Por lo general, las redes domésticas interconectan una amplia variedad de dispositivos finales, como computadoras portátiles y de escritorio, tablet PC, smartphones, televisores inteligentes y reproductores de medios de red que cumplen con los requisitos de la Digital Living Network Alliance (DLNA), como las consolas Xbox 360 o Playstation 3, entre otros.

Por lo general, todos estos dispositivos finales están conectados a un router doméstico. En realidad, los routers domésticos son cuatro dispositivos en uno:

* **Router** **:** reenvía paquetes de datos a Internet y recibe paquetes de datos de ella.
* **Switch** **:** conecta dispositivos finales mediante cables de red.
* **Punto de acceso inalámbrico** **:**consta de un transmisor de radio que puede conectar dispositivos finales en forma inalámbrica.
* **Dispositivo de firewall** **:** protege el tráfico saliente y restringe el tráfico entrante.

En las redes empresariales más grandes, con muchos más dispositivos y mucho más tráfico, estos se suelen incorporar como dispositivos independientes y autónomos que proporcionan un servicio dedicado. Los dispositivos finales, como las computadoras portátiles y de escritorio, se conectan a los switches de red mediante conexiones por cable. Para enviar paquetes más allá de la red local, los switches de red se conectan a routers de red. Entre los demás dispositivos de infraestructura en una red, se incluyen los puntos de acceso inalámbrico y los dispositivos de seguridad dedicados, como los firewalls.

Cada dispositivo es muy diferente en lo que respecta al hardware, el uso y la capacidad. Sin embargo, en todos los casos, el sistema operativo es lo que permite que el hardware funcione.

Prácticamente en todos los dispositivos para usuarios finales y de red conectados a Internet se utilizan sistemas operativos. Entre los dispositivos para usuarios finales, se incluyen los dispositivos como smartphones, tablet PC y computadoras portátiles y de escritorio. Los dispositivos de red, o intermediarios, se utilizan para transportar datos a través de la red. Entre estos se incluyen los switches, los routers, los puntos de acceso inalámbrico y los firewalls. El sistema operativo de un dispositivo de red se conoce como “sistema operativo de red”.

Sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco es un término genérico para la colección de sistemas operativos de red que se utilizan en los dispositivos de red Cisco. Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo de dispositivo.

En este capítulo, se hace referencia a una topología de red básica que consta de dos switches y dos PC, a fin de demostrar el uso de Cisco IOS.

Todos los dispositivos finales y de red conectados a Internet requieren un sistema operativo (SO) que los ayude a realizar sus funciones.

Al encender una computadora se carga el SO, por lo general desde una unidad de disco, en la RAM. La parte del código del SO que interactúa directamente con el hardware de la computadora se conoce como núcleo. La porción que interactúa con las aplicaciones y el usuario se conoce como “shell”. El usuario puede interactuar con el shell mediante la interfaz de línea de comandos (CLI, command-line interface) o la interfaz gráfica de usuario (GUI, graphical user interface).

Al emplear la CLI, el usuario interactúa directamente con el sistema en un entorno basado en texto introduciendo comandos con el teclado en una ventana de petición de entrada de comandos. El sistema ejecuta el comando y, por lo general, proporciona una respuesta en forma de texto. La interfaz GUI permite que el usuario interactúe con el sistema en un entorno que utiliza imágenes gráficas, formatos multimedia y texto. Las acciones se llevan a cabo al interactuar con las imágenes en la pantalla. La GUI es más fácil de usar y requiere un menor conocimiento de la estructura de comandos para utilizar el sistema. Por este motivo, muchas personas prefieren los entornos GUI. Muchos sistemas operativos ofrecen tanto una GUI como una CLI.

Haga clic en las porciones de Hardware, Núcleo y Shell de la ilustración para obtener más información.

A la mayoría de los sistemas operativos de los dispositivos finales, incluidos MS Windows, MAC OS X, Linux, Apple iOS y Android, entre otros, se accede mediante una GUI.

El sistema operativo de los routers domésticos generalmente se denomina “firmware”. El método más frecuente para configurar un router doméstico consiste en utilizar un explorador Web para acceder a una GUI fácil de usar. La mayoría de los routers domésticos habilitan la actualización del firmware a medida que se detectan nuevas características o vulnerabilidades de seguridad.

Los dispositivos de red de infraestructura utilizan un sistema operativo de red. El sistema operativo de red que se utiliza en los dispositivos Cisco se denomina Sistema operativo Internetwork (IOS, Internetwork Operating System). “Cisco IOS” es un término genérico para la colección de sistemas operativos de red que se utilizan en los dispositivos de red Cisco. Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo de dispositivo. El método más frecuente para acceder a estos dispositivos consiste en utilizar una CLI.

Este capítulo se centra en la topología de switch de la red de una pequeña empresa. La topología consta de dos switches y dos PC, y se utilizará para demostrar el uso de Cisco IOS mediante la CLI.

Los sistemas operativos de red se asemejan en gran medida a los sistemas operativos de PC. Los sistemas operativos realizan una serie de funciones técnicas “detrás de escena” que habilitan a los usuarios a hacer lo siguiente:

* Utilizar un mouse.
* Ver resultados en un monitor.
* Introducir comandos de texto.
* Seleccionar opciones en una ventana de cuadro de diálogo.

Las funciones “detrás de escena” de los switches y los routers son muy similares. El IOS de un switch o un router proporciona una interfaz a los técnicos de red. El técnico puede introducir comandos para configurar o programar el dispositivo a fin de que lleve a cabo diversas funciones de redes. Los detalles operativos de los IOS en los dispositivos de internetworking varían según el propósito del dispositivo y las características que admite.

Cisco IOS es un término que abarca diferentes sistemas operativos que se ejecutan en diversos dispositivos de redes. Existen muchas variaciones distintas de Cisco IOS:

* IOS para switches, routers y otros dispositivos de red Cisco
* Versiones numeradas de IOS para un dispositivo de red Cisco determinado
* Conjuntos de características de IOS que proporcionan paquetes específicos de características y servicios

Al igual que una PC puede ejecutar Microsoft Windows 8 y una MacBook puede ejecutar OS X, un dispositivo de red Cisco ejecuta una versión específica de Cisco IOS. La versión de IOS depende del tipo de dispositivo que se utilice y de las características necesarias. Si bien todos los dispositivos traen un IOS y un conjunto de características predeterminados, es posible actualizar el conjunto de características o la versión de IOS para obtener capacidades adicionales.

En este curso, se concentrará principalmente en Cisco IOS, versión 15.x. En la figura 1, se muestra una lista de las versiones del software IOS para un switch Cisco Catalyst 2960. En la figura 2, se muestra una lista de las versiones del software IOS para un router de servicios integrados (ISR, Integrated Services Router) Cisco 2911.

El archivo IOS en sí tiene un tamaño de varios megabytes y se encuentra almacenado en un área de memoria semipermanente llamada flash. En la ilustración, se muestra una tarjeta Compact Flash. La memoria flash provee almacenamiento no volátil. Esto significa que los contenidos de la memoria no se pierden cuando el dispositivo se apaga. Si bien el contenido de la memoria flash no se pierde durante un corte de la alimentación, puede modificarse o sobrescribirse si es necesario. Esto permite actualizar el IOS a una versión más reciente o agregarle nuevas características sin reemplazar el hardware. Además, se puede utilizar la memoria flash para almacenar varias versiones del software IOS al mismo tiempo.

En muchos dispositivos Cisco, el IOS de la memoria flash se copia a la memoria de acceso aleatorio (RAM, random access memory) cuando se enciende el dispositivo. Luego, cuando el dispositivo está en funcionamiento, el IOS se ejecuta desde la RAM. La RAM tiene muchas funciones, incluido el almacenamiento de los datos que utiliza el dispositivo para admitir las operaciones de la red. La ejecución del IOS en la RAM aumenta el rendimiento del dispositivo. Sin embargo, la RAM se considera memoria volátil dado que los datos se pierden durante un reinicio. Un reinicio consiste en apagar y volver a encender un dispositivo, ya sea a propósito o por accidente.

La cantidad de memoria flash y RAM requerida para un IOS determinado varía notablemente. A los efectos del mantenimiento y la planificación de redes, es importante determinar los requisitos de memoria flash y RAM para cada dispositivo, incluidas las configuraciones máximas de estos tipos de memoria. Es posible que los requisitos de las versiones más recientes de IOS exijan más memoria RAM y flash de la que puede instalarse en algunos dispositivos.

Los routers y switches en los que se utiliza Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma esperada. Las funciones principales que realizan o habilitan los routers y switches Cisco incluyen las siguientes:

* Prestación de seguridad de la red
* Direccionamiento IP de interfaces virtuales y físicas
* Habilitación de configuraciones específicas de la interfaz para optimizar la conectividad de los respectivos medios
* Enrutamiento
* Habilitación de tecnologías de calidad de servicio (QoS)
* Compatibilidad con tecnologías de administración de red

Cada característica o servicio tiene asociado un conjunto de comandos de configuración que permite su implementación por parte de los técnicos de red.

Por lo general, se accede a los servicios que proporciona Cisco IOS mediante una CLI.

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

* Consola
* Telnet o SSH
* Puerto auxiliar

**Consola**

El puerto de consola es un puerto de administración que proporciona acceso fuera de banda a los dispositivos Cisco. El acceso fuera de banda se refiere al acceso mediante un canal de administración dedicado que se utiliza únicamente para el mantenimiento del dispositivo. La ventaja de utilizar un puerto de consola es que es posible acceder al dispositivo incluso si no se configuró ningún servicio de red, por ejemplo, cuando se realiza la configuración inicial del dispositivo de red. Al realizar la configuración inicial, una PC con software de emulación de terminal se conecta al puerto de consola del dispositivo mediante un cable especial. Los comandos de configuración para el switch o el router se pueden introducir en la PC conectada.

El puerto de consola también puede utilizarse cuando fallan los servicios de red y no es posible acceder al dispositivo Cisco IOS de manera remota. Si esto ocurre, una conexión a la consola puede habilitar a una PC para determinar el estado del dispositivo. En forma predeterminada, la consola comunica el inicio del dispositivo, la depuración y los mensajes de error. Una vez que el técnico de red se conecta al dispositivo, puede ejecutar cualquier comando de configuración necesario mediante la sesión de consola.

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. También se debe colocar el dispositivo en una habitación bajo llave o en un bastidor de equipos para evitar el acceso físico no autorizado.

**Telnet**

Telnet es un método para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de redes activos en el dispositivo. El dispositivo de red debe tener, por lo menos, una interfaz activa configurada con una dirección de Internet, por ejemplo una dirección IPv4. Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que permite a los usuarios introducir comandos de configuración desde un cliente Telnet. Además de admitir el proceso de servidor Telnet, el dispositivo Cisco IOS también contiene un cliente Telnet. Esto permite que los administradores de red accedan mediante Telnet a cualquier otro dispositivo que admita un proceso de servidor Telnet desde la CLI del dispositivo Cisco.

**SSH**

El protocolo de Shell seguro (SSH) proporciona un inicio de sesión remoto similar al de Telnet, excepto 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. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.

La mayoría de las versiones de Cisco IOS incluyen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren que el servidor SSH se habilite en forma manual. Los dispositivos IOS también incluyen un cliente SSH que puede utilizarse para establecer sesiones SSH con otros dispositivos.

**AUX**

Una antigua forma de establecer una sesión de CLI de manera remota era mediante una conexión telefónica de dial-up con un módem conectado al puerto auxiliar (AUX) de un router, el cual aparece resaltado en la ilustración. Al igual que la conexión de consola, el método de puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red en el dispositivo. En caso de que los servicios de red fallen, es posible que un administrador remoto acceda al switch o al router mediante una línea telefónica.

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. No obstante, se prefiere el puerto de consola al puerto auxiliar para la resolución de problemas, ya que el primero muestra mensajes de inicio, depuración y error de manera predeterminada.

**Nota:** los switches Cisco Catalyst no admiten conexiones auxiliares.

Existen varios programas excelentes de emulación de terminales disponibles para conectarse a un dispositivo de red mediante una conexión serial por un puerto de consola o mediante una conexión Telnet o SSH. Algunos de estos programas incluyen los siguientes:

* PuTTY (figura 1)
* Tera Term (figura 2)
* SecureCRT (figura 3)
* HyperTerminal
* OS X Terminal

Estos programas le permiten aumentar la productividad mediante ajustes del tamaño de la ventana, modificaciones de los tamaños de fuente y cambios en los esquemas de colores.

Una vez que un técnico de red se conecta a un dispositivo, puede configurarlo. El técnico de red debe navegar a través de diversos modos del IOS. Los modos de Cisco IOS para los switches y los routers son muy similares. La CLI utiliza una estructura jerárquica para los modos.

En orden jerárquico desde el más básico hasta el más especializado, los modos principales son los siguientes:

* Modo de usuario (EXEC de usuario)
* Modo de ejecución privilegiado (EXEC privilegiado)
* Modo de configuración global
* Otros modos de configuración específicos, como el modo de configuración de interfaz

Cada modo tiene una petición de entrada distinta y se utiliza para realizar tareas determinadas con un conjunto específico de comandos que están disponibles solo para el modo en cuestión. Por ejemplo, el modo de configuración global permite que los técnicos configuren los parámetros del dispositivo que lo afectan en su conjunto, como la configuración del nombre de dispositivo. Sin embargo, se requiere un modo diferente si el técnico de red desea configurar los parámetros de seguridad en un puerto específico de un switch, por ejemplo. En ese caso, el técnico de red debe ingresar al modo de configuración de interfaz para ese puerto específico. Todas las configuraciones que se introducen en el modo de configuración de interfaz se aplican solo a ese puerto.

Se puede configurar la estructura jerárquica para 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.

En la ilustración, se muestra la estructura de los modos de IOS con sus peticiones de entrada y características típicas.

Los dos modos de funcionamiento principales son el modo EXEC del usuario y el modo EXEC privilegiado. Como característica de seguridad, el software Cisco IOS divide las sesiones de EXEC en dos niveles de acceso. Como se muestra en la ilustración, el modo EXEC privilegiado tiene un mayor nivel de autoridad con respecto a lo que permite que realicen los usuarios en el dispositivo.

**Modo EXEC del usuario**

El modo EXEC del usuario tiene capacidades limitadas, pero es útil para algunas operaciones básicas. El modo EXEC del usuario se encuentra en el nivel más básico de la estructura jerárquica modal. Este es el primer modo que se encuentra al entrar a la CLI de un dispositivo 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. Sin embargo, 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 los comandos de configuración y administración requiere que el administrador de red utilice el modo EXEC privilegiado o un modo más específico en la jerarquía. Esto significa que los usuarios deben ingresar primero al modo EXEC del usuario y, desde allí, acceder al modo EXEC privilegiado.

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

Switch#

De manera predeterminada, el modo 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. En una sección posterior de este capítulo, analizaremos la configuración de dispositivos y algunos de los modos de configuración.

Solo se puede ingresar al modo de configuración global y a los modos de configuración de interfaz por medio del modo EXEC privilegiado.

**Modo de configuración global**

El modo de configuración principal recibe el nombre de configuración global o global config. En el modo de configuración global, se realizan cambios en la configuración de la CLI que afectan el funcionamiento del dispositivo en su totalidad. Antes de acceder a los modos de configuración específicos, se accede al modo de configuración global.

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:

Switch# **configure terminal**

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

Switch(config)#

**Modos de configuración específicos**

En el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. 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).
* **Modo de línea**: para configurar una de las líneas físicas o virtuales (consola, auxiliar, VTY).

En la figura 1, se muestran las peticiones de entrada de algunos de estos modos. Para salir de un modo de configuración específico y volver al modo de configuración global, escriba **exit** (salir) en 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**.

**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. 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 del modo de configuración global en un switch sería la siguiente:

Switch(config)#

A medida que se utilizan los comandos y se cambian los modos, la petición de entrada cambia para reflejar el contexto actual, como se muestra en la figura 2.

**Cómo alternar entre los modos EXEC del usuario y 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:

Switch> **enable**

Este comando se ejecuta sin la necesidad de un argumento o una palabra clave. Una vez que se presiona la tecla Entrar, la petición de entrada pasa a ser la siguiente:

Switch#

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

Si se configuró la autenticación de contraseña para el modo EXEC privilegiado, el IOS solicita la contraseña.

Por ejemplo:

Switch> **enable**

Password:

Switch#

El comando **disable** se usa para volver del modo EXEC privilegiado al modo EXEC del usuario.

Por ejemplo:

Switch# **disable**

Switch>

Como se muestra en la ilustración, los comandos para acceder al modo EXEC privilegiado y para regresar al modo EXEC del usuario en un router Cisco son idénticos a los que se utilizan en un switch Cisco.

**Cómo alternar entre el modo y los submodos de configuración global**

Para salir del modo de configuración global y volver al modo EXEC privilegiado, introduzca el comando **exit**.

Tenga en cuenta que, al introducir el comando **exit** en el modo EXEC privilegiado, la sesión de consola finaliza. Es decir que, al introducir**exit** en el modo EXEC privilegiado, aparece la pantalla que se ve cuando se inicia una sesión de consola. En esta pantalla, se debe presionar la tecla Entrar para ingresar al modo EXEC del usuario.

Para pasar de cualquier submodo del modo de configuración global al modo que se encuentra un nivel más arriba en la jerarquía de modos, introduzca el comando **exit**. En la figura 1, se muestra cómo pasar del modo EXEC del usuario al modo EXEC privilegiado, cómo ingresar luego al modo de configuración global y al modo de configuración de interfaz, cómo volver al modo de configuración global y cómo regresar al modo EXEC privilegiado utilizando el comando **exit**.

Para pasar de cualquier submodo del modo EXEC privilegiado al modo EXEC privilegiado, introduzca el comando **end** o presione la combinación de teclas **Ctrl+Z**. En la figura 2, se muestra cómo pasar del modo de configuración de VLAN al modo EXEC privilegiado utilizando el comando**end**.

Para pasar de cualquier submodo del modo de configuración global a otro submodo “inmediato” de dicho modo, solo debe introducir el comando correspondiente que normalmente se introduce en el modo de configuración global. En la ilustración 3, se muestra cómo pasar del modo de configuración de línea, Switch(config-line)#, al modo de configuración de interfaz, Switch(config-if)#, sin tener que salir del modo de configuración de línea.

**Estructura básica de comandos de IOS**

Los dispositivos Cisco IOS admiten muchos comandos. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. 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. Los comandos se utilizan para ejecutar una acción y las palabras clave se utilizan para identificar dónde o cómo ejecutar el comando.

Como se muestra en la figura 1, el comando es la palabra o las palabras iniciales que se introducen en la línea de comandos a continuación de la petición de entrada. Los comandos no distinguen mayúsculas de minúsculas. A continuación del comando siguen una o más palabras clave y argumentos. Una vez que introduzca cada comando completo, incluidos cualquier palabra clave y argumento, presione la tecla Entrar para enviar el comando al intérprete de comandos.

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 deben utilizarse para definir el resultado específico que se debe mostrar. 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.

**Convenciones de los comandos de IOS**

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. Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulte la sintaxis de comandos. La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.

Por ejemplo, la sintaxis para utilizar el comando **description** es la siguiente:

Switch(config-if)# **description** *cadena*

Como se muestra en la figura 2, el texto en negrita indica los comandos y las palabras clave que se escriben como se muestran, y el texto en cursiva indica un argumento para el que el usuario proporciona el valor. Para el comando **description**, el argumento es un valor de cadena. El valor de cadena puede ser cualquier cadena de texto de hasta 80 caracteres.

En consecuencia, al aplicar una descripción a una interfaz con el comando **description**, se debe introducir una línea como la siguiente:

Switch(config-if)# **description** **Switch de oficina central**

El comando es **description**, y el argumento definido por el usuario es**Switch de oficina central**.

Los siguientes ejemplos muestran algunas convenciones utilizadas para registrar y usar comandos de IOS.

Para el comando **ping**:

Sintaxis:

Switch> **ping** *dirección IP*

Ejemplo con valores:

Switch> **ping** **10.10.10.5**

El comando es **ping**, y el argumento definido por el usuario es la dirección IP **10.10.10.5**.

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

Sintaxis:

Switch> **traceroute** *dirección IP*

Ejemplo con valores:

Switch> **traceroute** **192.168.254.254**

El comando es **traceroute**, y el argumento definido por el usuario es la dirección IP **192.168.254.254**.

Cisco IOS Command Reference (Referencia de comandos de Cisco IOS) es una colección de documentos en línea que describen en detalle los comandos de IOS utilizados en los dispositivos Cisco. La referencia de comandos es la mejor fuente de información sobre comandos de IOS específicos, de la misma manera en que un diccionario es la mejor fuente para obtener información sobre una palabra específica.

La referencia de comandos es un recurso fundamental que los ingenieros de redes utilizan para revisar diversas características de un comando de IOS determinado. Algunas de las características más frecuentes son las siguientes:

* **Sintaxis:** la versión más detallada de la sintaxis para un comando que se puede encontrar.
* **Predeterminado:** la manera en que el comando se implementa en un dispositivo con una configuración predeterminada.
* **Modo:** el modo de configuración del dispositivo en el que se introduce el comando.
* **Historial:** descripciones de cómo se implementa el comando en relación con la versión de IOS.
* **Pautas de uso:** pautas que describen específicamente cómo implementar el comando.
* **Ejemplos:** ejemplos útiles que muestran situaciones en las que se utiliza el comando con frecuencia.

Para navegar hasta la referencia de comandos y buscar un comando específico, siga los pasos que se indican a continuación:

**Paso 1.** Acceda a [www.cisco.com](http://www.cisco.com/).

**Paso 2.** Haga clic en **Support** (Soporte).

**Paso 3.** Haga clic en **Networking Software** (Software de redes) (IOS e NX-OS).

**Paso 4.** Haga clic en **15.2M&T**, (por ejemplo).

**Paso 5.** Haga clic en **Reference Guides** (Guías de referencia).

**Paso 6.** Haga clic en **Command References** (Referencias de comandos).

**Paso 7.** Haga clic en la tecnología específica que abarca el comando al que hace referencia.

**Paso 8.** Haga clic en el enlace de la izquierda que coincida alfabéticamente con el comando al que hace referencia.

**Paso 9.** Haga clic en el enlace del comando.

Por ejemplo, el comando **description** se encuentra en *Cisco IOS Interface and Hardware Component Command Reference* (Referencia de comandos de componentes de hardware y de interfaz de Cisco IOS), en el enlace para el rango alfabético *D through E* (D a E).

**Nota:** se pueden descargar versiones completas de las referencias de comandos para una tecnología determinada en formato PDF mediante los enlaces que se encuentran en la página a la que se llega después de completar el paso 7 mencionado anteriormente.

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, introduzca un signo de interrogación, **?**, en cualquier petición de entrada. Aparece una respuesta inmediata sin necesidad de utilizar la tecla Entrar.

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, introduzca un signo de interrogación, **?**, en la petición de entrada Switch>.

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. Si se introduce un signo de interrogación, sin espacio, inmediatamente después de introducir una secuencia de caracteres, el IOS muestra una lista de comandos o palabras clave para el contexto que comienzan con los caracteres introducidos.

Por ejemplo, introduzca **sh?** para obtener una lista de los comandos que comienzan 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. Al introducir un comando, introduzca un espacio seguido de un **?** para determinar qué puede o debe introducirse a continuación.

Como se muestra en la ilustración, después de introducir el comando**clock set 19:50:00**, se puede introducir el signo **?** para determinar las demás opciones o palabras clave disponibles para este comando.

**Verificación de la sintaxis del comando**

Cuando se emite un comando presionando la tecla Entrar, el intérprete de la línea de comandos analiza la sintaxis del comando de izquierda a derecha para determinar qué acción se solicitó. En general, el IOS solo proporciona comentarios negativos, como se muestra en la figura 1. 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.

En la figura 2, se muestran tres tipos distintos de mensajes de error:

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

El comando de IOS **clock set** es ideal para experimentar con los distintos mensajes de ayuda de la revisión de sintaxis de comandos, como se muestra en la figura 1. En la figura 2, se proporciona ayuda sobre los tres tipos de mensajes de error.

**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.

En la ilustración se muestran la mayoría de los métodos abreviados. Merece la pena tener en cuenta de manera especial los siguientes:

* **Flecha abajo:** permite al usuario desplazarse hacia delante a través de los comandos anteriores.
* **Flecha arriba:** permite al usuario desplazarse hacia atrás a través de los comandos anteriores.
* **Tabulación:** completa el resto de un comando o de una palabra clave que se escribió parcialmente.
* **Ctrl-A:** se traslada al comienzo de la línea.
* **Ctrl-E:** se traslada al final de la línea.
* **Ctrl-R**: vuelve a mostrar una línea
* **Ctrl-Z:** sale del modo de configuración y vuelve al modo EXEC del usuario.
* **Ctrl-C:** sale del modo de configuración o cancela el comando actual.
* **Ctrl-Mayús-6:** permite al usuario interrumpir un proceso de IOS, como ping o traceroute.

Análisis más detallado de algunos de ellos:

**Tabulación**

La tecla de tabulación se utiliza para completar el resto de los comandos y los parámetros abreviados, siempre que la abreviatura contenga 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.

Esta 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**

La función de volver a mostrar la línea actualiza la línea que se acaba de escribir. 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, utilice **Ctrl-R**:

Switch# **show mac**

**Ctrl-Z**

Esta combinación de teclas permite salir de cualquier modo de configuración y volver al modo EXEC privilegiado. Dado que el IOS tiene una estructura de modos jerárquica, el usuario puede encontrarse varios niveles hacia abajo. En lugar de salir de cada modo en forma individual, utilice **Ctrl-Z** para volver directamente a la petición de entrada de EXEC privilegiado en el nivel superior.

**Flechas arriba y abajo**

Las teclas de comandos anteriores recuerdan el historial de comandos introducidos. 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 volver a introducir comandos sin tener que volver a escribirlos.

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

**Ctrl-Mayús-6**

La secuencia de escape interrumpe cualquier proceso en ejecución. 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-Mayús-6**.

**Ctrl-C**

Interrumpe la entrada de un comando y sale del modo de configuración, lo que resulta útil después de introducir un comando que se necesita cancelar.

**Abreviación de comandos o palabras clave**

Los comandos y las palabras clave pueden abreviarse a la cantidad mínima de caracteres que identifiquen 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:

Switch# **show interfaces**

Switch# **show int**

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

Switch# **sh int**

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**. Utilice el comando **show ?** para obtener una lista de los comandos disponibles en un modo o contexto determinado.

Un comando **show** típico puede proporcionar información sobre la configuración, el funcionamiento y el estado de las partes de un switch o un router Cisco. En la ilustración, se destacan algunos de los comandos de IOS frecuentes.

En este curso, la atención se centra principalmente en los comandos**show** básicos.

Un comando **show** de uso frecuente es **show interfaces**. Este comando muestra estadísticas de todas las interfaces del dispositivo. Para ver las estadísticas de una interfaz específica, introduzca el comando **show interfaces** seguido del tipo de interfaz específico y el número de ranura o de puerto. Por ejemplo:

Switch# **show interfaces fastethernet 0/1**

Algunos otros comandos **show** que los técnicos de red utilizan con frecuencia incluyen los siguientes:

**show startup-config:**muestra la configuración guardada ubicada en la NVRAM.

**show running-config:**muestra el contenido del archivo de configuración en ejecución actual.

**La petición de entrada More**

Cuando un comando devuelve más resultados de los que pueden mostrarse en una sola pantalla, aparece la petición de entrada **--More--** en la parte inferior de la pantalla. Cuando aparezca la petición de entrada **--More--**, presione la **barra espaciadora** para ver el siguiente tramo 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.

Uno de los comandos de uso más frecuente en un switch o un router es el siguiente:

Switch# **show version**

Este comando muestra información sobre la versión de IOS cargada actualmente, además de información sobre el hardware y los dispositivos. Si inició sesión en un router o un switch de manera remota, el comando **show version** es un medio excelente para obtener rápidamente un resumen de información útil sobre el dispositivo específico al cual está conectado. Algunos de los datos que se obtienen a partir de este comando son los siguientes:

* **Versión del software:** versión del software IOS (almacenada en la memoria flash).
* **Versión de bootstrap:** versión de bootstrap (almacenada en la ROM de arranque).
* **Tiempo de actividad del sistema:** tiempo transcurrido desde la última vez que se reinició.
* **Información de reinicio del sistema**: método de reinicio (por ejemplo, apagado y encendido, colapso).
* **Nombre de la imagen del software:** nombre del archivo de IOS almacenado en la memoria flash.
* **Tipo de router y tipo de procesador:** número de modelo y tipo de procesador.
* **Tipo y asignación de memoria (compartida/principal):** memoria RAM del procesador principal y almacenamiento en búfer de E/S de paquetes compartidos.
* **Características del software:** protocolos y conjuntos de características admitidos.
* **Interfaces de hardware:** interfaces disponibles en el dispositivo.
* **Registro de configuración:** establece especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados.

En la figura 1, se muestra el resultado para un ISR Cisco 1941, mientras que en la figura 2 se muestra el resultado para un switch Cisco Catalyst 2960.

Según lo analizado, los switches y los routers Cisco tienen muchas similitudes: admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial durante su implementación en una red son idénticos para ambos dispositivos.

Sin embargo, un switch Cisco IOS es uno de los dispositivos más simples que se pueden configurar en una red. Esto se debe a que no se requiere ninguna configuración antes de poner en funcionamiento el dispositivo. En su versión más básica, se puede conectar un switch sin ninguna configuración, y de todas maneras conmutará los datos entre los dispositivos conectados.

Un switch también es uno de los dispositivos fundamentales que se utilizan para crear una red pequeña. Al conectar dos PC a un switch, esas PC tienen conectividad mutua en forma inmediata.

Por lo tanto, el resto de este capítulo se centra en la creación de una pequeña red de dos PC conectada mediante un switch configurado con los parámetros iniciales. Los parámetros iniciales incluyen la configuración de un nombre para el switch, la limitación del acceso a la configuración del dispositivo, la configuración de mensajes de aviso y guardar la configuración.

Al configurar un dispositivo de red, uno de los primeros pasos es la configuración de un nombre de dispositivo único o “nombre de host”. Los nombres de host aparecen en las peticiones de entrada de la CLI, pueden utilizarse en varios procesos de autenticación entre dispositivos y deben utilizarse en los diagramas de topologías.

Los nombres de host se configuran en el dispositivo de red activo. Si el nombre del dispositivo no se configura explícitamente, Cisco IOS utiliza un nombre de dispositivo predeterminado de fábrica. El nombre predeterminado de los switches Cisco IOS es “Switch”.

Imagine si una internetwork tuviera varios switches con el nombre predeterminado “Switch” (como se muestra en la ilustración). Esto generaría una gran confusión durante la configuración y el mantenimiento de la red. Al acceder a un dispositivo remoto mediante SSH, es importante tener la confirmación de que se está conectado al dispositivo correcto. Si se dejara el nombre predeterminado en todos los dispositivos, sería difícil determinar que el dispositivo correcto está conectado.

Al elegir nombres adecuados, resulta más fácil recordar, analizar, registrar 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. A fin de permitir la continuidad dentro de una organización, siempre conviene crear la convención de nomenclatura al mismo tiempo que el esquema de direccionamiento.

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

* Comenzar con una letra.
* No contener espacios.
* Finalizar con una letra o dígito.
* Utilizar solamente letras, dígitos y guiones.
* Tener menos de 64 caracteres de longitud.

Los nombres de host utilizados en el IOS del dispositivo conservan el uso de caracteres en mayúscula y minúscula. 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.

Los nombres de host permiten que los administradores de red identifiquen dispositivos a través de una red o de Internet.

**Ejemplo de aplicación de nombres**

Utilicemos un ejemplo de tres switches conectados en una red que abarca tres pisos diferentes.

A fin de crear una convención de nomenclatura para los switches, se debe tener en cuenta la ubicación y el propósito de los dispositivos.

Por ejemplo, en la ilustración se denominó a los tres switches como Sw-piso-1, Sw-piso-2 y Sw-piso-3.

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 identifica la convención de nomenclatura, el paso siguiente es aplicar los nombres a los dispositivos usando la CLI.

**Configuración del nombre de host de IOS**

En el modo EXEC privilegiado, acceda al modo de configuración global introduciendo el comando **configure terminal**:

Switch# **configure terminal**

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

Switch(config)#

Introduzca el nombre de host en el modo de configuración global, como se muestra en la ilustración:

Switch(config)# **hostname Sw-piso-1**

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

Sw-piso-1 (config)#

Observe que el nombre de host aparece en la petición de entrada. Para salir del modo de configuración global, utilice 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 deshacer los efectos de un comando, escriba la palabra clave**no** antes del comando.

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

Sw-piso-1 (config)# **no hostname**

Switch(config)#

Observe que el comando **no hostname** provocó que el switch volviera a usar el nombre de host predeterminado “Switch”.

En la ilustración, practique la introducción de un nombre de host en un switch.

La limitación física del acceso a los dispositivos de red mediante su colocación en armarios y bastidores bajo llave es aconsejable; sin embargo, las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red. Todos los dispositivos, incluso los routers domésticos, deben tener contraseñas configuradas en forma local para limitar el acceso. Más adelante, se presentará la forma de reforzar la seguridad mediante la solicitud de un nombre de usuario junto con una contraseña. Por ahora, presentaremos precauciones de seguridad básicas mediante el uso de contraseñas únicamente.

Como se comentó anteriormente, el IOS usa modos jerárquicos para colaborar con la seguridad del dispositivo. Como parte de este cumplimiento de seguridad, el IOS puede aceptar diversas contraseñas para permitir diferentes privilegios de acceso al dispositivo.

Las contraseñas ingresadas aquí son:

* **Contraseña de enable:** limita el acceso al modo EXEC privilegiado.
* **Contraseña secreta de enable:** es una contraseña encriptada que limita el acceso al modo EXEC privilegiado.
* **Contraseña de consola:** limita el acceso a los dispositivos mediante la conexión de consola.
* **Contraseña de VTY:** limita el acceso a los dispositivos a través de Telnet.

Siempre conviene utilizar contraseñas de autenticación diferentes para cada uno de estos niveles de acceso. Si bien no es práctico iniciar sesión con varias contraseñas diferentes, es una precaución necesaria para proteger adecuadamente la infraestructura de la red ante accesos no autorizados.

Además, utilice contraseñas seguras que no se descubran fácilmente El uso de contraseñas simples o fáciles de adivinar continúa siendo un problema de seguridad en muchas facetas del mundo empresarial.

Considere estos puntos clave cuando elija contraseñas:

* Use contraseñas que tengan más de 8 caracteres.
* Utilice una combinación de letras mayúsculas y minúsculas, números, caracteres especiales o secuencias numéricas en las contraseñas.
* Evite el uso de la misma contraseña para todos los dispositivos.
* Evite el uso de palabras comunes como contraseña o administrador, porque se descubren fácilmente.

**Nota:** en la mayoría de las prácticas de laboratorio de este curso, se utilizan contraseñas simples como **cisco** o **class**. Estas contraseñas se consideran no seguras y fáciles de adivinar, y deben evitarse en un entorno laboral. Estas contraseñas solo se utilizan por comodidad en el aula o para ilustrar ejemplos de configuración.

Para proteger el acceso a EXEC privilegiado, utilice el comando **enable secret***contraseña*. Una variación más antigua y menos segura de este comando es el comando **enable password***contraseña*. Si bien puede utilizarse cualquiera de estos comandos para establecer la autenticación antes de permitir el acceso al modo EXEC privilegiado (enable), se recomienda utilizar el comando **enable secret**. El comando **enable secret** proporciona mayor seguridad, dado que la contraseña está encriptada.

Comando de ejemplo para establecer contraseñas:

Switch(config)# **enable secret class**

El ejemplo de la ilustración muestra que no se solicita una contraseña cuando se utiliza el comando **enable** por primera vez. A continuación, se configura el comando **enable secret class**, y el acceso a EXEC privilegiado ahora queda protegido. Observe que, por motivos de seguridad, la contraseña no se muestra cuando se introduce.

El puerto de consola de dispositivos de red debe estar asegurado, como mínimo, mediante el pedido de una contraseña segura al usuario. Así se reducen las posibilidades de que personal no autorizado conecte físicamente un cable al dispositivo y obtenga acceso a éste.

Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

Switch(config)# **line console 0**

Switch(config-line)# **password cisco**

Switch(config-line)# **login**

En el modo de configuración global, se usa el comando **line console 0** para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

El segundo comando, **password cisco**, especifica una contraseña para la línea de consola.

El comando **login** configura el switch para que requiera autenticación al iniciar sesión. Cuando se habilita el inicio de sesión y se establece una contraseña, se solicita al usuario de la consola que introduzca una contraseña antes de darle acceso a la CLI.

**Contraseña de VTY**

Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un router Cisco varía según el tipo de router y la versión de IOS. No obstante, la cantidad más frecuente de líneas vty configuradas es cinco. Estas líneas se numeran del 0 al 4 de manera predeterminada, aunque se pueden configurar líneas adicionales. Es necesario establecer 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.

Comandos de ejemplo utilizados para establecer una contraseña en las líneas vty:

Switch(config)# **line vty 0 15**

Switch(config-line)# **password cisco**

Switch(config-line)# **login**

De manera predeterminada, el IOS incluye el comando **login** en las líneas VTY. Esto impide el acceso al dispositivo mediante Telnet sin autenticación. Si por error se establece el comando **no login**, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de la red utilizando Telnet. Esto representaría un riesgo importante para la seguridad.

En la ilustración, se muestra la protección del acceso a EXEC del usuario en las líneas de consola y las líneas Telnet.

Existe otro comando de utilidad que impide que las contraseñas aparezcan como texto no cifrado cuando se visualizan los archivos de configuración: se trata del comando **service password-encryption**.

Este comando provee la encriptación de la contraseña cuando ésta se configura. El comando **service password-encryption** aplica una encriptación mínima a todas las contraseñas sin encriptar. Esta encriptación solo se aplica a las contraseñas del archivo de configuración; no a las contraseñas mientras se envían a través de los medios. 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 sin encriptar resultan 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.

En la ilustración, practique la introducción del comando para configurar la encriptación de contraseñas.

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 utiliza un aviso, este nunca debe invitar a un usuario al dispositivo. 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 de configuración global.

El comando **banner motd** requiere el uso de delimitadores para identificar el contenido del mensaje de 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 "#".

La sintaxis para configurar un MOTD en el modo de configuración global es la siguiente:

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.

El ejemplo de la ilustración muestra un anuncio configurado con el símbolo delimitador “#”. Observe cómo aparece ahora el anuncio cuando se accede al switch.

El archivo de configuración en ejecución refleja la configuración actual aplicada a un dispositivo Cisco IOS. Contiene los comandos utilizados para determinar cómo funciona el dispositivo en la red, tal como se muestra en la figura 1. La modificación de la configuración en ejecución afecta el funcionamiento de un dispositivo Cisco de inmediato.

El archivo de configuración en ejecución se almacena en la memoria de trabajo del dispositivo o memoria de acceso aleatorio (RAM). Esto significa que el archivo de configuración en ejecución está temporalmente activo mientras el dispositivo Cisco está en funcionamiento (encendido). Sin embargo, si se corta la alimentación al dispositivo o se lo reinicia, se pierden todos los cambios de configuración, a menos que se hayan guardado.

Después de realizar cambios a un archivo de configuración en ejecución, tenga en cuenta estas distintas opciones:

* Volver a la configuración original del dispositivo.
* Eliminar todas las configuraciones del dispositivo.
* Convertir la configuración cambiada en la nueva configuración de inicio.

El archivo de configuración de inicio refleja la configuración que utilizará el dispositivo cuando se lo reinicie. El archivo de configuración de inicio se almacena en NVRAM. Cuando se configura un dispositivo de red y se modifica la configuración en ejecución, es importante guardar esos cambios en el archivo de configuración de inicio. Esto evita que los cambios se pierdan debido a cortes de energía o a un reinicio intencional.

Antes de asignar los cambios, use los correspondientes comandos **show**para verificar la operación del dispositivo. Como se muestra en la ilustración, 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 comando para guardar la configuración en ejecución en el archivo de configuración de inicio es:

Switch# **copy running-config startup-config**

Una vez que se ejecuta, el archivo de configuración en ejecución actualiza el archivo de configuración de inicio.

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 Entrar. Si se presiona cualquier otra tecla, se cancelará el proceso.

Por ejemplo:

Switch# **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)

Soporte técnico: http://www.cisco.com/techsupport

Derechos de autor © 2004 por 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

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 mediante el 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:

Switch# **erase startup-config**

Una vez que se emite el comando, el switch le solicita 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 Entrar. Si se presiona cualquier otra tecla, se cancelará el proceso.

**Precaución:** tenga cuidado al utilizar el comando **erase**. Este comando puede utilizarse para borrar cualquier archivo del dispositivo. El uso incorrecto del comando puede borrar el IOS mismo u otro archivo esencial.

En un switch, también se debe emitir el comando **delete vlan.dat**además del comando **erase startup-config**, a fin de devolver el dispositivo a la configuración predeterminada inicial (similar a un restablecimiento de la configuración predeterminada de fábrica):

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# **erase startup-config**

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

[OK]

Erase of nvram: complete

Switch#

Después de eliminar la configuración de inicio de la NVRAM (y de borrar el archivo vlan.dat en el caso de un switch), vuelva a cargar el dispositivo para eliminar el archivo de configuración actual en ejecución de la RAM. El dispositivo cargará entonces la configuración de inicio predeterminada que se envió originalmente con el dispositivo en la configuración en ejecución.

En la figura 2, practique la introducción de comandos para guardar la configuración en ejecución de la RAM en la NVRAM.

**Copia de seguridad de las configuraciones mediante captura de texto**

Además de guardar las configuraciones en ejecución en la configuración de inicio, los archivos de configuración también se pueden guardar y archivar en documentos 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.

En la figura 1, los archivos de configuración se pueden guardar y archivar en un documento de texto utilizando Tera Term.

Los pasos son los siguientes:

* En el menú File, haga clic en **Log**.
* Elija la ubicación. Tera Term comenzará a capturar texto.
* Una vez que comienza la captura, ejecute el comando **show running-config** o **show startup-config** en la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
* Cuando la captura haya finalizado, seleccione **Close** (Cerrar) en la ventana Log (Registro) de TeraTerm.
* Observe el resultado para verificar que no esté dañado.

De manera similar, en la figura 2, se muestra cómo se pueden guardar y archivar los archivos en un documento de texto utilizando HyperTerminal.

**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. Es posible que deba editar el archivo antes de copiarlo. Se recomienda cambiar las contraseñas encriptadas a texto no cifrado y eliminar el parámetro, ya sea el número 5 o 7, que especifica que la contraseña está encriptada. Los mensajes de IOS y el texto que no represente comandos, como “--More--”, se deben eliminar. 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 Tera Term, los pasos son los siguientes:

* Edite el texto para eliminar lo que no represente comandos y guarde los cambios.
* En el menú **File** haga clic en **Send** para enviar el archivo.
* Ubique el archivo que debe copiar en el dispositivo y haga clic en**Open**.
* Tera Term 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. Este método es conveniente para configurar dispositivos en forma manual.

El uso de direcciones IP, ya sean IPv4 o IPv6, es el principal medio para permitir que los dispositivos se ubiquen entre sí y para establecer la comunicación de extremo a extremo en Internet. De hecho, en cualquier internetwork, las direcciones IP son fundamentales para que los dispositivos se comuniquen de origen a destino y viceversa.

Cada dispositivo final en una red se debe configurar con direcciones IP. Algunos ejemplos de dispositivos finales son:

* Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
* Impresoras de red
* Teléfonos VoIP
* Cámaras de seguridad
* Smartphones
* Dispositivos portátiles móviles (como los escáneres inalámbricos para códigos de barras)

La estructura de una dirección IPv4 se denomina “notación decimal punteada” y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red. Son de naturaleza lógica, ya que proporcionan información sobre la ubicación del dispositivo.

Con la dirección IP, también se necesita una máscara de subred. Las máscaras de subred son un tipo especial de direcciones IPv4 que, combinadas con las direcciones IP, determinan de qué subred específica de una red más grande forma parte el dispositivo.

Las direcciones IP se pueden asignar tanto a los puertos físicos como a las interfaces virtuales de los dispositivos. Una interfaz virtual significa que no hay hardware físico en el dispositivo asociado a ella.

Las comunicaciones de red dependen de las interfaces de los dispositivos para usuarios finales, las interfaces de los dispositivos de red y los cables que las conectan.

Cada interfaz física tiene especificaciones o estándares que la definen. Los cables que se conectan a la interfaz deben estar diseñados para cumplir con los estándares físicos de la interfaz. Los tipos de medios de red incluyen los cables de cobre de par trenzado, los cables de fibra óptica, los cables coaxiales y la tecnología inalámbrica. Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Algunas de las diferencias entre los distintos tipos de medios incluyen las siguientes:

* La distancia a través de la cual los medios pueden transportar una señal correctamente.
* El entorno en el que se instalarán los medios.
* La cantidad de datos y la velocidad a la que se deben transmitir.
* El costo de los medios y de la instalación.

Cada enlace de Internet no solo requiere un tipo específico de medio de red, sino que también requiere una determinada tecnología de red. Ethernet es la tecnología de red de área local (LAN) de uso más frecuente en la actualidad. Hay puertos Ethernet en los dispositivos para usuarios finales, en los dispositivos de switch y en otros dispositivos de red que se pueden conectar físicamente a la red mediante un cable. Para que un cable conecte dispositivos mediante un puerto Ethernet, este debe tener el conector correcto: un conector RJ-45.

Los switches Cisco IOS tienen puertos físicos a los que se pueden conectar los dispositivos, pero también cuentan con una o más interfaces virtuales de switch (SVI, switch virtual interfaces). Son interfaces virtuales porque no hay hardware físico en el dispositivo asociado a ellas; las SVI se crean en el software. La interfaz virtual proporciona un medio para administrar un switch de manera remota a través de una red usando IPv4. Cada switch viene con una SVI que aparece en la configuración predeterminada inicial. La SVI predeterminada es interface VLAN1.

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI:

* **Dirección IP:** junto con la máscara de subred, identifica el dispositivo final en la internetwork de manera exclusiva.
* **Máscara de subred:** determina qué parte de una red más grande utiliza una dirección IP.

Por el momento, se mantendrá el enfoque en IPv4; más adelante, se explorará IPv6.

Pronto aprenderá el sentido detrás de todas estas direcciones IP; por el momento, el objetivo es configurar rápidamente el switch para admitir el acceso remoto. En la ilustración, se muestra el comando para habilitar la conectividad IP del S1 mediante la dirección IP 192.168.10.2:

* **interface vlan 1:** se utiliza para navegar hasta el modo de configuración de interfaz desde el modo de configuración global.
* **ip address 192.168.10.2 255.255.255.0:** configura la dirección IP y la máscara de subred del switch (esta es solo una de muchas combinaciones posibles de una dirección IP y una máscara de subred).
* **no shutdown:** habilita administrativamente el estado activo de la interfaz.

Una vez que se configuran estos comandos, el switch tiene todos los elementos IP listos para la comunicación a través de la red.

**Nota:** todavía se deben configurar uno o más puertos físicos en el switch, así como las líneas VTY, para completar la configuración que permite la administración remota del switch.

Practique la configuración de una interfaz virtual de switch introduciendo comandos en la ilustración.

Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta. De modo similar al de una SVI, el dispositivo final se debe configurar con una dirección IP y una máscara de subred. Esta información se configura en los parámetros de la PC.

Para que un dispositivo final se conecte correctamente a la red, se deben configurar todos estos parámetros. Esta información se configura en los parámetros de red de la PC. Además de la información de dirección IP y máscara de subred, es posible configurar la información del gateway predeterminado y del servidor DNS, como se muestra en la ilustración.

La dirección de gateway predeterminado es la dirección IP de la interfaz del router que se utiliza para que el tráfico de la red salga de la red local. El gateway predeterminado es una dirección IP que, por lo general, asigna el administrador de red y se utiliza cuando se debe enrutar tráfico a otra red.

La dirección del servidor DNS es la dirección IP del servidor del Sistema de nombres de dominios (DNS, Domain Name System), que se utiliza para traducir direcciones IP a direcciones Web, como [www.cisco.com](http://www.cisco.com/). A todos los dispositivos de Internet se les asigna una dirección IP, mediante la cual se accede a ellos. Sin embargo, resulta más fácil recordar nombres que números. Por lo tanto, los sitios Web tienen nombres para simplificar el proceso. El servidor DNS se utiliza para mantener la asignación entre las direcciones IP y los nombres de los diversos dispositivos.

La información de dirección IP se puede introducir en la PC en forma manual o mediante el Protocolo de configuración dinámica de host (DHCP). El protocolo DHCP permite configurar la información de IP de los dispositivos finales de manera automática.

DHCP es una tecnología que se utiliza en casi todas las redes comerciales. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo.

DHCP permite la configuración automática de direcciones IPv4 para cada dispositivo final de una red con DHCP habilitado. Imagine la cantidad de tiempo que le llevaría si cada vez que se conectara a la red tuviera que introducir manualmente la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS. Multiplique eso por cada usuario y cada uno de los dispositivos en la red, y se dará cuenta del problema.

DHCP es un ejemplo de la tecnología en su máxima expresión. Uno de los propósitos principales de cualquier tecnología es facilitar las tareas que se desean o se deben realizar. Con DHCP, el usuario final ingresa al área que abarca una red determinada, conecta un cable Ethernet o habilita una conexión inalámbrica e, inmediatamente, se le asigna la información de IPv4 necesaria para comunicarse de manera correcta a través de la red.

Como se muestra en la figura 1, para configurar el protocolo DHCP en un equipo Windows, solo debe seleccionar “Obtener una dirección IP automáticamente” y “Obtener la dirección del servidor DNS automáticamente”. Se asigna información de un grupo de direcciones IP a la PC y se configura la información de IP relacionada en el servidor de DHCP.

Es posible mostrar las opciones de configuración IP en un equipo Windows usando el comando **ipconfig** en el símbolo del sistema. El resultado muestra la dirección IP, la máscara de subred y el gateway que la PC recibió del servidor de DHCP.

Practique cómo mostrar la dirección IP de un equipo Windows introduciendo comandos en la figura 2.

Si se define una dirección IP estática (manual) para un dispositivo de red; por ejemplo, una impresora, y luego se instala un servidor de DHCP, pueden ocurrir conflictos de direcciones IP duplicadas entre el dispositivo de red y una PC que obtiene información de direccionamiento IP automático del servidor de DHCP. También puede ocurrir un conflicto si se define manualmente una dirección IP estática para un dispositivo de red durante una falla de red relacionada con el servidor de DHCP; una vez que se resuelve la falla de red y se puede acceder al servidor de DHCP a través de la red, surge el conflicto.

Para resolver tales conflictos de direccionamiento IP, convierta el dispositivo de red con la dirección IP estática en cliente DHCP o excluya la dirección IP estática para el dispositivo final del ámbito de DHCP en el servidor de DHCP.

La segunda solución requiere privilegios de nivel administrativo en el servidor de DHCP y que esté familiarizado con la configuración de DHCP en un servidor.

También puede encontrar conflictos de direccionamiento IP al realizar manualmente la configuración de IP en un dispositivo final de una red que solo utiliza direcciones IP estáticas. En este caso, debe determinar qué direcciones IP están disponibles en la subred IP específica y realizar la configuración según corresponda. Este caso muestra por qué es tan importante que un administrador de red mantenga un registro detallado de los dispositivos finales que incluya las asignaciones de direcciones IP.

**Nota:** por lo general, en redes de pequeñas o medianas empresas, se utilizan direcciones IP estáticas en los servidores e impresoras, mientras que los dispositivos de los empleados utilizan información de dirección IP asignada mediante DHCP.

**Prueba de loopback**

En la ilustración, se muestra el primer paso de la secuencia de prueba. El comando **ping** se utiliza para verificar la configuración IP interna en un host local. Esta prueba se realiza utilizando el comando **ping** en una dirección reservada denominada “dirección de loopback” (127.0.0.1). El protocolo TCP/IP define la dirección de loopback, 127.0.0.1, como una dirección reservada que permite enrutar los paquetes de regreso al host.

Los comandos ping se introducen en una línea de comandos en el host local con la siguiente sintaxis:

C:\> **ping 127.0.0.1**

La respuesta de este comando se parecería a ésta:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 127.0.0.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Tiempo aproximado de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

El resultado indica que se enviaron cuatro paquetes de prueba de 32 bytes cada uno desde el host 127.0.0.1 y se devolvieron a este en un tiempo de menos de 1 ms. Esta solicitud de ping correcta verifica que la tarjeta de interfaz de red, los controladores y la implementación del protocolo TCP/IP funcionan correctamente.

Practique la prueba de una dirección de loopback introduciendo comandos en la figura 2.

Así como se utilizan comandos y utilidades para verificar una configuración de host, también se utilizan 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 switch**

Al examinar el S1 y el S2, se utiliza el comando **show ip interface brief** para verificar la condición de las interfaces del switch, como se muestra en la ilustración. La dirección IP asignada a la interfaz VLAN 1 en el S1 es 192.168.10.2. La dirección IP asignada a la interfaz VLAN 1 en el S2 es 192.168.10.3. Las interfaces físicas F0/1 y F0/2 en el S1 funcionan, al igual que las interfaces físicas F0/1 y F0/2 en el S2.

Practique la verificación de una interfaz VLAN introduciendo comandos en la ilustración.

**Prueba de la conectividad de PC a switch**

El comando **ping** se puede utilizar en una PC de la misma forma que en un dispositivo Cisco IOS. En la ilustración, se muestra que el ping de la PC1 a la dirección IP de la interfaz VLAN 1 del S1, 192.168.10.2, debe ser correcto.

**Prueba de la conectividad de extremo a extremo**

La dirección IP de la PC1 es 192.168.10.10, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.

La dirección IP de la PC2 es 192.168.10.11, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.

El ping de la PC1 a la PC2 también debe ser correcto. Si un ping de la PC1 a la PC2 se realiza correctamente, se verifica la conectividad de extremo a extremo en la red.