y configurar el software de cliente SSH en su equipo.

Puerto auxiliar

Otra manera de establecer una sesión CLI en forma remota es a través de una conexión dial-up telefónica mediante un módem conectado al puerto auxiliar del router. De manera similar a la conexión de consola, este método no requiere ningún servicio de networking para configurarlo o activarlo en el dispositivo.

El puerto auxiliar también puede usarse en forma local, como el puerto de consola, con una conexión directa a una computadora que ejecute un programa de emulación de terminal. El puerto de consola es necesario para la configuración del router, pero no todos los routers tienen un puerto auxiliar.

También se prefiere el puerto de consola antes que el puerto auxiliar para la resolución de problemas, ya que muestra de manera predeterminada la puesta en marcha del router, la depuración y los mensajes de error.

Generalmente, en la única oportunidad que el puerto auxiliar se usa en forma local en lugar del puerto de consola es cuando surgen problemas en el uso del puerto de consola, como por ejemplo cuando no se conocen ciertos parámetros de consola.

ARCHIVOS DE CONFIGURACIÓN

Los dispositivos de red dependen de dos tipos de software para su funcionamiento: el sistema operativo y la configuración. Al igual que el sistema operativo en cualquier computadora, el sistema operativo facilita la operación básica de los componentes de hardware del dispositivo.

Los archivos de configuración contienen los comandos del software IOS utilizados para personalizar la funcionalidad de un dispositivo. Los comandos son analizados (traducidos y ejecutados) por el software IOS cuando inicia el sistema (desde el archivo startup-config) o cuando se ingresan los comandos en la CLI mientras está en modo configuración.

El administrador de red crea una configuración que define la funcionalidad deseada del dispositivo. El tamaño del archivo de configuración normalmente es de unos cientos a unos miles de bytes.

Tipos de archivos de configuración

Un dispositivo de red puede contener dos archivos de configuración:

1. El archivo de configuración en ejecución, utilizado durante el funcionamiento actual del dispositivo
2. El archivo de configuración de inicio, utilizado como la configuración de respaldo, que se carga al iniciar el dispositivo

Archivo de configuración de inicio

El archivo de configuración de inicio (startup-config) se usa durante el inicio del sistema para configurar el dispositivo. El archivo de configuración de inicio o el archivo startup-config se almacena en la RAM no volátil (NVRAM). Como la NVRAM es no volátil, el archivo permanece intacto cuando el dispositivo se apaga. Los archivos startup-config se cargan en la RAM cada vez que se inicia o se vuelve a cargar el router. Una vez que se ha cargado el archivo de configuración en la RAM, se le considera la configuración en ejecución o running-config.

Configuración en ejecución

Una vez en la RAM, esta configuración se utiliza para operar el dispositivo de red.

La configuración en ejecución se modifica cuando el administrador de red realiza la configuración del dispositivo. Los cambios en la configuración en ejecución afectarán la operación del dispositivo en forma inmediata. Luego de realizar los cambios necesarios, el administrador tiene la opción de guardar tales cambios en el archivo startup-config, de manera que se utilicen la próxima vez que se reinicie el dispositivo.

Como el archivo de configuración en ejecución se encuentra en la RAM, se pierde si se apaga la energía que alimenta al dispositivo o si se reinicia el dispositivo. También se perderán los cambios

realizados en el archivo running-config si no se guardan en el archivo startup-config antes de apagar el dispositivo.

IOS Sistema Operativo Modal

El IOS está diseñado como un sistema operativo modal. El término modal describe un sistema en el que hay distintos modos de operación, cada uno con su propio dominio de operación.

En orden descendente, los principales modos son:

- Modo de usuario
- Modo de ejecución privilegiado
- Modo de configuración global
- Otros modos de configuración específicos

Cada modo se utiliza para cumplir determinadas tareas y tiene un conjunto específico de comandos que se encuentran disponibles cuando el modo está habilitado. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Todas las configuraciones que se ingresan en el modo de configuración de interfaz se aplican sólo a esa interfaz.

Algunos comandos están disponibles para todos los usuarios; otros pueden ejecutarse únicamente después de ingresar el modo en el que ese comando está disponible. Cada modo se distingue por una petición de entrada singular y sólo se permiten los comandos apropiados para ese modo.

Se puede configurar la estructura modal jerárquica a fin de proporcionar seguridad. Puede requerirse una autenticación diferente para cada modo jerárquico. Así se controla el nivel de acceso que puede concederse al personal de red.

Indicadores del sistema

Cuando se usa la CLI, el modo se identifica mediante la petición de entrada de línea de comandos que es exclusiva de ese modo. La petición de entrada está compuesta por las palabras y los símbolos en la línea a la izquierda del área de entrada. Se usa la frase petición de entrada porque el sistema le solicita que ejecute una entrada.

De manera predeterminada, cada petición de entrada empieza con el nombre del dispositivo. Después del nombre, el resto de la petición de entrada indica el modo. Por ejemplo, la petición de entrada predeterminada para el modo de configuración global en un router sería:

Router(config)#
Como se utilizan comandos y cambian los modos, la petición de entrada cambia para reflejar el contexto actual, como se muestra en la figura.

Estructura del indicador del IOS

```
Router>ping 192.168.10.5
Router#show running-config
Router(config)#Interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

El indicador cambia para indicar el modo CLI actual.

```
Switch>ping 192.168.10.9
Switch#show running-config
Switch(config)#Interface FastEthernet 0/1
Switch(config-if)#Description connection to WEST LAN4
```

Modos principales
Los dos modos de operación principales son:

- EXEC del usuario
- EXEC privilegiado

Como característica de seguridad, el software IOS divide las sesiones EXEC en dos modos de acceso. Estos dos modos de acceso principales se usan dentro de la estructura jerárquica.

Cada modo tiene comandos similares. Sin embargo, el modo EXEC privilegiado tiene un nivel de autoridad superior en cuanto a lo que permite que se ejecute.

Modo de usuario

El modo de ejecución usuario, o, para abreviar, EXEC del usuario, tiene capacidades limitadas pero resulta útil en el caso de algunas operaciones básicas. El modo EXEC usuario se encuentra en la parte superior de la estructura jerárquica modal. Este modo es la primera entrada en la CLI de un router IOS.

El modo EXEC del usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo de visualización solamente. El nivel EXEC del usuario no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo.

En forma predeterminada, no se requiere autenticación para acceder al modo EXEC del usuario desde la consola. Siempre conviene asegurarse de que se configure la autenticación durante la configuración inicial.

El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >. Este es un ejemplo que muestra el símbolo > en la petición de entrada:

Switch>

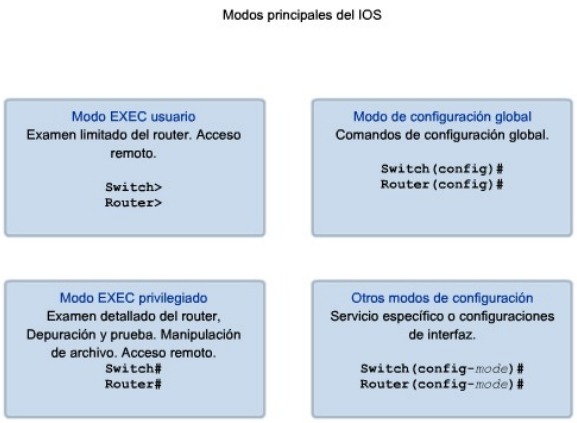
Modo EXEC privilegiado
La ejecución de comandos de configuración y administración requiere que el administrador de red use el modo EXEC privilegiado, o un modo específico que esté más abajo en la jerarquía.

El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #.

Switch#

En forma predeterminada, EXEC privilegiado no requiere autenticación. Siempre conviene asegurarse de que la autenticación esté configurada.

Para ingresar al modo de configuración global y a todos los demás modos de configuración más específicos, es necesario entrar al modo EXEC privilegiado.



Intercambio entre los modos EXEC del usuario y EXEC privilegiado

Los comandos enable y disable se usan para cambiar la CLI entre el modo EXEC del usuario y el modo EXEC privilegiado, respectivamente.

Para acceder al modo EXEC privilegiado, use el comando enable. El modo EXEC privilegiado en ocasiones se denomina modo enable.

La sintaxis para ingresar el comando enable es:

Router>enable

Este comando se ejecuta sin la necesidad de un argumento o una palabra clave. Una vez que se presiona <Intro>, la petición de entrada del router cambia a:

Router#

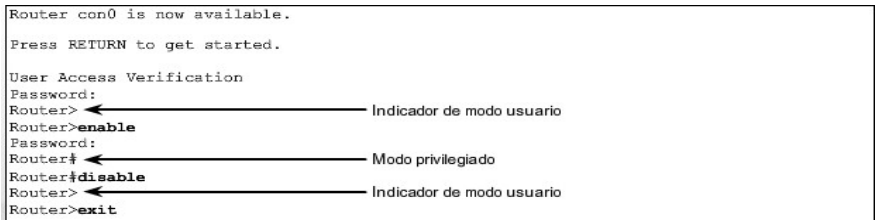
El símbolo # al final de la petición indica que el router está ahora en modo EXEC privilegiado.

Si se ha configurado la autenticación de la contraseña para el modo EXEC privilegiado, el IOS pide la contraseña.
Por ejemplo:

Router>enable
Contraseña:
Router#

El comando disable se usa para volver del modo EXEC privilegiado al modo EXEC del usuario.
Por ejemplo:

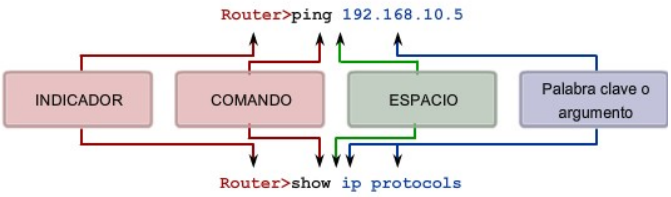
Router#disable
Router>



ESTRUCTURA BASICA DE COMANDOS DE IOS

Cada comando de IOS tiene un formato o sintaxis específicos y se ejecuta con la petición de entrada correspondiente. La sintaxis general para un comando es el comando seguido de las palabras clave y los argumentos correspondientes. Algunos comandos incluyen un subconjunto de palabras clave y argumentos que proporcionan funcionalidad adicional. La figura muestra estas partes de un comando.

Estructura básica de comandos del IOS



Los comandos del indicador están seguidos de un espacio y luego una palabra clave o argumentos.

El comando es la palabra o las palabras iniciales ingresadas en la línea de comandos. Los comandos no distinguen mayúsculas de minúsculas. A continuación del comando siguen una o más palabras clave y argumentos.

Las palabras clave describen parámetros específicos al intérprete de comandos. Por ejemplo, el comando show se usa para mostrar información sobre el dispositivo. Este comando tiene varias palabras clave que pueden usarse para definir el resultado particular que se mostrará. Por ejemplo:

Switch#show running-config

El comando show va seguido de la palabra clave running-config. La palabra clave especifica que se mostrará la configuración en ejecución como resultado.

Un comando podría requerir uno o más argumentos. A diferencia de una palabra clave, generalmente un argumento no es una palabra predefinida. Un argumento es un valor o una variable definida por el usuario. A modo de ejemplo, al aplicar una descripción a una interfaz con el comando description, ingrese una línea como ésta:

Switch(config-if)#description MainHQ Office Switch

El comando es: description. El argumento es: MainHQ Office Switch. El usuario define el argumento. Para este comando, el argumento puede ser cualquier cadena de texto con un máximo de 80 caracteres.

Después de ingresar cada comando completo, incluso cualquier palabra clave y argumento, presione la tecla <Intro> para enviar el comando al intérprete de comandos.

Convenciones de IOS

La figura y los siguientes ejemplos demuestran algunas convenciones para documentar comandos IOS.

Para el comando ping:

Formato:

Router>ping dirección IP

Ejemplo con valores:
Router>ping 10.10.10.5

El comando es ping y el argumento es la dirección IP.

De manera similar, la sintaxis para ingresar el comando traceroute es:

Formato:
Switch>traceroute dirección IP

Ejemplo con valores:
Switch>traceroute 192.168.254.254

El comando es traceroute y el argumento es la dirección IP.

Los comandos se utilizan para ejecutar una acción y las palabras clave se utilizan para identificar dónde o cómo ejecutar el comando.

Por citar otro ejemplo, vuelva a examinar el comando description.

Formato:
Router(config-if)#description cadena

Ejemplo con valores:
Switch(config-if)#description Interfaz para crear una LAN

El comando es description y el argumento aplicado a la interfaz es la cadena de texto, Interfaz para crear una LAN. Una vez que se ejecuta el comando, esa descripción se aplicará a la interfaz específica.

USO DE LA AYUDA DE LA CLI

El IOS ofrece varias formas de ayuda:
Ayuda contextual
Verificación de la sintaxis del comando
Teclas de acceso rápido y métodos abreviados

Ayuda contextual
La ayuda contextual proporciona una lista de comandos y los argumentos asociados con esos comandos dentro del contexto del modo actual. Para acceder a la ayuda contextual, ingrese un signo de interrogación (?) ante cualquier petición de entrada. Habrá una respuesta inmediata sin necesidad de usar la tecla <Intro>.

Uno de los usos de la ayuda contextual es para la obtención de una lista de los comandos disponibles. Dicha lista puede utilizarse cuando existen dudas sobre el nombre de un comando o se desea verificar si el IOS admite un comando específico en un modo determinado.

Por ejemplo, para obtener una lista de los comandos disponibles en el nivel EXEC del usuario, ingrese un signo de interrogación? ante la petición de entrada Router>.

Otro de los usos de la ayuda contextual es visualizar una lista de los comandos o palabras clave que empiezan con uno o varios caracteres específicos. Después de ingresar una secuencia de caracteres, si inmediatamente se ingresa un signo de interrogación, sin espacio, el IOS mostrará una lista de comandos o palabras clave para este contexto que comienzan con los caracteres ingresados.

Por ejemplo, ingrese sh? para obtener una lista de los comandos que empiezan con la secuencia de caracteres sh.

Un último tipo de ayuda contextual se utiliza para determinar qué opciones, palabras clave o argumentos coinciden con un comando específico. Cuando ingresa un comando, escriba un espacio seguido de ? para determinar qué puede o debe ingresarse a continuación.

Como se muestra en la figura, después de ingresar el comando clock set 19:50:00, podemos ingresar el signo ? para determinar las opciones o palabras clave adecuadas para este comando.

Ayuda contextual

Ejemplo de una secuencia de comandos usando la ayuda contextual de CLI

```
Cisco#cl?
clear  clock
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

```
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 25 6
                            ^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Explicaciones de comandos
Mensajes de comandos incompletos
Mensajes de entradas no válidas
Formatos variables

Verificación de la sintaxis del comando

Cuando se envía un comando al presionar la tecla <Intro>, el intérprete de la línea de comandos analiza al comando de izquierda a derecha para determinar qué acción se está solicitando. El IOS generalmente provee sólo comentarios negativos. Si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente. Sin embargo, si el intérprete no puede comprender el comando que se ingresa, mostrará un comentario que describe el error del comando.

Existen tres tipos diferentes de mensajes de error:

- Ambiguous command (comando ambiguo)
- Incomplete command (comando incompleto)
- Incorrect command (comando incorrecto)

Vea la figura para conocer los tipos de errores y las soluciones.

Ayuda para verificar la sintaxis de comandos

El IOS devuelve un mensaje de ayuda que indica que las palabras clave o los argumentos se omitieron del final del comando:

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

El IOS devuelve un mensaje de ayuda para indicar que no hay suficientes caracteres introducidos para que el intérprete de comandos reconozca el comando.

```
Switch#c
% Ambiguous command:'c'
```

El IOS devuelve un "^" para indicar dónde el intérprete de comandos no puede descifrar el comando:

```
Switch#clock set 19:50:00 25 6
                            ^
% Invalid input detected at '^' marker.
```

Ayuda para verificar la sintaxis de comandos

Mensaje de error	Significado	Ejemplos	Cómo obtener ayuda
% Ambiguous command: 'command'	No se introdujeron suficientes caracteres para que el IOS reconozca el comando.	Switch#**c % Ambiguous command:'c'**	Vuelva a introducir el comando seguido de un signo de interrogación (?) sin ningún espacio entre el comando y el signo de interrogación. Aparecen las posibles palabras clave que puede introducir con el comando.
% Incomplete command.	No se ingresaron todas las palabras clave ni los argumentos requeridos.	Switch#**clock set % Incomplete command.**	Vuelva a ingresar el comando seguido de un signo de interrogación (?) con un espacio después de la última palabra. Aparecen las palabras clave o los argumentos requeridos.
% Invalid input detected at '^' marker	El comando se introdujo incorrectamente. El error se produjo donde aparece la marca de acento (^).	Switch#**clock set 19:50:00 25 6** **^** **% Invalid input detected at '^' marker.**	Vuelva a ingresar el comando seguido de un signo de interrogación (?) en un lugar señalado por la marca '^'. También puede ser necesario borrar las últimas palabras clave o argumentos.

Teclas de acceso rápido y métodos abreviados

La interfaz de línea de comandos IOS proporciona teclas de acceso rápido y métodos abreviados que facilitan la configuración, el monitoreo y la resolución de problemas.

La figura muestra la mayoría de los métodos abreviados. Merece la pena tener en cuenta de manera especial los siguientes:

- Tab: completa la parte restante del comando o palabra clave
- Ctrl-R: vuelve a mostrar una línea
- Ctrl-Z: sale del modo de configuración y vuelve al EXEC
- Flecha hacia abajo: permite al usuario desplazarse hacia adelante a través de los comandos anteriores
- Flecha hacia arriba: permite al usuario desplazarse hacia atrás a través de los comandos anteriores
- Ctrl-Shift-6: permite al usuario interrumpir un proceso IOS tal como ping o traceroute
- Ctrl-C: cancela el comando actual y sale del modo configuración

Análisis con mayor profundidad:

Tab: Tab complete se utiliza para completar la parte restante de los comandos y parámetros abreviados, si la abreviatura contiene suficientes letras para diferenciarse de cualquier otro comando o parámetro actualmente disponible. Cuando se ha ingresado una parte suficiente del comando o la palabra clave como para que sean únicos, presione la tecla Tab y la CLI mostrará el resto del comando o palabra clave.

Ésta es una buena técnica para usar cuando se está aprendiendo, porque permite ver la palabra completa utilizada para el comando o palabra clave.

Ctrl-R: Volver a mostrar línea actualizará la línea recientemente ingresada. Use Ctrl-R para volver a mostrar la línea. Por ejemplo, puede ocurrir que el IOS esté reenviando un mensaje a la CLI justo cuando se está escribiendo una línea. Puede usar Ctrl-R para actualizar la línea y evitar tener que volver a escribirla.

En este ejemplo, aparece en medio de un comando un mensaje sobre una falla en una interfaz.

Switch#show mac-
16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down
16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down

Para volver a mostrar la línea que estaba escribiendo use Ctrl-R:

Switch#show mac

Ctrl-Z: Salir del modo de configuración. Para salir de un modo de configuración y regresar al modo EXEC privilegiado, use Ctrl-Z. Dado que el IOS tiene una estructura jerárquica de modos, el usuario puede encontrarse varios niveles hacia abajo. En lugar de salir de cada modo en forma individual, use Ctrl-Z para volver directamente a la petición de entrada de EXEC privilegiado en el nivel superior.

Flechas arriba y abajo: uso de comandos anteriores. El software IOS de Cisco almacena temporalmente varios caracteres y comandos anteriores de manera tal que las entradas puedan recuperarse. El búfer es útil para reingresar comandos sin tener que volver a escribir.

Existen secuencias clave para desplazarse a través de estos comandos almacenados en el búfer. Use la tecla flecha hacia arriba (Ctrl P) para visualizar los comandos previamente ingresados. Cada vez que se presiona esta tecla, se mostrará el siguiente comando sucesivo anterior. Use la tecla flecha hacia abajo (Ctrl N) para desplazarse hacia adelante en el historial y visualizar los comandos más recientes.

Ctrl-Shift-6: uso de la secuencia de escape. Cuando se inicia un proceso del IOS desde la CLI, como un ping o traceroute, el comando se ejecuta hasta que se termina o interrumpe. Mientras el proceso está en ejecución, la CLI no responde. Para interrumpir el resultado e interactuar con la CLI, presione Ctrl-Shift-6.

Ctrl-C: interrumpe la entrada de un comando y sale del modo de configuración. Resulta útil cuando se ingresa un comando que luego se decide cancelar y se sale del modo de configuración.

Comandos o palabras clave abreviados. Los comandos y las palabras clave pueden abreviarse a la cantidad mínima de caracteres que identifica a una selección única. Por ejemplo, el comando configure puede abreviarse en conf ya que configure es el único comando que empieza con conf. La abreviatura con no dará resultado ya que hay más de un comando que empieza con con.

Las palabras clave también pueden abreviarse.

Otro ejemplo podría ser show interfaces, que se puede abreviar de la siguiente manera:

```
Router#show interfaces
Router#show int
```

Se puede abreviar tanto el comando como las palabras clave, por ejemplo:

```
Router#sh int
```

Teclas de acceso rápido y métodos abreviados de CLI

Edición de línea de CLI	
Tab	Completa una entrada de nombre de comando parcial.
Retroceso	Borra el carácter a la izquierda del cursor.
Ctrl-D	Borra el carácter donde está el cursor.
Ctrl-K	Borra todos los caracteres desde el cursor hasta el final de la línea de comandos.
Esc D	Borra todos los caracteres desde el cursor hasta el final de la palabra.
Ctrl-U o Ctrl-X	Borra todos los caracteres desde el cursor hasta el comienzo de la línea de comandos.
Ctrl-W	Borra la palabra a la izquierda del cursor.
Ctrl-W	Desplaza el cursor hacia el principio de la línea.
Tecla flecha izquierda o Ctrl-B	Desplaza el cursor un carácter hacia la izquierda.
Esc B	Desplaza el cursor una palabra hacia la izquierda.
Esc F	Desplaza el cursor una palabra hacia la derecha.
Tecla flecha derecha o Ctrl-F	Desplaza el cursor un carácter hacia la derecha.
Ctrl-E	Desplaza el cursor hasta el final de la línea de comandos.
Tecla flecha arriba o Ctrl-P	Vuelve a introducir el comando que se encuentra en el búfer del historial, a partir de los comandos más recientes.
Ctrl-R o Ctrl-I o Ctrl-L	Vuelve a mostrar la petición de entrada del sistema y la línea de comando después de que se recibe un mensaje de la consola.

(NOTA: "Eliminar", la tecla para eliminar a la derecha del cursor, no es reconocida por los programas de emulación de terminales.)

En la petición "-----More-----"	
Tecla Intro	Muestra la siguiente línea.
Barra espaciadora	Muestra la siguiente pantalla.
Cualquier otra tecla alfanumérica	Regresa al indicador EXEC.

Teclas Pausa	
Ctrl-C	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC privilegiado. Cuando está en modo de configuración, interrumpe y regresa al indicador de comando.
Ctrl-Z	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de pausa multiuso. Se la utiliza para interrumpir búsquedas DNS, traceroutes, pings.

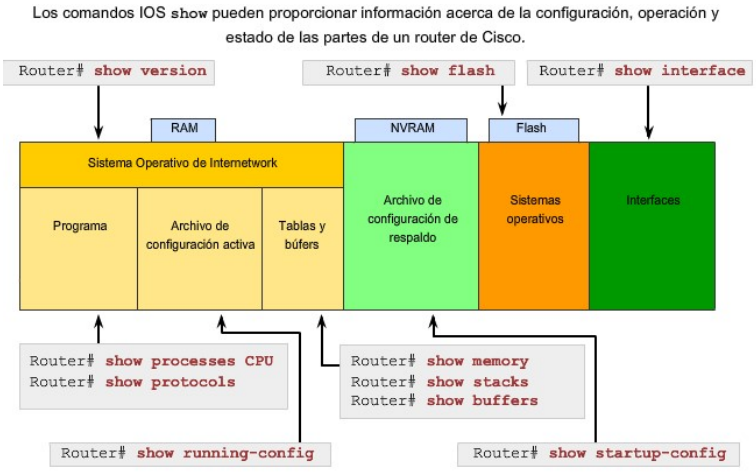
Nota: Teclas de control: Mantenga presionada la tecla <Ctrl> y luego presione la tecla de la letra específica.
Secuencias de escape: Presione y libere la tecla <Esc> y luego presione la tecla de la letra.

COMANDO DE “ANÁLISIS” DE IOS

Para verificar y resolver problemas en la operación de la red, debemos examinar la operación de los dispositivos. El comando básico de examen es el comando show.

Existen muchas variantes diferentes de este comando. A medida que el usuario adquiera más conocimientos sobre IOS, aprenderá a usar e interpretar el resultado de los comandos show. Use el comando show ? para obtener una lista de los comandos disponibles en un modo o contexto determinado.

La figura muestra cómo el típico comando show puede proporcionar información sobre la configuración, la operación y el estado de partes de un router.



Algunos de los comandos más utilizados son:

show interfaces

Muestra estadísticas para todas las interfaces del dispositivo. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido del número de puerto/ranura de la interfaz específica. Por ejemplo:

Router#show interfaces serial 0/1

show version

Muestra información sobre la versión de software actualmente cargada, además de información sobre el hardware y el dispositivo.

show arp: muestra la tabla ARP del dispositivo.
show mac-address-table: (sólo switch) muestra la tabla MAC de un switch.
show startup-config: muestra la configuración guardada que se ubica en la NVRAM.
show running-config: muestra el contenido del archivo de configuración actualmente en ejecución o la configuración para una interfaz específica, o información de clase de mapa.
show ip interfaces: muestra las estadísticas IPv4 para todas las interfaces de un router. Para ver las estadísticas de una interfaz específica, ejecute el comando show ip interfaces seguido del número de puerto/ranura de la interfaz específica. Otro formato importante de este comando es show ip interface brief. Es útil para obtener un resumen rápido de las interfaces y su estado operativo.

Por ejemplo:

Router#show ip interface brief

Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 172.16.255.254 YES manual up up
FastEthernet0/1 unassigned YES unset down down
Serial0/0/0 10.10.10.5 YES manual up up
Serial0/0/1 unassigned YES unset down down

La petición de entrada More

Cuando un comando devuelve más resultados de los que pueden mostrarse en una única pantalla, aparece la petición de entrada --More-- en la parte inferior de la pantalla. Cuando aparece la petición de entrada --More--, presione la barra espaciadora para visualizar el tramo siguiente del resultado. Para visualizar sólo la siguiente línea, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancela el resultado y se vuelve a la petición de entrada.

MODO DE CONFIGURACIÓN

El modo de configuración principal recibe el nombre de configuración global o global config. Desde configuración global, se realizan cambios en la configuración de la CLI que afectan la operación del dispositivo en su totalidad.

El modo de configuración global también se usa como precursor para acceder a modos de configuración específicos.

El siguiente comando de la CLI se usa para cambiar el dispositivo del modo EXEC privilegiado al modo de configuración global y para permitir la entrada de comandos de configuración desde una terminal:

Router#configure terminal

Una vez que se ejecuta el comando, la petición de entrada cambia para mostrar que el router está en modo de configuración global.

Router(config)#

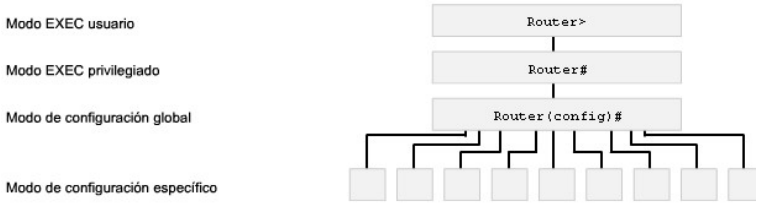
Modos de configuración específicos

Desde el modo de configuración global, pueden ingresarse muchos modos de configuración diferentes. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. La lista que se presenta a continuación muestra algunos de ellos:

Modo de interfaz: para configurar una de las interfaces de red (Fa0/0, S0/0/0, etc.).
Modo de línea: para configurar una de las líneas (física o virtual) (consola, ,auxiliar, VTY, etc.).
Modo de router: para configurar los parámetros de uno de los protocolos de enrutamiento.

La figura muestra las peticiones de entrada para algunos modos. Recuerde que como los cambios de configuración se hacen en una interfaz o proceso, los cambios sólo afectan a esa interfaz o proceso.

Modos de configuración del IOS



Modo de configuración	Indicador
Interfaz	Router(config-if)#
Línea	Router(config-line)#
Routers	Router(config-router)#

Para salir de un modo de configuración específico y volver al modo de configuración global, ingrese exit ante la petición de entrada. Para salir completamente del modo de configuración y volver al modo EXEC privilegiado, ingrese end o use la secuencia de teclas Ctrl-Z.

Cuando se ha realizado un cambio desde el modo global, conviene guardarlo en el archivo de configuración de inicio almacenado en la NVRAM. Así se evita que los cambios se pierdan por cortes de energía o un reinicio intencional. El comando para guardar la configuración en ejecución en el archivo de configuración de inicio es:

Router#copy running-config startup-config

APLICACIÓN DE UNA CONFIGURACIÓN BÁSICA CON IOS

LOS DISPOSITIVOS NECESITAN NOMBRES

El nombre de host se usa en las peticiones de entrada de la CLI. Si el nombre de host no está explícitamente configurado, el router usa el nombre de host predeterminado, asignado de fábrica, "Router". El switch tiene el nombre de host predeterminado, asignado de fábrica, "Switch". Imagine que una internetwork tiene varios routers y todos recibieron el nombre predeterminado "Router". Se crearía una importante confusión durante la configuración y el mantenimiento de la red.

Cuando se accede a un dispositivo remoto con Telnet o SSH, es importante tener la confirmación de que se ha hecho una conexión al dispositivo adecuado. Si todos los dispositivos quedaran con sus nombres predeterminados, no se podría identificar que el dispositivo correcto esté conectado.

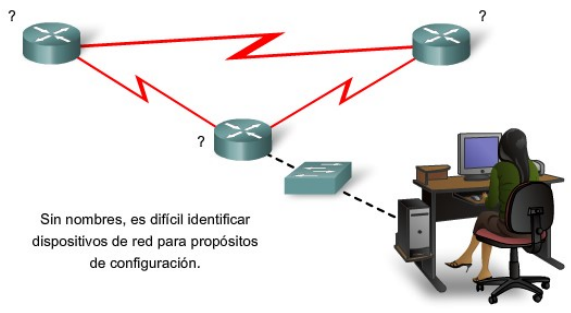
Al elegir y documentar nombres atinadamente, resulta más fácil recordar, analizar e identificar los dispositivos de red. Para nombrar los dispositivos de manera uniforme y provechosa, es necesario el establecimiento de una convención de denominación que se extienda por toda la empresa o, al menos, por la división. Siempre conviene crear la convención de denominación al mismo tiempo que el esquema de direccionamiento para permitir la continuidad dentro de la organización.

Según ciertas pautas de convenciones de denominación, los nombres deberían:

- Comenzar con una letra
- No incluir espacios
- Finalizar con una letra o dígito
- Incluir caracteres que sólo sean letras, dígitos y guiones
- Tener 63 caracteres o menos

Los nombres de hosts utilizados en el IOS del dispositivo conservan su uso de mayúsculas y minúsculas. Por lo tanto, es posible escribir un nombre con mayúsculas como se haría normalmente. Esto contrasta con la mayoría de los esquemas de denominación de Internet, donde los caracteres en mayúsculas y minúsculas reciben igual trato. RFC 1178 provee algunas de las reglas que pueden usarse como referencia para la denominación de dispositivos.

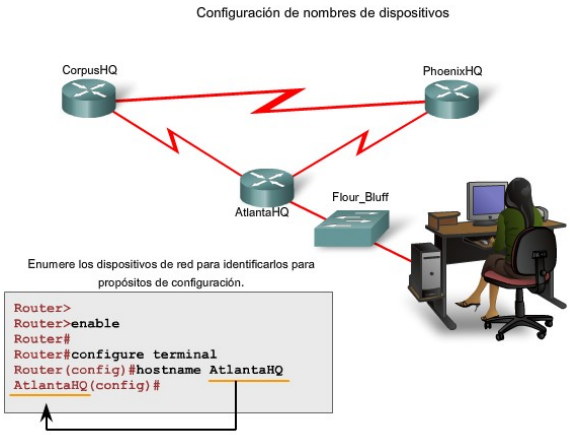
Como parte de la configuración del dispositivo, debe configurarse un nombre de host único para cada dispositivo.



Nota: Sólo los administradores usan los nombres de host de los dispositivos cuando usan la CLI para configurar y monitorear los dispositivos. A menos que estén configurados

para hacerlo, los dispositivos no usan estos nombres cuando se detectan entre sí e interoperan.
Aplicación de nombres: ejemplo

Veamos un ejemplo de tres routers conectados en una red que abarca tres ciudades diferentes (Atlanta, Phoenix y Corpus) como se muestra en la figura.



Para crear una convención de denominación para los routers, se debe tener en cuenta la ubicación y el propósito de los dispositivos. Pregúntese lo siguiente: ¿Serán estos routers parte de la sede de una organización? ¿Tiene cada router un propósito diferente? Por ejemplo, ¿es el router de Atlanta un punto de unión principal en la red o es una unión en una cadena?

En este ejemplo, cada router se identificará como una sucursal de la sede para cada ciudad. Los nombres podrían ser AtlantaHQ, PhoenixHQ y CorpusHQ. Si cada router hubiera sido una unión en una cadena sucesiva, los nombres podrían haber sido AtlantaJunction1, PhoenixJunction2 y CorpusJunction3.

En la documentación de la red, se incluirán estos nombres y los motivos de su elección, a fin de asegurar la continuidad de nuestra convención de denominación a medida que se agregan dispositivos.

Una vez que se ha identificado la convención de denominación, el próximo paso es aplicar los nombres al router usando la CLI. Este ejemplo nos conducirá a través del proceso de denominación del router de Atlanta.

Configuración del nombre de host de IOS

Desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando configure terminal:

```
Router#configure terminal
```

Después de que se ejecuta el comando, la petición de entrada cambiará a:

```
Router(config)#
```

En el modo global, ingrese el nombre de host:

```
Router(config)#hostname AtlantaHQ
```

Después de que se ejecuta el comando, la petición de entrada cambiará a:

AtlantaHQ(config)#

Observe que el nombre de host aparece en la petición de entrada. Para salir del modo global, use el comando exit.

Siempre asegúrese de que la documentación esté actualizada cada vez que se agrega o modifica un dispositivo. Identifique los dispositivos en la documentación por su ubicación, propósito y dirección.

Nota: Para anular los efectos de un comando, establezca el prefacio del comando con la palabra clave no.

Por ejemplo, para eliminar el nombre de un dispositivo, utilice:

```
AtlantaHQ(config)#no hostname
Router(config)#
```

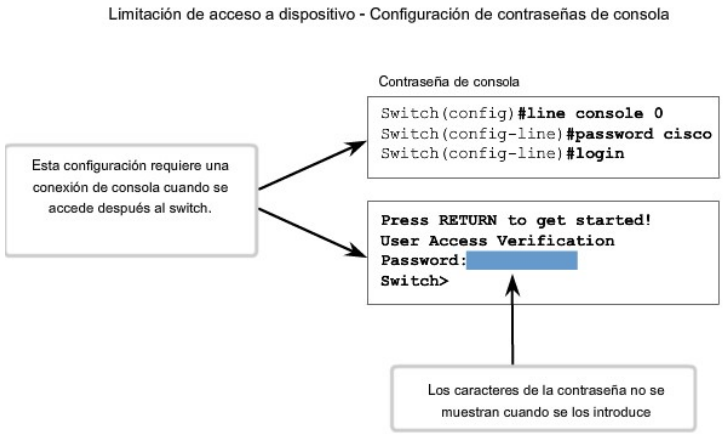
Nótese que el comando no hostname provocó que el router volviera a usar el nombre de host predeterminado "Router".

Enlaces

RFC 1178, "Choosing a Name for Your Computer" (Elección de un nombre para su computadora),

http://www.faqs.org/rfcs/rfc1178.html

LIMITACIÓN DE ACCESO A DISPOSITIVO: CONFIGURACIÓN DE CONTRASEÑAS Y USO DE MENSAJES



Contraseña de enable y contraseña secreta de enable

Para proporcionar una mayor seguridad, utilice el comando enable password o el comando enable secret. Puede usarse cualquiera de estos comandos para establecer la autenticación antes de acceder al modo EXEC privilegiado (enable).

Si es posible, siempre use el comando enable secret, no el comando anterior enable password. El comando enable secret provee mayor seguridad porque la contraseña está encriptada. El comando enable password puede usarse sólo si enable secret no se ha configurado aún.

Los siguientes comandos se utilizan para configurar las contraseñas:

```
Router(config)#enable password contraseña
Router(config)#enable secret contraseña
```

Contraseña de VTY

Las líneas vty permiten el acceso a un router a través de Telnet. Es necesario configurar una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las conexiones. Sin embargo, con frecuencia conviene configurar una única contraseña para una línea a fin de proporcionar un recurso secundario para el ingreso administrativo al dispositivo si las demás conexiones están en uso.

Los siguientes comandos se usan para configurar una contraseña en líneas vty:

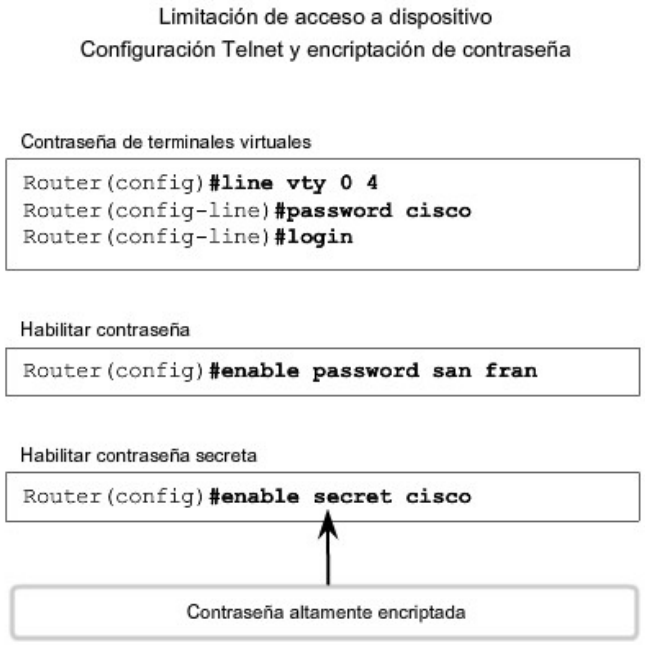
```
Router(config)#line vty 0 4
Router(config-line)#password contraseña
Router(config-line)#login
```

En forma predeterminada, el IOS incluye el comando login en las líneas VTY. Esto impide el acceso Telnet al dispositivo sin la previa solicitud de autenticación. Si por error, se configura el comando no login, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de Telnet. Esto representaría un riesgo importante para la seguridad.

Visualización de contraseñas de encriptación

Existe otro comando de utilidad que impide que las contraseñas aparezcan como texto sin cifrar cuando se visualizan los archivos de configuración. Ese comando es el service password-encryption.

Este comando provee la encriptación de la contraseña cuando ésta se configura. El comando service password-encryption aplica una encriptación débil a todas las contraseñas no encriptadas. Esta encriptación no se aplica a las contraseñas cuando se envían a través de medios únicamente en la configuración. El propósito de este comando es evitar que individuos no autorizados vean las contraseñas en el archivo de configuración.



Si se ejecuta el comando show running-config o show startup-config antes de ejecutar el comando service password-encryption, las contraseñas no encriptadas estarán visibles en el resultado de configuración. El comando service password-encryption puede entonces ejecutarse y se aplicará la encriptación a las contraseñas. Una vez que se ha aplicado la encriptación, la cancelación del servicio de encriptación no revierte la encriptación.

Mensajes de aviso

Aunque el pedido de contraseñas es un modo de impedir el acceso a la red de personas no autorizadas, resulta vital proveer un método para informar que sólo el personal autorizado debe intentar obtener acceso al dispositivo. Para hacerlo, agregue un aviso a la salida del dispositivo.

Los avisos pueden ser una parte importante en los procesos legales en el caso de una demanda por el ingreso no autorizado a un dispositivo. Algunos sistemas legales no permiten la acusación, y ni siquiera el monitoreo de los usuarios, a menos que haya una notificación visible.

El contenido o las palabras exactas de un aviso dependen de las leyes locales y de las políticas de la empresa. A continuación se muestran algunos ejemplos de información que se debe incluir en un aviso:

"El uso del dispositivo es exclusivo del personal autorizado".
"Es posible que se esté controlando la actividad".
"Se iniciarán acciones legales en caso de uso no autorizado".

Ya que cualquier persona que intenta iniciar sesión puede ver los avisos, se debe redactar el mensaje cuidadosamente. Es inapropiada toda redacción que implique que "se acepta" o "se invita" al usuario a iniciar sesión. Si una persona causa problemas en la red luego de obtener acceso no autorizado, será difícil probar la responsabilidad si hay algún indicio de invitación.

La creación de avisos es un proceso simple; sin embargo, éstos deben usarse en forma apropiada. Cuando se usa un aviso, nunca debe invitar a un usuario al router. Debe aclarar que sólo el personal autorizado tiene permitido el acceso al dispositivo. Asimismo, el aviso puede incluir cierres programados del sistema y demás información que afecte a todos los usuarios de la red.

El IOS proporciona varios tipos de avisos. Un aviso común es el mensaje del día (MOTD). Con frecuencia se usa para notificaciones legales ya que se visualiza en todos los terminales conectados.

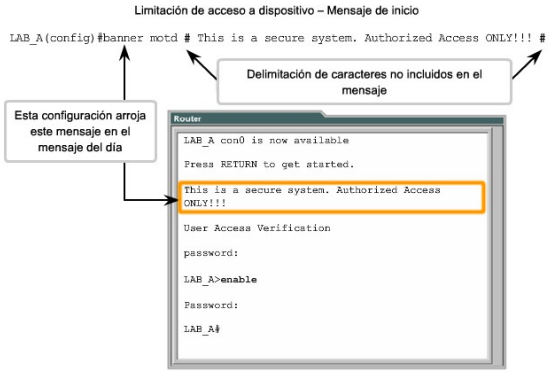
Configure el MOTD con el comando banner motd del modo global.

Como se muestra en la figura, el comando banner motd requiere el uso de delimitadores para identificar el contenido del mensaje del aviso. El comando banner motd va seguido de un espacio y un carácter delimitador. Luego, se ingresan una o más líneas de texto para representar el mensaje del aviso. Una segunda ocurrencia del carácter delimitador denota el final del mensaje. El carácter delimitador puede ser cualquier carácter siempre que no aparezca en el mensaje. Por este motivo, a menudo se usan símbolos como "#".

Para configurar un MOTD, ingrese el comando banner motd desde el modo de configuración global:

```
Switch(config)#banner motd # mensaje #
```

Una vez que se ha ejecutado el comando, aparecerá el aviso en todos los intentos posteriores de acceso al dispositivo hasta que el aviso se elimine.



ADMINISTRACIÓN DE ARCHIVOS DE CONFIGURACIÓN

Como se analizó anteriormente, la modificación de la configuración en ejecución afecta el funcionamiento del dispositivo en forma inmediata.

Después de hacer cambios en una configuración, considere estas opciones como siguiente paso:

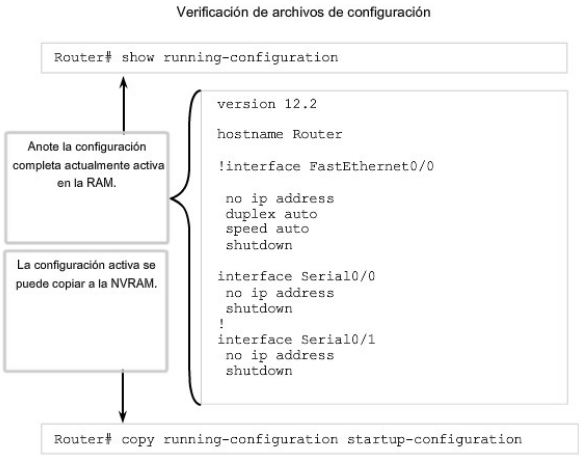
1. Convertir la configuración cambiada en la nueva configuración de inicio.
2. Volver a la configuración original del dispositivo.
3. Eliminar toda la configuración del dispositivo.

1. *Establecer la configuración modificada como la nueva configuración de inicio.*

Recuerde: ya que la configuración en ejecución se almacena en la RAM, se encuentra temporalmente activa mientras se ejecuta (se encuentra encendido) el dispositivo. Si se corta la energía al router o si se reinicia el router, se perderán todos los cambios de configuración a menos que se hayan guardado.

Al guardar la configuración en ejecución en el archivo de configuración de inicio en la NVRAM se mantienen los cambios como la nueva configuración de inicio.

Antes de asignar los cambios, use los correspondientes comandos show para verificar la operación del dispositivo. Como se muestra en la figura, se puede utilizar el comando show running-config para ver un archivo de configuración en ejecución.



Cuando se verifica que los cambios son correctos, utilice el comando copy running-config startup-config en la petición de entrada del modo EXEC privilegiado. El siguiente ejemplo muestra el comando:

```
Switch#copy running-config startup-config
```

Una vez ejecutado, el archivo de configuración en ejecución reemplaza al archivo de configuración de inicio.

2. *Volver a la configuración original del dispositivo*

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado, puede ser necesario volver a la configuración previa del dispositivo. Suponiendo que no se ha sobreescrito la configuración de inicio con los cambios, se puede reemplazar la configuración en ejecución por la configuración de inicio. La mejor manera de hacerlo es reiniciando el dispositivo con el comando reload ante la petición de entrada del modo EXEC privilegiado.

Cuando se inicia una recarga, el IOS detectará que la configuración en ejecución tiene cambios que no se guardaron en la configuración de inicio. Aparecerá una petición de entrada para preguntar si se desean guardar los cambios realizados. Para descartar los cambios, ingrese n o no.

Aparecerá otra petición de entrada para confirmar la recarga. Para confirmar, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancelará el proceso.

Por ejemplo:

```
Router#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2004 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 processor with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled
```

Copia de respaldo de las configuraciones sin conexión

Los archivos de configuración deben guardarse como archivos de respaldo ante cualquier problema que surja. Los archivos de configuración se pueden almacenar en un servidor Trivial File Transfer Protocol (TFTP), un CD, una barra de memoria USB o un disquete almacenado en un lugar seguro. Un archivo de configuración también tendría que incluirse en la documentación de red.

Configuración de respaldo en el servidor TFTP

Como se muestra en la figura, una opción es guardar la configuración en ejecución o la configuración de inicio en un servidor TFTP. Utilice el comando copy running-config tftp o copy startup-config tftp y siga estos pasos:

1. Ingrese el comando copy running-config tftp.
2. Ingrese la dirección IP del host en el cual se almacenará el archivo de configuración.
3. Ingrese el nombre que se asignará al archivo de configuración.
4. Presione Intro para confirmar cada elección.

Estudie la figura para observar este proceso.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!! [OK]
```

3. Eliminación de todas las configuraciones

Si se guardan cambios no deseados en la configuración de inicio, posiblemente sea necesario eliminar todas las configuraciones. Esto requiere borrar la configuración de inicio y reiniciar el dispositivo.

La configuración de inicio se elimina con el uso del comando erase startup-config .

Para borrar el archivo de configuración de inicio utilice erase NVRAM:startup-config o erase startup-config en la petición de entrada del modo EXEC privilegiado:

Router#erase startup-config

Una vez que se ejecuta el comando, el router solicitará la confirmación:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Confirm es la respuesta predeterminada. Para confirmar y borrar el archivo de configuración de inicio, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancelará el proceso.

Precaución: Use el comando erase con cautela. Este comando puede utilizarse para borrar cualquier archivo del dispositivo. El uso incorrecto del comando puede borrar el IOS mismo u otro archivo esencial.

Después de eliminar la configuración de inicio de la NVRAM, recargue el dispositivo para eliminar el archivo de configuración actual en ejecución de la memoria RAM. El dispositivo cargará entonces la configuración de inicio predeterminada que se envió originalmente con el dispositivo en la configuración en ejecución.

Configuraciones de respaldo con captura de texto (HyperTerminal)

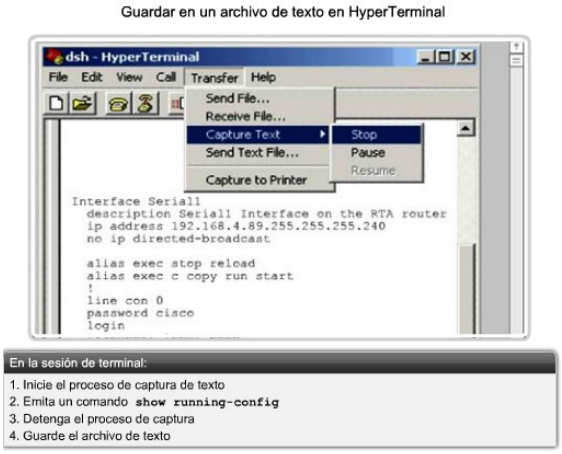
Los archivos de configuración pueden guardarse o archivarse en un documento de texto. Esta secuencia de pasos asegura la disponibilidad de una copia utilizable de los archivos de configuración para su modificación o reutilización en otra oportunidad.

Cuando se use HyperTerminal, siga estos pasos:

1. En el menú Transfer, haga clic en Capture Text.
2. Elija la ubicación.

3. Haga clic en Start para comenzar la captura del texto.
4. Una vez que la captura ha comenzado, ejecute el comando show running-config o show startup-config ante la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
5. Una vez que se han visualizado las configuraciones, haga clic en Stop para finalizar la captura.
6. Observe el resultado para verificar que no esté dañado.

Observe el ejemplo en la figura.



Configuraciones de respaldo con captura de texto (TeraTerm)

Los archivos de configuración pueden guardarse o archivarse en un documento de texto mediante TeraTerm.

Como se muestra en la figura, los pasos son:

1. En el menú File, haga clic en Log.
2. Elija la ubicación. TeraTerm comenzará a capturar texto.
3. Una vez que la captura ha comenzado, ejecute el comando show running-config o show startup-config ante la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
4. Cuando la captura haya finalizado, seleccione Close en TeraTerm: Ventana de registro.
5. Observe el resultado para verificar que no esté dañado.

Restauración de las configuraciones de texto

Se puede copiar un archivo de configuración desde el almacenamiento a un dispositivo. Cuando se copia en la terminal, el IOS ejecuta cada línea del texto de configuración como un comando. Esto significa que el archivo necesitará edición para asegurar que las contraseñas encriptadas estén en forma de texto y que se eliminen los mensajes de IOS y el texto de no comando, como "--More--". Este proceso se analiza en la práctica de laboratorio.

A su vez, en la CLI, el dispositivo debe establecerse en el modo de configuración global para recibir los comandos del archivo de texto que se copia.

Cuando se usa HyperTerminal, los pasos son:

1. Ubicar el archivo que se debe copiar en el dispositivo y abrir el documento de texto.

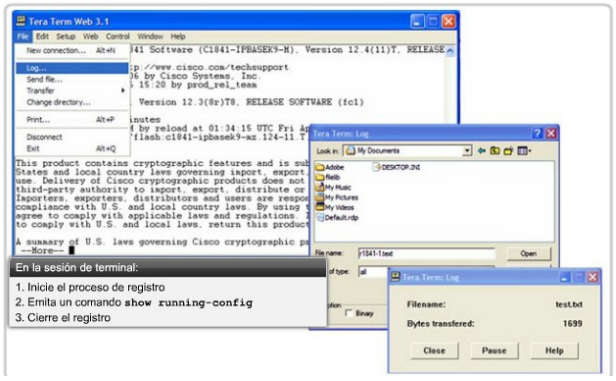
2. Copiar el texto completo.
3. En el menú Edit, haga clic en paste to host.

Cuando se usa TeraTerm, los pasos son:

1. En el menú File haga clic en Send para enviar el archivo.
2. Ubique el archivo que debe copiar en el dispositivo y haga clic en Open.
3. TeraTerm pegará el archivo en el dispositivo.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Éste es un método conveniente para configurar manualmente un router.

Guardar en un archivo de texto en TeraTerm



CONFIGURACIÓN DE INTERFACES

La mayoría de los dispositivos de red intermediarios tienen una dirección IP para la administración del dispositivo. Algunos dispositivos, como los switches y los puntos de acceso inalámbricos, pueden operar sin tener una dirección IP.

Dado que el objetivo de un router es interconectar diferentes redes, cada interfaz en un router tiene su propia dirección IPv4 exclusiva. La dirección asignada a cada interfaz existe en una red separada dedicada a la interconexión de routers.

Hay muchos parámetros que pueden configurarse en las interfaces del router. Analizaremos los comandos de interfaz más básicos, que se resumen en la figura.

Configuración de las interfaces del router

Se accede a todas las interfaces ejecutando el comando **interface** en la petición de configuración global.

En los siguientes comandos, el argumento *teclear* incluye serial, ethernet, fastethernet y otros:

```
Router(config)#interface teclear puerto
Router(config)#interface teclear ranura/puerto
Router(config)#interface teclear ranura/ranura secundaria/puerto
```

El siguiente comando se utiliza para desactivar la interfaz de forma administrativa:

```
Router(config-if)#shutdown
```

El siguiente comando se utiliza para activar una interfaz que se desactivó:

```
Router(config-if)#no shutdown
```

El siguiente comando se utiliza para salir del modo de configuración de interfaz actual:

```
Router(config-if)#exit
```

Cuando la configuración está completa, la interfaz queda habilitada y se sale del modo de configuración de interfaz.

Configuración de las interfaces Ethernet del router

Las interfaces Ethernet del router se utilizan como gateway para los dispositivos finales en las LAN conectadas directamente al router.

Cada interfaz Ethernet debe tener una dirección IP y una máscara de subred para enrutar paquetes IP.

Para configurar una interfaz Ethernet, siga estos pasos:

1. Ingrese el modo de configuración global.
2. Ingrese el modo de configuración de interfaz.
3. Especifique la máscara de subred y la dirección de la interfaz.
4. Habilite la interfaz.

Como se muestra en la figura, configure la dirección IP de Ethernet mediante los siguientes comandos:

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address dirección ip máscara de red
Router(config-if)#no shutdown
```

Habilitación de la interfaz

De manera predeterminada, las interfaces se encuentran deshabilitadas. Para habilitar una interfaz, ingrese el comando no shutdown en el modo de configuración de interfaz. Si es necesario desactivar una interfaz por cuestiones de mantenimiento o para resolver problemas, use el comando shutdown.

Configuración de las interfaces seriales del router

Las interfaces seriales se usan para conectar WAN a routers en un sitio remoto o ISP.
Para configurar una interfaz serial, siga estos pasos:

1. Ingrese el modo de configuración global.
2. Ingrese el modo de interfaz.
3. Especifique la máscara de subred y la dirección de la interfaz.
4. Si el cable de conexión es DCE, fije la frecuencia de reloj. Omita este paso si el cable es DTE.
5. Encienda la interfaz.

Cada interfaz serial conectada debe tener una dirección IP y una máscara de subred para enrutar paquetes IP.

Configure la dirección IP con los siguientes comandos:

```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address dirección ip máscara de red
```

Las interfaces seriales necesitan una señal de temporización para controlar los tiempos de la comunicación. En la mayoría de los entornos, un dispositivo DCE como por ejemplo un CSU/DSU, proporciona dicha señal. En forma predeterminada, los routers son dispositivos DTE, pero pueden configurarse como dispositivos DCE.

En los enlaces seriales interconectados directamente, como en nuestro entorno de laboratorio, un extremo debe operar como DCE para proporcionar la señal del reloj. Se activa el reloj y la velocidad se especifica con el comando clock rate. Algunas frecuencias de bit pueden no estar disponibles en ciertas interfaces seriales. Esto depende de la capacidad de cada interfaz.

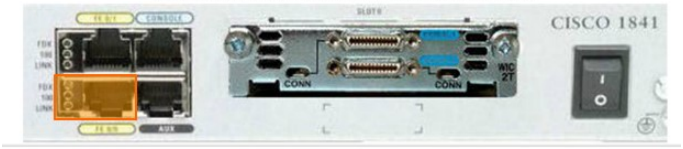
En la práctica de laboratorio, si debe establecerse una frecuencia de reloj en una interfaz identificada como DCE, se debe usar la frecuencia de reloj 56000.

Como se muestra en la figura, los comandos que se utilizan para establecer una frecuencia de reloj y habilitar una interfaz serial son:

```
Router(config)#interface Serial 0/0/0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

Una vez que se aplicaron los cambios de configuración en el router, recuerde utilizar los comandos show para verificar la precisión de los cambios y luego guardar la configuración modificada como configuración de inicio.

Configuración de las interfaces Ethernet del router




```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configure las interfaces seriales del router


```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Así como el nombre del host ayuda a identificar el dispositivo en una red, una descripción de interfaz indica el propósito de la interfaz. Una descripción de lo que una interfaz hace o dónde está conectada debe ser parte de la configuración de cada interfaz. Esta descripción puede ser útil para la resolución de problemas.

La descripción de interfaz aparecerá en el resultado de estos comandos: show startup-config, show running-config y show interfaces.

Por ejemplo, esta descripción proporciona información valiosa sobre el propósito de la interfaz:

Esta interfaz es el gateway para la LAN administrativa.

Una descripción puede ayudar a determinar los dispositivos o las ubicaciones conectadas a la interfaz. A continuación, se proporciona otro ejemplo:

La interfaz F0/0 está conectada al switch principal en el edificio administrativo.

Cuando el personal de soporte puede identificar con facilidad el propósito de una interfaz o de un dispositivo conectado, puede comprender más fácilmente el alcance del problema, y esto puede conducir a la resolución más pronta del problema.

Para crear una descripción, use el comando description. Este ejemplo muestra los comandos utilizados para crear una descripción para una interfaz FastEthernet:

```
HQ-switch1#configure terminal
HQ-switch1(config)#interface fa0/1
HQ-switch1(config-if)#description Conectarse al switch principal del Edificio A
```

Una vez que se aplica la descripción a la interfaz, utilice el comando show interfaces para verificar que la descripción sea correcta.

Observe el ejemplo en la figura.

Configuración de una interfaz de switch

Un switch LAN es un dispositivo intermediario que interconecta segmentos dentro de una red. Por lo tanto, las interfaces físicas en el switch no tienen direcciones IP. A diferencia de un router en el que las interfaces están conectadas a diferentes redes, una interfaz física en un switch conecta dispositivos dentro de una red.

Las interfaces de switch también están habilitadas en forma predeterminada. Como se muestra en la figura del Switch 1, podemos asignar descripciones, pero no es necesario habilitar la interfaz.

Configuración del switch

```
Switch#configure terminal
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#description To TAM switch
Switch(config-if)#exit
Switch(config)#hostname Flour_Bluff
Flour_Bluff(config)#exit
Flour_Bluff#
```

Para poder administrar un switch, asignamos direcciones al dispositivo hacia dicho switch. Con una dirección IP asignada al switch, actúa como dispositivo host. Una vez que se asigna la dirección, se accede al switch con telnet, ssh o servicios Web.

La dirección para un switch se asigna a una interfaz virtual representada como una interfaz LAN virtual (VLAN). En la mayoría de los casos, esta es la interfaz VLAN 1. En la figura del Switch 2, se

asigna una dirección IP a la interfaz VLAN 1. Al igual que las interfaces físicas de un router, también se debe activar esta interfaz con el comando no shutdown.

Como cualquier otro host, el switch necesita una dirección de gateway definida para comunicarse fuera de la red local. Como se muestra en la figura del Switch 2, este gateway se asigna con el comando ip default-gateway.

Configuración del switch

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#exit
Switch#
```

VERIFICACIÓN DE LA CONECTIVIDAD

PRUEBA DE STACK

El comando ping

El comando ping es una manera eficaz de probar la conectividad. La prueba se denomina prueba de stack de protocolos, porque el comando ping se mueve desde la Capa 3 del Modelo OSI hasta la Capa 2 y luego hacia a la Capa 1. El ping utiliza el protocolo ICMP (Protocolo de mensajes de control de Internet) para comprobar la conectividad.

Uso de ping en una secuencia de prueba

En esta sección se utilizará el comando ping del router IOS en una secuencia de pasos planificada para establecer conexiones válidas, comenzando por el dispositivo individual y luego extendiéndose a la LAN y, por último, a las redes remotas. Mediante el uso del comando ping en esta secuencia ordenada, los problemas pueden aislarse. El comando ping no siempre indicará con precisión la naturaleza del problema, pero puede ayudar a identificar el origen del problema, un primer paso importante en la resolución de una falla en la red.

El comando ping proporciona un método para comprobar la stack de protocolos y la configuración de la dirección IPv4 en un host. Existen herramientas adicionales que pueden proporcionar más información que el ping, como Telnet o Trace.

Indicadores de ping IOS

Un ping de IOS cederá a una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:
!: indica la recepción de una respuesta de eco ICMP.
.: indica un límite de tiempo cuando se espera una respuesta.
U: se recibió un mensaje ICMP inalcanzable.

El "!" (signo de exclamación) indica que el ping se completó correctamente y verifica la conectividad de la Capa 3.

El "." (punto) puede indicar problemas en la comunicación. Puede señalar que ocurrió un problema de conectividad en algún sector de la ruta. También puede indicar que un router a lo largo de la ruta no tenía una ruta hacia el destino y no envió un mensaje ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo.

La "U" indica que un router del camino no tenía una ruta hacia la dirección de destino y respondió con un mensaje ICMP inalcanzable.

Prueba de loopback

A modo de primer paso en la secuencia de prueba, se utiliza el comando ping para verificar la configuración IP interna en el host local. Recuerde que esta prueba se cumple con el comando ping en una dirección reservada denominada loopback (127.0.0.1). Esto verifica la correcta operación del stack de protocolos desde la capa de red a la capa Física, y viceversa, sin colocar realmente una señal en el medio.

Los comandos ping se ingresan en una línea de comandos.

Ingrese el comando de loopback ping con esta sintaxis:

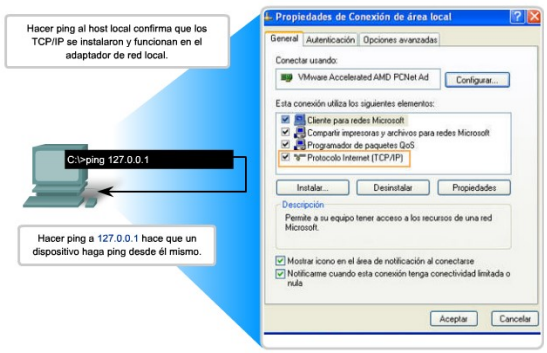
C:\>ping 127.0.0.1

La respuesta de este comando se parecería a ésta:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

El resultado indica que se enviaron cuatro paquetes (cada uno con un tamaño de 32 bytes) y se devolvieron del host 127.0.0.1 en un tiempo menor a 1 milisegundo. TTL significa Tiempo de vida y define la cantidad de saltos que le quedan al paquete de ping antes de que se descarte.

Prueba del stack TCP/IP local



PRUEBA DE LA ASIGNACIÓN DE INTERFAZ

Del mismo modo que se usan comandos y utilidades para verificar la configuración de un host, se deben aprender los comandos para verificar las interfaces de dispositivos intermediarios. El IOS proporciona comandos para verificar el funcionamiento de interfaces de router y switch.

Verificación de las interfaces del router

Uno de los comandos más usados es el comando show ip interface brief. Este proporciona un resultado más abreviado que el comando show ip interface. Proporciona además un resumen de la información clave de todas las interfaces.

Si se observa la figura del Router 1, se puede ver que este resultado muestra todas las interfaces conectadas al router, la dirección IP, si la hay, asignada a cada interfaz y el estado operativo de la interfaz.

Si se observa la línea de la interfaz FastEthernet 0/0, se ve que la dirección IP es 192.168.254.254. Si se observan las dos últimas columnas, se advierte el estado de la interfaz de Capa 1 y Capa 2. El up en la columna de estado muestra que esta interfaz está en funcionamiento en la Capa 1. El up en la columna de protocolo señala que el protocolo de Capa 2 está funcionando.

En la misma figura, se observa que la interfaz serial 0/0/1 no ha sido habilitada. La indicación correspondiente es administratively down en la columna de estado. Esta interfaz puede habilitarse con el comando no shutdown.

Prueba de conectividad del router

Como con un dispositivo final, es posible verificar la conectividad de la Capa 3 con los comandos ping y traceroute. En la figura del Router 1 se puede ver un ejemplo de los resultados de un ping a un host en la LAN local y un trace a un host remoto a través de la WAN.

Prueba de interfaz

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method  Status                Protocol
FastEthernet0/0        192.168.254.254 YES NVRAM   up                    up
FastEthernet0/1/0      unassigned      YES unset   down                  down
Serial0/0/0            172.16.0.254    YES NVRAM   up                    up
Serial0/0/1            unassigned      YES unset   administratively down down

Router1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
  1 172.16.0.253 8 msec 4 msec 8 msec
  2 10.0.0.254 16 msec 16 msec 8 msec
  3 192.168.0.1 16 msec * 20 msec
```

Verificación de las interfaces del switch

Al examinar la figura del Switch 1 se puede ver el uso del comando show ip interface brief para verificar la condición de las interfaces del switch. Como se aprendió anteriormente, la dirección IP para el switch se aplica a una interfaz VLAN (Red de área local virtual). En este caso, se asigna una dirección IP 192.168.254.250 a la interfaz Vlan1. También se puede observar que esta interfaz está habilitada y en funcionamiento.

Al examinar la interfaz FastEthernet0/1, se puede detectar que esta interfaz está desactivada. Esto quiere decir que no hay un dispositivo conectado a la interfaz o que la interfaz de red de los dispositivos conectada no está funcionando.

Por otro lado, los resultados de las interfaces FastEthernet0/2 y FastEthernet0/3 muestran que están en funcionamiento. Esto se indica en el Estado y en el Protocolo, cuando ambos se muestran activos.

Prueba de la conectividad del switch

Del mismo modo que otros hosts, el switch puede probar la conectividad de su Capa 3 con los comandos ping y traceroute. La figura del Switch1 también muestra un ping al host local y un trace a un host remoto.

No deben olvidarse dos cosas importantes: que no se requiere una dirección IP para que un switch cumpla su tarea de reenvío de trama y que el switch requiere un gateway para comunicarse con el exterior de su red local.

Prueba de interfaz

```
Switch1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      192.168.254.250 YES manual up                    up
FastEthernet0/1            unassigned      YES unset  down                  down
FastEthernet0/2            unassigned      YES unset  up                    up
FastEthernet0/3            unassigned      YES unset  up                    up
<se omite el resultado>
```

```
Switch1#ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Switch1#traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
  1 192.168.254.254   4 msec 2 msec 3 msec
  2 172.16.0.253   8 msec 4 msec 8 msec
  3 10.0.0.254   16 msec 16 msec 8 msec
  4 192.168.0.1   16 msec * 20 msec
```

Prueba de interfaz

El siguiente paso en la secuencia de prueba es verificar que la dirección NIC esté unida a la dirección IPv4 y que la NIC esté lista para transmitir señales a través de los medios.

En este ejemplo, que también se muestra en la figura, asumimos que la dirección IPv4 asignada a una NIC es 10.0.0.5.

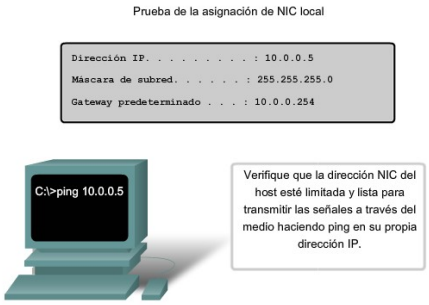
Para verificar la dirección IPv4, siga estos pasos:

En la línea de comandos, ingrese lo siguiente:

C:\>ping 10.0.0.5
A successful reply would resemble:
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Esta prueba verifica que el controlador de la NIC y la mayor parte del hardware de la NIC están funcionando correctamente. También verifica que la dirección IP esté correctamente unida a la NIC, sin colocar realmente una señal en los medios.

Si la prueba falla, es probable que existan problemas con el controlador del software y el hardware de la NIC que pueden requerir la reinstalación de uno de ellos, o de ambos. Este procedimiento depende del tipo de host y su sistema operativo.



PRUEBA DE LA RED LOCAL

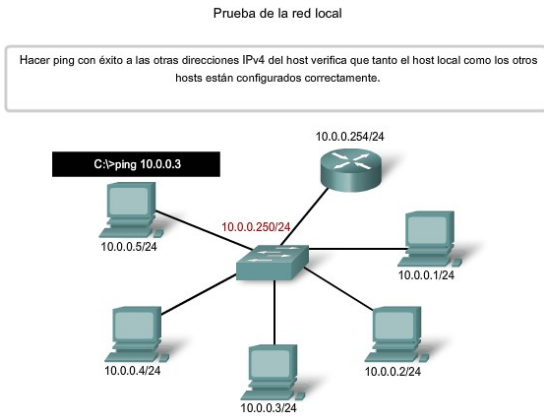
La siguiente prueba de la secuencia corresponde a los hosts en la LAN local.

Al hacer ping a los hosts remotos satisfactoriamente se verifica que tanto el host local (en este caso, el router) como el host remoto estén configurados correctamente. Esta prueba se realiza al hacer ping a cada host en forma individual en la LAN.

Observe el ejemplo en la figura.

Si un host responde con el mensaje "Destination Unreachable" (destino inalcanzable), observe qué dirección no fue satisfactoria y continúe haciendo ping a los otros hosts de la LAN.

Otro mensaje de falla es "Request Timed Out" (la solicitud ha expirado). Indica que no hubo respuesta al intento del ping en el período de tiempo predeterminado, lo cual indica que el problema puede estar en la latencia de red.



PRUEBA DE GATEWAY Y CONECTIVIDAD REMOTA

El siguiente paso de la secuencia de prueba es utilizar el comando ping para verificar que un host local puede conectarse con una dirección de gateway. Esto es sumamente importante porque el gateway es la entrada y salida del host hacia la red más amplia. Si el comando ping devuelve una respuesta satisfactoria, se verifica la conectividad al gateway.

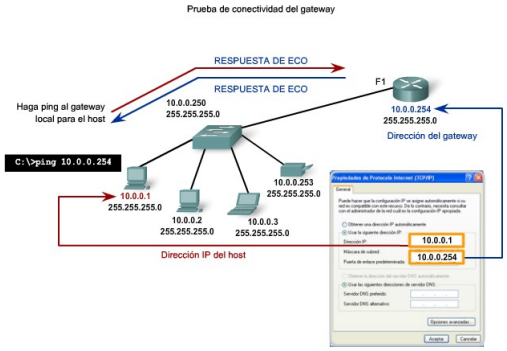
Para comenzar, elija una estación como dispositivo de origen. En este caso, se optó por 10.0.0.1, como se indica en la figura. Use el comando ping para llegar a la dirección del gateway, en este caso 10.0.0.254.

c:\>ping 10.0.0.254

La dirección IPv4 del gateway debería ser fácil de conseguir en la documentación de la red, pero si no se encontrara disponible, utilice el comando ipconfig para detectar la dirección IP del gateway.

Si la prueba de gateway falla, retroceda un paso en la secuencia y pruebe otro host en la LAN local para verificar que el problema no sea el host origen. Luego verifique la dirección de gateway con el administrador de red a fin de asegurar que se esté probando la dirección correcta.

Si todos los dispositivos están configurados en forma adecuada, controle el cableado físico para asegurar que esté firme y correctamente conectado. Mantenga un registro preciso de los intentos que se han realizado para verificar la conectividad. Esto será de ayuda para solucionar este problema y, tal vez, problemas futuros.



Prueba del siguiente salto en la ruta

En un router, use el IOS para probar el siguiente salto de las rutas individuales. Como se analizó anteriormente, la tabla de enrutamiento muestra el siguiente salto de cada ruta. Para determinar el siguiente salto, examine la tabla de enrutamiento desde el resultado del comando show ip route. Los paquetes que trasladan tramas y que se dirigen a la red destino indicada en la tabla de enrutamiento se envían al dispositivo que representa el siguiente salto. Si el siguiente salto es inaccesible, el paquete se descarta. Para probar el siguiente salto, determine la ruta apropiada hacia el destino y trate de hacer ping al siguiente salto apropiado para esa ruta en la tabla de enrutamiento. Una falla en el ping indica que puede existir un problema de configuración o de hardware. Sin embargo, el ping también puede estar prohibido por la seguridad del dispositivo. Si el ping tiene éxito puede pasar a probar la conectividad a hosts remotos.

Prueba de hosts remotos

Una vez que se ha completado la verificación de la LAN local y el gateway, la prueba puede continuar con los dispositivos remotos, lo cual es el siguiente paso en la secuencia de prueba.

La figura ilustra un ejemplo de topología de la red. Hay 3 hosts dentro de una LAN, un router (que actúa como gateway) que está conectado a otro router (que actúa como gateway para una LAN remota) y 3 hosts remotos. Las pruebas de verificación deben comenzar dentro de la red local y progresar externamente hacia los dispositivos remotos.

Comience con la prueba de la interfaz externa de un router que esté directamente conectada a una red remota. En este caso, el comando ping prueba la conexión a 192.168.0.253, la interfaz externa del router del gateway de la red local.

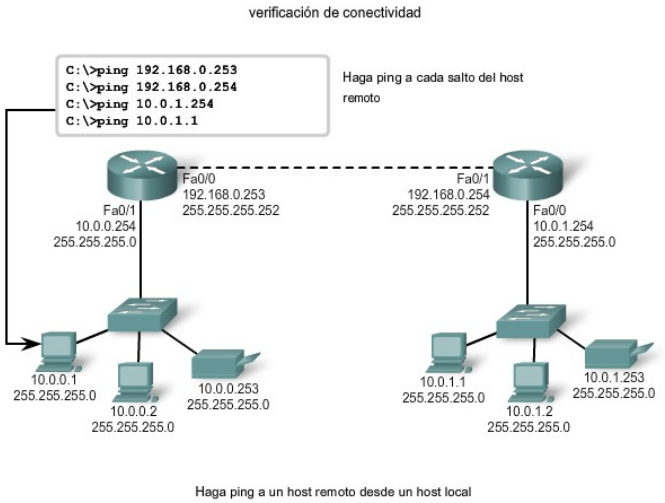
Si el comando ping resulta satisfactorio, se verifica la conectividad a la interfaz externa. A continuación, haga ping a la dirección IP externa del router remoto, en este caso, 192.168.0.254. Si es satisfactorio, se verifica la conectividad del router remoto. Si se produce una falla, intente aislar el problema. Vuelva a realizar la prueba hasta que exista una conexión válida a un dispositivo y verifique dos veces cada una de las direcciones.

El comando ping no siempre será de ayuda para identificar el motivo subyacente de un problema, pero puede aislar los problemas y orientar el proceso de resolución de problemas. Documente cada prueba, los dispositivos involucrados y los resultados.

Verifique la conectividad remota del router

Un router establece una conexión entre ciertas redes gracias al reenvío de paquetes entre ellas. Para reenviar paquetes entre dos redes dadas, el router debe poder comunicarse tanto con la red de origen como con la red de destino. El router necesitará rutas hacia ambas redes en su tabla de enrutamiento.

Para probar la comunicación hacia la red remota, se puede hacer ping a un host conocido en esta red remota. Si no puede hacer ping correctamente en el host de la red remota desde un router, primero debe verificar la tabla de enrutamiento en busca de una ruta adecuada hacia cada red remota. Es posible que el router use la ruta predeterminada para llegar a un destino. Si no hay una ruta para llegar a esta red, será necesario determinar por qué no existe la ruta. Como siempre, también se debe descartar que el ping no esté prohibido administrativamente.



RASTREO O INTERPRETACIÓN DE LOS RESULTADOS DE RASTREO

rastreo.

Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red. La forma del comando depende de dónde se emita el comando. Cuando lleve a cabo el rastreo desde un equipo con Windows, utilice tracert. Cuando lleve a cabo el rastreo desde la CLI de un router, utilice traceroute.

Ping y Trace

Ping y trace pueden utilizarse en forma conjunta para diagnosticar un problema.

Supongamos que se ha establecido una conexión satisfactoria entre el Host 1 y el Router A, como se muestra en la figura.

Luego, supongamos que el Host 1 hace ping al Host 2 mediante este comando.

C:\>ping 10.1.0.2

El comando ping devuelve este resultado:

Pinging 10.1.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
The ping test failed.

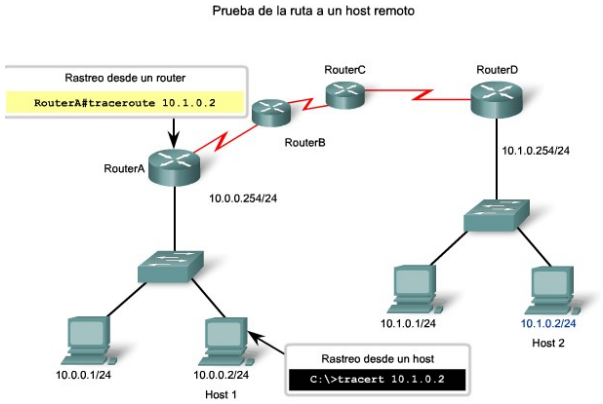
Ésta es una prueba de comunicación más allá de la red local a un dispositivo remoto. Dado que el gateway local respondió pero el host más distante no lo hizo, el problema parece estar en algún punto fuera de la red local. Un próximo paso es aislar el problema de una red en particular fuera de la red local. Los comandos trace pueden mostrar la ruta de la última comunicación satisfactoria.

Trace a un host remoto

Del mismo modo que los comandos ping, los comandos trace se ingresan en la línea de comandos y toman una dirección IP como argumento.

Suponiendo que se emitirá el comando desde una computadora con Windows, se utilizará el formato tracert:

C:\>tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
1 2 ms 2 ms 2 ms 10.0.0.254
2 * * * Request timed out.
3 * * * Request timed out.
4 ^C
La única respuesta satisfactoria provino del gateway en el Router A. Las solicitudes de rastreo al siguiente salto expiraron, lo cual significa que el siguiente salto no respondió. Los resultados del comando trace indican que la falla entonces se encuentra en la internetwork más allá de la LAN.



Secuencia de prueba: Unificación

A modo de revisión, recorramos la secuencia de prueba en otra situación.

Prueba 1: Loopback local: Exitoso

C:\>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

El Host 1 tiene la stack de IP configurada correctamente.

Prueba 2: NIC local: Exitosa

C:\>ping 192.168.23.3
Pinging 192.168.23.3 with 32 bytes of data:
Reply from 192.168.23.3: bytes=32 time<1ms TTL=128
Reply from 192.168.23.3: bytes=32 time<1ms TTL=128
Reply from 192.168.23.3: bytes=32 time<1ms TTL=128
Reply from 192.168.23.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.23.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Se asignó correctamente la dirección IP a la NIC y la electrónica de la NIC responde a la dirección IP.

Prueba 3: Ping de gateway local: Exitoso

C:\>ping 192.168.23.254
Pinging 192.168.23.254 with 32 bytes of data:
Reply from 192.168.23.254: bytes=32 time<1ms TTL=128
Reply from 192.168.23.254: bytes=32 time<1ms TTL=128
Reply from 192.168.23.254: bytes=32 time<1ms TTL=128
Reply from 192.168.23.254: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.23.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

El gateway predeterminado está en funcionamiento. De esta manera también se verifica el funcionamiento de la red local.

Prueba 4: Ping de host remoto: falla

C:\>ping 192.168.11.1
Pinging 192.168.11.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Request timed out.
Ping statistics for 192.168.11.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Esta es una prueba de la comunicación más allá de la red local. Dado que el gateway respondió pero el host más distante no lo hizo, el problema parece estar en algún punto más allá de la red local.

Prueba 5: Traceroute al host remoto: Falla en el primer salto
C:\>tracert 192.168.11.1
Tracing route to 192.168.11.1 over a maximum of 30 hops
1 * * * Request timed out.
2 * * * Request timed out.
3 ^C

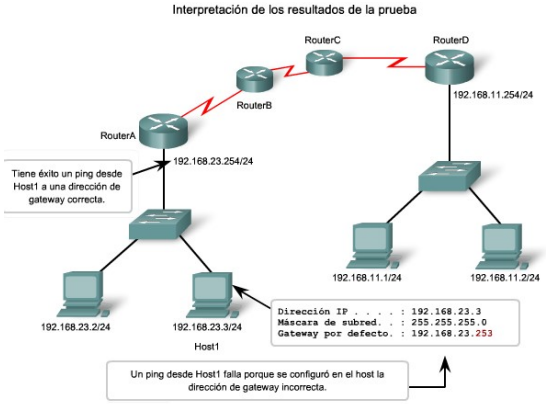
Parece haber resultados contradictorios. El gateway por defecto responde, lo cual indica que existe comunicación entre el Host1 y el gateway. Por otro lado, el gateway parece no estar respondiendo a traceroute.

Una explicación posible es que el host local no esté correctamente configurado para usar 192.168.23.254 como gateway predeterminado. Para confirmarlo se analizará la configuración del Host1.

Prueba 6: Análisis de configuración de host para determinar el gateway local apropiado: Incorrecto
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
IP Address. . . . . : 192.168.23.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.23.253

A partir del resultado del comando ipconfig se puede determinar que el gateway no se encuentra configurado correctamente en el host. Esto explica la falsa indicación de que el problema se encontraba en la internetwork fuera de la red local. Aunque la dirección 192.168.23.254 respondía, esta no era la dirección configurada en el Host1 como gateway.

Al no poder construir una trama, el Host1 descarta el paquete. En este caso, no hay respuesta indicada desde el rastreo al host remoto.



MONITOREO Y DOCUMENTACIÓN DE RED

LINEAS DE BASE DE RED FUNDAMENTALES

Una de las herramientas más efectivas para controlar y resolver problemas relacionados con el rendimiento de la red es establecer una línea de base de red. Una línea de base es un proceso para estudiar la red en intervalos regulares a fin de asegurar que la red funciona según su diseño. Es más que un simple informe que detalla el estado de la red en un momento determinado. La creación de una línea de base efectiva del rendimiento de la red se logra con el tiempo. La medición del rendimiento en distintos momentos y de las cargas le ayudará al usuario a tener una idea más precisa del rendimiento general de la red.

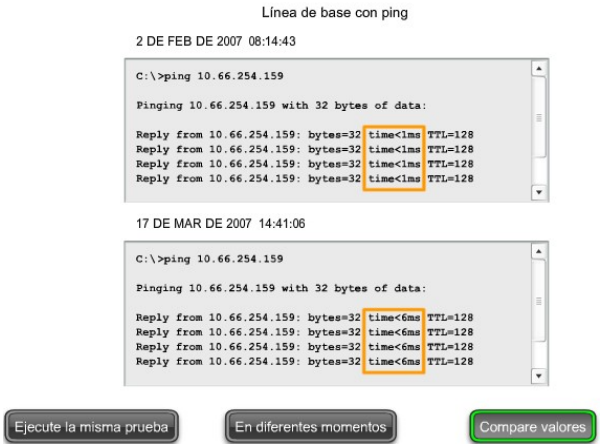
El resultado que deriva de los comandos de la red puede aportar datos a la línea de base de red. La figura muestra la información que se debe registrar.

Un método para iniciar una línea de base es copiar y pegar en un archivo de texto los resultados de los comandos ping, trace u otro comando relevante. Estos archivos de texto pueden tener grabada la fecha y la hora y pueden guardarse en un archivo para su posterior recuperación.

Un uso efectivo de la información guardada es comparar los resultados en el transcurso del tiempo. Entre los elementos que se deben considerar se encuentran los mensajes de error y los tiempos de respuesta de host a host. Si se observa un aumento considerable de los tiempos de respuesta, es posible que exista un problema de latencia para considerar.

No bastan las palabras para destacar la importancia de crear documentación. La verificación de la conectividad de host a host, los problemas de latencia y las resoluciones de problemas identificados puede ayudar a un administrador de red a mantener el funcionamiento más eficiente posible de la red.

Las redes corporativas deben tener líneas de base extensas. Existen herramientas de software a nivel profesional para almacenar y mantener información de línea de base. Analizaremos algunas técnicas básicas y el propósito de las líneas de base.



NOCIONES SOBRE LOS NODOS DE LA RED

Si existe un esquema de direccionamiento adecuado, la identificación de direcciones IPv4 para los dispositivos de una red debería ser tarea sencilla. Sin embargo, la identificación de las direcciones físicas (MAC) puede resultar una tarea desalentadora. Necesitaría acceso a todos los dispositivos y tiempo suficiente para visualizar la información, un host por vez. Debido a que esta opción en muchos casos no resulta práctica, existe un medio alternativo para la identificación de direcciones MAC a través del comando arp.

El comando arp proporciona la asignación de direcciones físicas a direcciones IPv4 conocidas. Un método común para ejecutar el comando arp es ejecutarlo desde la petición de entrada del comando. Este método implica el envío de una solicitud de ARP. El dispositivo que necesita la información envía una solicitud de ARP broadcast a la red y sólo el dispositivo local que concuerda con la dirección IP de la solicitud envía una respuesta ARP que contiene su par IP-MAC.

Para ejecutar un comando arp, en el indicador del sistema de un host ingrese:
C:\host1>arp -a

Como se muestra en la figura, el comando arp enumera todos los dispositivos que se encuentran actualmente en la caché ARP, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché mediante el comando arp -d en caso de que el administrador de red desee volver a llenarla con información actualizada.

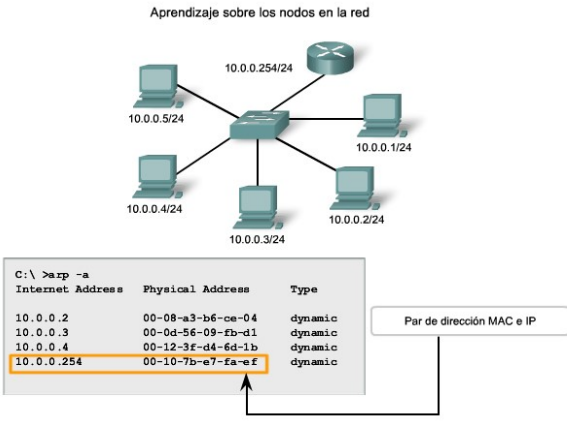
Nota: El caché ARP sólo se carga con información de dispositivos a los que se ha accedido recientemente. Para asegurar que la caché ARP esté cargada, haga ping a un dispositivo de manera tal que tenga una entrada en la tabla ARP.

Barrido de ping

Otro método para reunir direcciones MAC es hacer un ping sweep a través de un rango de direcciones IP. Un barrido de ping es un método de escaneo que puede ejecutarse en la línea de comandos o mediante el uso de herramientas de administración de red. Estas herramientas proporcionan un método para especificar un rango de hosts a los que se hará ping con un comando.

A través del barrido de ping, se pueden generar datos de red de dos maneras. En primer lugar, muchas de las herramientas de barrido de ping construyen una tabla con los hosts que responden. Estas tablas a menudo enumeran a los hosts según la dirección IP y la dirección MAC. Así se obtiene un mapa de los hosts activos en el momento del barrido.

A medida que se intenta cada ping, se realiza una solicitud de ARP para obtener la dirección IP en la caché ARP. De tal modo, se activa cada host al que se ha accedido recientemente y se garantiza que la tabla ARP esté actualizada. El comando arp puede mostrar la tabla de direcciones MAC, como se mencionó anteriormente, pero ahora se puede confiar razonablemente en que la tabla ARP está actualizada.



Conexiones del switch

Una herramienta adicional que puede resultar útil es un mapeo de cómo están conectados los hosts a un switch. Este mapeo puede obtenerse ejecutando el comando show tabla de direcciones mac.

Por medio de una línea de comandos de un switch, ingrese el comando show con el argumento tabla de direcciones mac:

Sw1-2950#show tabla de direcciones mac

Vea la figura para obtener un ejemplo del resultado.

La tabla que aparece en la figura enumera la dirección MAC de los hosts que se encuentran conectados a este switch. Como otros resultados en la ventana de comando, esta información puede copiarse y pegarse en un archivo. Los datos también pueden pegarse en una hoja de cálculo para una manipulación más sencilla en el futuro.

El análisis de esta tabla también revela que la interfaz Fa0/23 es un segmento compartido o está conectada a otro switch. Varias direcciones MAC representan múltiples nodos. Esto indica que un puerto está conectado a otro dispositivo intermediario, como por ejemplo un hub, un punto de acceso inalámbrico u otro switch.

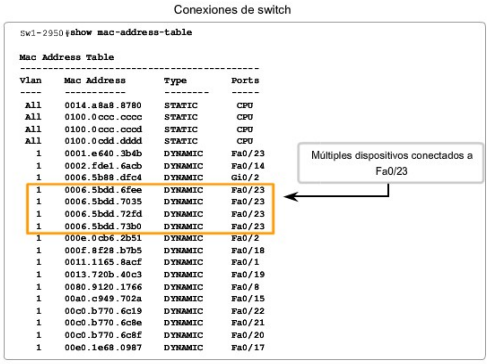


Tabla que muestra las direcciones MAC conectadas a las interfaces del switch