Capítulo 2: Configuración de un sistema operativo de red.

Todas las computadoras requieren un sistema operativo para funcionar, incluso los dispositivos de red basados en PC, como switches, routers, puntos de acceso y firewalls. Estos dispositivos de red utilizan un sistema operativo conocido como sistema operativo de red.

Un sistema operativo de red habilita el hardware del dispositivo que funcione y proporciona una interfaz para que los usuarios interactúen. En el curso de CCNA, los alumnos aprenden a configurar los dos dispositivos que se conectan a la red (terminales como PC) y dispositivos que conectan redes entre sí (dispositivos intermediarios como routers y switches). Aprender a configurar el sistema operativo Internetwork de Cisco (Cisco IOS) en routers y switches de Cisco es una gran parte del programa de estudio de CCNA de Cisco.

El Sistema operativo Internetwork (IOS) 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.

Actividad de clase: Es solo un sistema operativo

En esta actividad, imagine que lo contratan como ingeniero para una empresa automotriz. Actualmente, la empresa trabaja en un nuevo modelo de automóvil. Este modelo tendrá ciertas funciones que el conductor podrá controlar mediante comandos de voz específicos.

Diseñe el conjunto de comandos que utiliza este sistema de control activado por voz e identifique la forma en que se ejecutarán. Las funciones del automóvil que se pueden controlar mediante comandos de voz son las siguientes:

- Luces
- Limpiaparabrisas
- Radio
- Equipo de teléfono
- Aire acondicionado
- Encendido

Cisco IOS. Sistemas operativos.

Todos los terminales y dispositivos de red requieren un sistema operativo (SO). Como se muestra en la figura 1, la parte del SO que interactúa directamente con el hardware de la PC se conoce como núcleo. La parte 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) o la interfaz gráfica del usuario (GUI).

Al emplear la CLI como se muestra en la figura 2, 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 CLI necesita muy poca sobrecarga para operar. Sin embargo, exige que el usuario tenga conocimientos de la estructura subyacente que controla el sistema.

Una interfaz GUI, como Windows, SO X, Apple IOS o Android, permite que el usuario interactúe con el sistema en un entorno que utiliza íconos gráficos, menús y ventanas. El ejemplo de GUI en la figura 3 es más fácil de utilizar y exige menos conocimientos de la estructura de comandos subyacente que controla el sistema. Por este motivo, muchas personas prefieren los entornos GUI.

Sin embargo, las GUI no siempre pueden proporcionar todas las funcionalidades que hay disponibles en la CLI. Las GUI también pueden fallar, colapsar o simplemente no operar como se les indica. Por estos motivos, se suele acceder a los dispositivos de red mediante una CLI. La CLI consume menos recursos y es muy estable en comparación con una GUI.

El sistema operativo de red que se utiliza en los dispositivos Cisco se denomina Sistema operativo Internetwork (IOS). Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo de dispositivo.

Nota: 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

SHELL

la interfaz del usuario que permite a los usuarios solicitar tareas específicas desde la computadora. Estas solicitudes se pueden llevar a cabo a través de interfaces CLI o GUI.

Kernel

Establece la comunicación entre el hardware y el software de una computadora y administra el uso de los recursos de hardware para cumplir los requisitos del software.

Hardware

La parte física de una computadora, incluida la electrónica subyacente.

Propósito de los SO

Los sistemas operativos de red son similares al sistema operativo de una PC. Mediante una GUI, un sistema operativo de PC permite que el usuario realice lo siguiente:

- Utilice un mouse para hacer selecciones y ejecutar programas.
- Introduzca texto y comandos de texto.
- Vea resultados en un monitor.

Un sistema operativo basado en CLI como el Cisco IOS en un switch o router, permite que un técnico de red realice lo siguiente:

- Utilice un teclado para ejecutar programas de red basados en la CLI.
- Utilice un teclado para introducir texto y comandos basados en texto.
- Vea resultados en un monitor.

Los dispositivos de red de Cisco ejecutan versiones especiales 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 se muestra una lista de las versiones del software IOS para un switch Cisco Catalyst 2960.

Acceso a Cisco IOS: Métodos de acceso

Un switch de Cisco puede implementarse sin ninguna configuración, y de todas maneras conmutará los datos entre los dispositivos conectados. Al conectar dos PC a un switch, esas PC tienen conectividad mutua en forma inmediata.

Si bien un switch de Cisco funcionará de inmediato, la mejor práctica recomendada es configurar los parámetros iniciales. Existen varias formas de acceder al entorno de la CLI y configurar el dispositivo. Los métodos más comunes son los siguientes:

- **Consola:** este es un puerto de administración que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de mantenimiento del dispositivo.
- **Shell seguro (SSH):** SSH es un método para establecer de manera remota una conexión CLI segura a través de una interfaz virtual por medio de una red. A diferencia de las conexiones de consola, las conexiones SSH requieren servicios de red activos en el dispositivo, incluida una interfaz activa configurada con una dirección.
- **Telnet:** Telnet es un método inseguro para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. A diferencia de las conexiones SSH, Telnet no proporciona una conexión cifrada de manera segura. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.

Nota: Algunos dispositivos, como routers, también pueden admitir un puerto auxiliar antiguo que se utilizaba para establecer una sesión de CLI de forma remota con un módem. Al igual que la conexión de consola, el puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red.

Consola 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 computadora con software de emulación de terminal se conecta al puerto de consola del dispositivo mediante un cable especial. En la computadora conectada pueden ingresarse los comandos de configuración para iniciar el switch o el router.

SSH El SSH es el método recomendado para administración remota ya que proporciona una conexión segura. El SSH proporciona autenticación de contraseña y transporte de 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. La mayoría de las versiones de Cisco IOS incluyen un servidor SSH y un cliente SSH que pueden utilizarse para establecer sesiones SSH con otros dispositivos.

Telnet Las mejores prácticas aconsejan el uso de SSH en lugar de Telnet para las conexiones de administración remota de la CLI. Cisco IOS incluye un servidor Telnet y un cliente Telnet que pueden utilizarse para establecer sesiones Telnet con otros dispositivos.

Programas de emulación de terminal

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)
- 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.

Navegación de IOS.

Modos de funcionamiento de Cisco IOS.

Para configurar por primera vez un dispositivo Cisco, se debe establecer una conexión de consola. Una vez listo este paso, el técnico de red debe navegar a través de diversos modos de comando de la CLI del IOS. Los modos de Cisco IOS utilizan una estructura jerárquica y son muy similares para switches y routers.

Modos del comando primario

Como característica de seguridad, el software IOS de Cisco divide el acceso de administración en los siguientes dos modos de comando:

- **Modo de ejecución de usuario:** este tiene capacidades limitadas pero resulta útil en el caso de algunas operaciones básicas. Permite solo una cantidad limitada de comandos de monitoreo básicos, pero no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo. El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >
- **Modo de ejecución privilegiado:** para ejecutar comandos de configuración, un administrador de redes debe acceder al modo de ejecución privilegiado. Solo se puede ingresar al modo de configuración global y a los modos de configuración más altos por medio del modo EXEC privilegiado. El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #.

La tabla de la figura resume los dos modos y muestra las peticiones de entrada de la CLI predeterminadas de un router y switch de Cisco.

Configuración de los modos de comando

Para configurar el dispositivo, el usuario debe ingresa al **modo de configuración global,** que normalmente se denomina "modo de config. global".

Desde el momo de 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 se identifica por una petición de entrada que finaliza con (config)# luego del nombre del dispositivo, como **Switch(config)#.**

Antes de acceder a otros modos de configuración específicos, se accede al modo de configuración global. 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. Los dos tipos de modos de subconfiguración incluyen lo siguiente:

- **Modo de configuración de línea:** se utiliza para configurar la consola, SSH, Telnet o el acceso auxiliar.
- **Modo de configuración de interfaz:** se utiliza para configurar un puerto de switch o una interfaz de red de router.

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 para el modo de configuración de línea es **Switch(config-line)#** y la petición de entrada predeterminada para el modo de configuración de interfaz es **Swith(config-if)#.**

Navegación entre los modos de IOS

Se utilizan varios comandos para pasar dentro o fuera de los comandos de petición de entrada. Para pasar del modo EXEC del usuario al modo EXEC privilegiado, ingrese el comando **enable.** Utilice el comando **disable** del modo EXEC privilegiado para regresar al modo EXEC del usuario.

Nota: El modo EXEC privilegiado se suele llamar modo enable.

Para pasar dentro y fuera del modo de configuración global, utilice el comando **configure terminal** del modo EXEC privilegiado. Para regresar al modo EXEC privilegiado, introduzca el comando **exit** en el modo de configuración global.

Existen diversos tipos de modos de subconfiguración. Por ejemplo, para introducir un modo de subconfiguración, debe utilizar el comando **line** seguido del número y tipo de línea de administración al que desea acceder. Para salir de un modo de subconfiguración y volver al modo de configuración global, utilice el comando **exit.** Observe los cambios en el comando de petición de entrada.

*Switch(config)# **line console 0***

Switch(config-line)#

Para pasar de cualquier modo de subconfiguración del modo de configuración global al modo que se encuentra un nivel más arriba en la jerarquía de modos, introduzca el comando exit.

Switch(config-line)# exit

Switch(config)#

Para pasar de cualquier modo de subconfiguración al modo EXEC privilegiado, introduzca el comando **end** o presione la combinación de teclas **Ctrl+Z.**

Switch(config-line)# ***end***

Switch#

Puede trasladarse directamente desde un modo de subconfiguración a otro. Observe cómo después del nombre del dispositivo de red, el comando de petición de entrada cambia de (config-line)# a (config-if)#.

Switch(config-line)# ***interface FastEthernet 0/1***

La estructura de los comandos.

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.

- Palabra clave: un parámetro específico que se define en el sistema operativo (en la figura, protocolos ip).
- Argumento - no está predefinido; es un valor o variable definido por el usuario, (en la figura, 192.168.10.5)

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

Sintaxis de comandos IOS

Un comando podría requerir uno o más argumentos. 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.

Como se identifica en la tabla de la figura, el texto en negrita indica comandos y palabras clave que se introducen literalmente como se muestra. El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.

Por ejemplo, la sintaxis para utilizar el comando description es la cadena de caracteres description . El argumento es un valor de cadena de caracteres proporcionado por el usuario. El comando description suele utilizarse para identificar el propósito de una interfaz. Por ejemplo, cuando se ingresa el comando, description se conecta al switch de la oficina de la sede principal, describe la ubicación del otro dispositivo al otro extremo de la conexión.

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

- **ping** ip-address - El comando es ping y el argumento definido por el usuario es la ip-address del dispositivo de destino. Por ejemplo, haga ping a 10.10.10.5.
- **traceroute** ip-address - El comando es traceroute y el argumento definido por el usuario es la ip-address del dispositivo de destino. Por ejemplo, traceroute 192.168.254.254.

La referencia de comando de Cisco IOS es la última fuente de información para un comando de IOS en particular.

Característica de ayuda de IOS

El IOS tiene dos formas de ayuda disponible:

- Ayuda contextual
- Verificación de la sintaxis del comando

La ayuda contextual le permite encontrar rápidamente los comandos que están disponibles en cada modo de comando, qué comandos comienzan con caracteres o grupo de caracteres específicos y qué argumentos y palabras clave están disponibles para comandos determinados. Para acceder a la ayuda contextual, ingrese un signo de interrogación, **?**, en la CLI.

La verificación de la sintaxis del comando comprueba que el usuario haya introducido un comando válido. Cuando se introduce un comando, el intérprete de la línea de comandos analiza al comando de izquierda a derecha. 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.

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

Los comandos y las palabras clave pueden acortarse a la cantidad mínima de caracteres que identifica a una selección única. Por ejemplo, el comando configure **puede acortarse a** conf**, ya que** configure **es el único comando que empieza con** conf**. Una versión más breve, como** con**, no dará resultado, ya que hay más de un comando que empieza con** con**. Las palabras clave también pueden acortarse.**

Nombres de host.

Nombres de los dispositivos.

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.

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”. Si se dejara el nombre predeterminado en todos los dispositivos de red, sería difícil identificar un dispositivo determinado. Por ejemplo, al acceder a un dispositivo remoto mediante SSH, es importante tener la confirmación de que se está conectado al dispositivo correcto.

Al elegir nombres atinadamente, resulta más fácil recordar, analizar e identificar los dispositivos de red.

Pautas para la configuración de nombres de host.

Los Nombre de host deben:

- 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.

Por ejemplo, en la figura 1, tres switches que se encuentran en tres pisos diferentes están interconectados en una red. La convención de denominación que se utilizó tuvo en cuenta la ubicación y el propósito de los dispositivos. La documentación de red debe explicar cómo se seleccionaron estos nombres para que se pueda seguir el mismo criterio en la denominación de los dispositivos adicionales.

Configuración de los nombres de host

Una vez que se ha identificado la convención de denominación, el próximo paso es aplicar los nombres a los dispositivos usando la CLI.

Como se muestra en la figura 1, desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando **configure terminal:** Observe el cambio en el comando de petición de entrada.

Desde el modo de configuración global, introduzca el comando **hostname** seguido del nombre del switch y presione la tecla Intro. Observe el cambio en el comando de petición de entrada.

Nota: Para eliminar el nombre de host configurado y regresar a la petición de entrada predeterminada, utilice el comando de configuración global **no hostname**

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.

Limitación del acceso a las configuraciones de los dispositivos. Acceso seguro de los dispositivos.

El uso de contraseñas simples o fáciles de adivinar continúa siendo un problema de seguridad en muchas facetas del mundo empresarial. Los dispositivos de red, incluso los routers inalámbricos hogareños, siempre deben tener contraseñas configuradas para limitar el acceso administrativo.

Cisco IOS puede configurarse para utilizar contraseñas en modo jerárquico y permitir diferentes privilegios de acceso al dispositivo de red.

Todos los dispositivos de red deben tener acceso limitado.

Protección de acceso administrativo

- Proteja el acceso a EXEC privilegiado con una contraseña
- Proteja el acceso a EXEC de usuario con una contraseña
- Proteja el acceso a Telnet remoto con una contraseña
- Encripte todas las contraseñas
- Proporcione notificación legal

Other task

- Encrypt all passwords
- Provide legal notification

Utilice contraseñas seguras que no se descubran fácilmente.

Cuando seleccione contraseñas

- Use contraseñas que tengan más de 8 caracteres.
- Use una combinación de letras mayúsculas y minúsculas, números, caracteres especiales o secuencias numéricas.
- Evite el uso de la misma contraseña para todos los dispositivos.
- No use palabras comunes porque se descubren fácilmente.

Nota: En la mayoría de las prácticas de laboratorio, usaremos contraseñas simples como **cisco** o **clase**. Estas contraseñas se consideran simples y fáciles de adivinar, y deben evitarse en un entorno de producción. Estas contraseñas solo se utilizan por comodidad en el aula o para ilustrar ejemplos de configuración.

Cifrado de las contraseñas

Los archivos startup-config y running-config muestran la mayoría de las contraseñas en texto no cifrado. Esta es una amenaza de seguridad dado que cualquier persona puede ver las contraseñas utilizadas si tiene acceso a estos archivos.

Para cifrar las contraseñas, utilice el comando de configuración global **service password-encryption**. El comando aplica un cifrado débil a todas las contraseñas no cifradas. Este cifrado 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.

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 solo 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.

Para crear un mensaje de aviso del día en un dispositivo de red, utilice el comando de configuración global **banner motd #** el mensaje del día **#**. El símbolo "#" en la sintaxis del comando se denomina carácter delimitador. Se ingresa antes y después 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 "#". 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.

Guardar el archivo de configuración en ejecución.

Existen dos archivos de sistema que almacenan la configuración de dispositivos.

- **startup-config:** el archivo almacenado en la memoria no volátil de acceso aleatorio (NVRAM) que contiene todos los comandos que utilizará el dispositivo durante el inicio o reinicio. La memoria NVRAM no pierde su contenido cuando el dispositivo se desconecta.
- **running-config:** el archivo almacenado en la memoria de acceso aleatorio (RAM) que refleja la configuración actual. La modificación de una configuración en ejecución afecta el funcionamiento de un dispositivo Cisco de inmediato. La memoria RAM es volátil. Pierde todo el contenido cuando el dispositivo se apaga o se reinicia

Como se muestra en la figura, se puede utilizar el comando **show running-config** en el modo EXEC privilegiado para ver un archivo de configuración en ejecución. Para ver el archivo de configuración de inicio, ejecute el comando **show startup-config** en el modo EXEC privilegiado.

Si se corta la energía al dispositivo o si este se reinicia, se perderán todos los cambios de configuración a menos que se hayan guardado. Para guardar los cambios realizados en la configuración en ejecución en el archivo de configuración de inicio utilice el comando **copy running-config startup-config** en el modo EXEC privilegiado.

.Configuración de contraseñas

La contraseña más importante para configurar es la de acceso al modo EXEC privilegiado, como se muestra en la figura 1. Para proteger el acceso a EXEC privilegiado, utilice el comando de configuración global **enable secret** *password.*

Para proteger el acceso a EXEC de usuario, el puerto de consola debe estar configurado, como se muestra en la figura 2. Ingrese al modo de configuración de consola de línea con el comando de configuración global **line console 0**. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola. Luego, configure la contraseña de modo EXEC de usuario con el comando **password** *password*. Finalmente, habilite el acceso EXEC de usuario con el comando **login**. El acceso a la consola ahora requerirá una contraseña antes de poder acceder al modo EXEC del usuario.

Las líneas de terminal virtual (VTY) habilitan el acceso remoto al dispositivo. Para proteger las líneas VTY que se utilizan para SSH y Telnet, ingrese al modo de línea VTY con el comando de configuración global **line vty 0 15**, como se muestra en la figura 3. Muchos switches de Cisco admiten hasta 16 líneas VTY que se numeran del 0 al 15. Luego, especifique la contraseña de VTY con el comando **password** *password*. Por último, habilite el acceso a VTY con el comando **login**.

Modificación de la configuración en ejecución

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado y el archivo running-config aún no se ha guardado, puede restablecer el dispositivo a su configuración anterior eliminando los comandos modificados, o bien volver a cargar el dispositivo con el comando **reload** en el modo EXEC con privilegios para restablecer la configuración de inicio.

La desventaja de utilizar el comando reload para eliminar una configuración en ejecución sin guardar es el breve tiempo que el dispositivo estará sin conexión, lo que provoca tiempo de inactividad de la red.

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. Para descartar los cambios, ingrese **n** o **no**.

Como alternativa, 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** en el modo EXEC privilegiado. Una vez que se emite el comando, el switch le solicita confirmación. Presione **Intro** para aceptar.

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. En la recarga, un switch cargará la configuración de inicio predeterminada que se envió originalmente con el dispositivo

Captura de configuración a un archivo de texto

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

Por ejemplo, suponga que se configuró un switch y que la configuración en ejecución se guardó en el dispositivo.

- Abra un software de emulación de terminal como PuTTY o Tera Term (figura 1) conectado a un switch.
- Habilite el inicio de sesión al software de terminal, como PuTTY o Tera Term y asigne un nombre y ubicación de archivo donde guardar el archivo de registro. La figura 2 muestra que **todos los resultados de sesión** se capturarán en el archivo especificado (es decir, MySwitchLogs).
- 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 del terminal se colocará en el archivo elegido.
- Desactive el inicio de sesión en el software del terminal. En la figura 3 se muestra desactivar el inicio de sesión mediante la selección de la opción de inicio de sesión **None**.

El archivo de texto creado se puede utilizar como un registro del modo en que se implementa actualmente el dispositivo. El archivo puede requerir edición antes de poder utilizarse para restaurar una configuración guardada a un dispositivo.

Para restaurar un archivo de configuración a un dispositivo:

- Ingrese al modo de configuración global en el dispositivo.
- Copie y pegue el archivo de texto en la ventana del terminal conectada al switch.

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