CAPÍTULO 2: CONFIGURACIÓN DE UN SISTEMA OPERATIVO DE RED

2.0.1.1 Introducción

Los dispositivos de red basados en PC, como swiches, routers, puntos de acceso o firewalls utilizan un sistema operativo conocido como un sistema operativo de red. Este sistema operativo habilita el hardware del dispositivo para que funcione y proporciona una interfaz para que los usuarios interactúen.

2.1.1.1 Sistemas operativos

Todos los terminales y dispositivos de red requieren un sistema operativo (SO) que se puede dividir en tres partes:

- **Hardware**: parte física de una computadora.
- **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.
- **Shell**: interfaz de 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.

Interfaz CLI

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 CLI necesita muy poca sobrecarga para operar. Sin embargo, exige que el usuario tenga conocimientos de la estructura subyacente que controla el sistema.

Interfaz GUI

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. Es más fácil de utilizar y exige menos conocimientos de la estructura de comandos subyacente que controla el sistema.

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.

2.1.2.1 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.

  La ventaja de usar un puerto de consola es que es posible acceder al dispositivo incluso si no se configuró ningún servició 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 puede ingresarse los comandos de configuración para iniciar el switch o el router.

- **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.

  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:** 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.

2.1.2.2 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
- Tera Term
- SecureCRT
- OS X Terminal

2.1.3.2 Modos del comando primario

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

Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC del usuario	• Permite el acceso solamente a una cantidad limitada de comandos básicos de monitoreo. • A menudo se le describe como un modo de "visualización solamente".	`Switch>` `Router>`
Modo EXEC privilegiado	• Permite el acceso a todos los comandos y funciones. • El usuario puede utilizar cualquier comando de monitoreo y ejecutar comandos de configuración y de administración.	`Switch#` `Router#`

2.1.3.3 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 modo 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)#**

2.1.3.4 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**

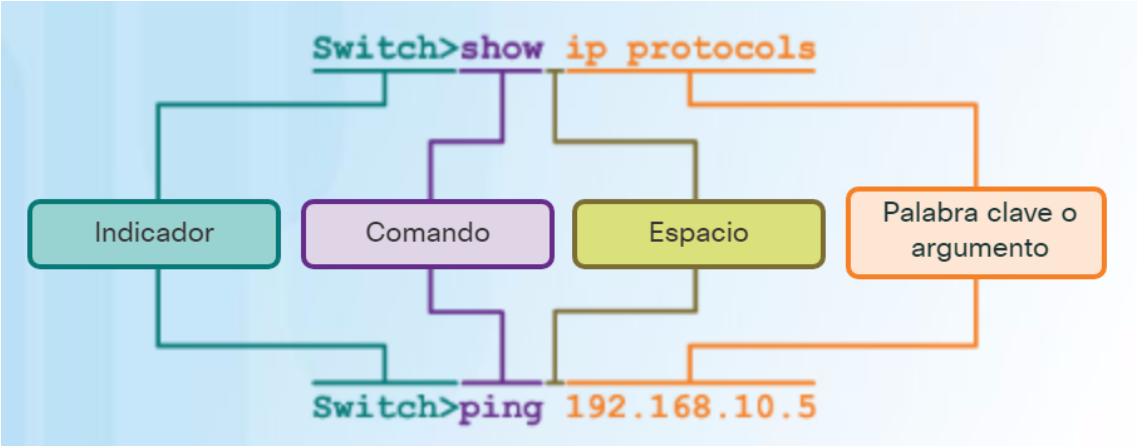
Switch(config-if)#

2.1.4.1 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.



2.1.4.2 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.

Cuando se describe el uso de comandos, generalmente utilizamos estas convenciones.

Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que se introducen literalmente como se muestran.
cursiva	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento opcional (palabra clave o argumento).
{x}	Las llaves indican un elemento obligatorio (palabra clave o argumento).
[x {y | z}]	Las llaves y las líneas verticales dentro de corchetes indican una opción obligatoria dentro de un elemento opcional.

2.1.4.3 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.

2.1.4.4 Teclas de acceso rápido y métodos abreviados

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.

Edición de líneas de la CLI	
Tabulación	Completa una entrada de nombre de comando parcial.
Retroceso	Borra el carácter a la izquierda del cursor.
Ctrl-D	Borra el carácter donde está el cursor.
Ctrl-K	Borra todos los caracteres desde el cursor hasta el final de la línea de comandos.
Esc D	Borra todos los caracteres desde el cursor hasta el final de la palabra.
Ctrl-U o Ctrl-X	Borra todos los caracteres desde el cursor hasta el comienzo de la línea de comandos.
Ctrl-W	Borra la palabra a la izquierda del cursor.
Ctrl-A	Desplaza el cursor hacia el principio de la línea.
Flecha izquierda o Ctrl-B	Desplaza el cursor un carácter hacia la izquierda.
Esc B	Desplaza el cursor de una palabra hacia la izquierda.
Esc F	Desplaza el cursor una palabra hacia la derecha.
Flecha derecha o Ctrl-F	Desplaza el cursor un carácter hacia la derecha.
Ctrl-E	Desplaza el cursor hasta el final de la línea de comandos.
Flecha arriba o Ctrl-P	Vuelve a introducir el comando que se encuentra en el búfer del historial a partir de los comandos más recientes.
Ctrl-R, Ctrl-l o Ctrl-L	Vuelve a mostrar la petición de entrada del sistema y la línea de comando después de que se recibe un mensaje de la consola.
NOTA: “Eliminar”, la tecla para eliminar a la derecha del cursor no es reconocida por los programas de emulación de terminales.	

En la petición de entrada "----More----"	
Tecla Entrar	Muestra la siguiente línea.
Barra espaciadora	Muestra la siguiente pantalla.
Cualquier tecla	Termina la cadena que se muestra y vuelve al modo EXEC privilegiado.

Teclas de interrupción	
Ctrl-C	Cuando está en cualquier modo de configuración, terina el modo de configuración y regresa al modo EXEC privilegiado. Cuando está en modo de configuración, interrumpe y regresa al símbolo del sistema.
Ctrl-Z	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC privilegiado.
Ctrl-Shift-6	Secuencia de pausa multiuso. Se utiliza para interrumpir búsquedas DNS, traceroutes, pings.
NOTA: Teclas de control: mantenga presionada la tecla y luego presione la tecla dela letra especificada. Secuencias de escape: presione y libere la tecla y luego presione la tecla de la letra.	

2.2.1.1 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.

Los nombres 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.

NOTA: Se distinguen entre mayúsculas y minúsculas.

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**.

2.2.2.1 Acceso seguro de los dispositivos

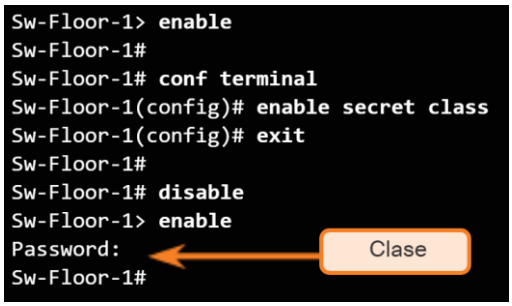
Cisco IOS puede configurarse para utilizar contraseñas en modo jerárquico y permitir diferentes privilegios de acceso al dispositivo de red. Todos los dispositivos de red deben tener acceso limitado para:

- Proteger el acceso de EXEC privilegiado con una contraseña.
- Proteger el acceso a EXEC de usuario con una contraseña.
- Proteger el acceso a Telnet remoto con una contraseña.

2.2.2.2 Configuración de contraseñas

Contraseña para el modo EXEC privilegiado

Utilice el comando de configuración global **enable secret** *password*.



Contraseña para el modo EXEC usuario

Para proteger el acceso a EXEC de usuario, el puerto de consola debe estar configurado. 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.

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
Sw-Floor-1(config)#
```

Contraseña para las líneas de terminal virtual

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**. 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**.

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#
```

2.2.2.3 Cifrado de las contraseñas

El comando show running-configuration permite ver las contraseñas que hemos puesto. En caso de estar encriptadas, veremos la encriptación y si no lo están, veremos la propia contraseña.

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.

2.2.2.4 Mensajes de aviso

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 de acceso al dispositivo hasta que el aviso se elimine.

2.2.3.1 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.

2.2.3.2 Modificación de la configuración en ejecución

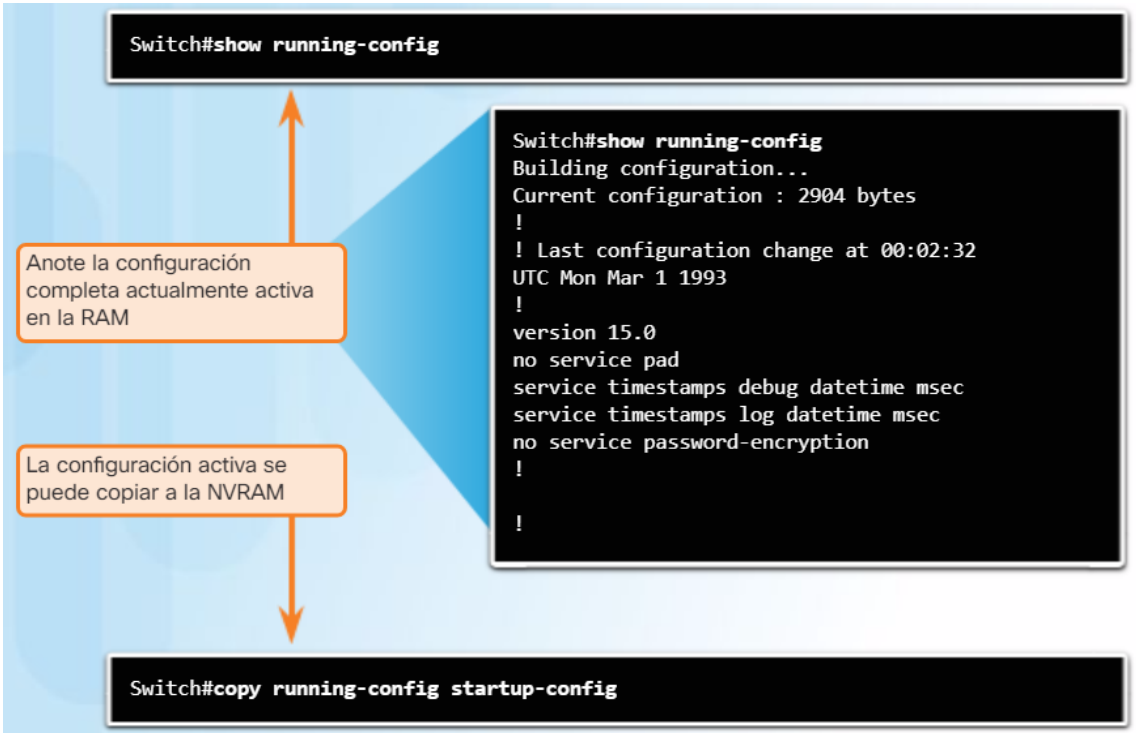
Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado y el archivo running-config aún no se ha guardado, puede restablecer el dispositivo a su configuración anterior eliminando los comandos modificados, o bien volver a cargar el dispositivo con el comando **reload** en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



2.2.3.3 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.

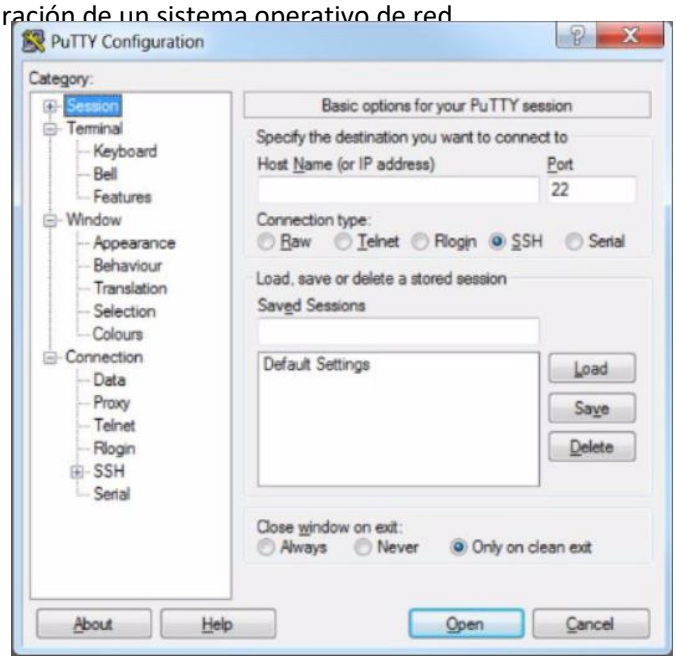
El archivo de texto creado se puede utilizar como un registro del modo en que se implementa actualmente el dispositivo. El archivo puede requerir edición antes de poder utilizarse para restaurar una configuración guardada a un dispositivo.

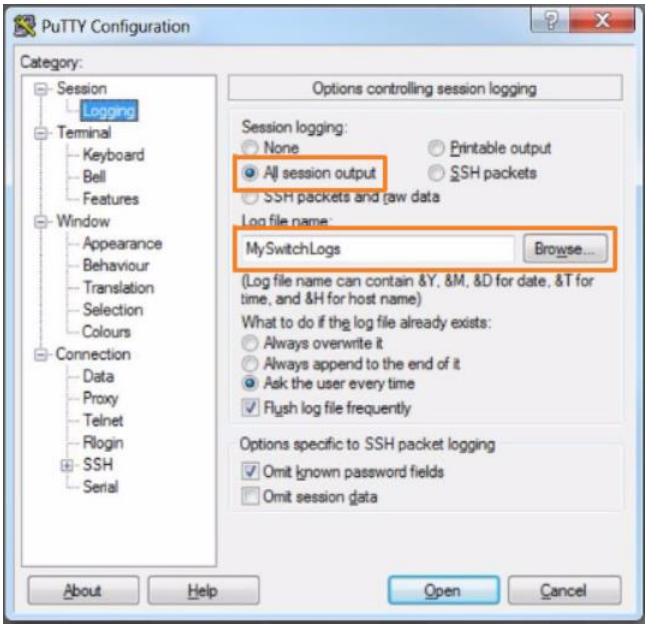
Para restaurar un archivo de configuración a un dispositivo:

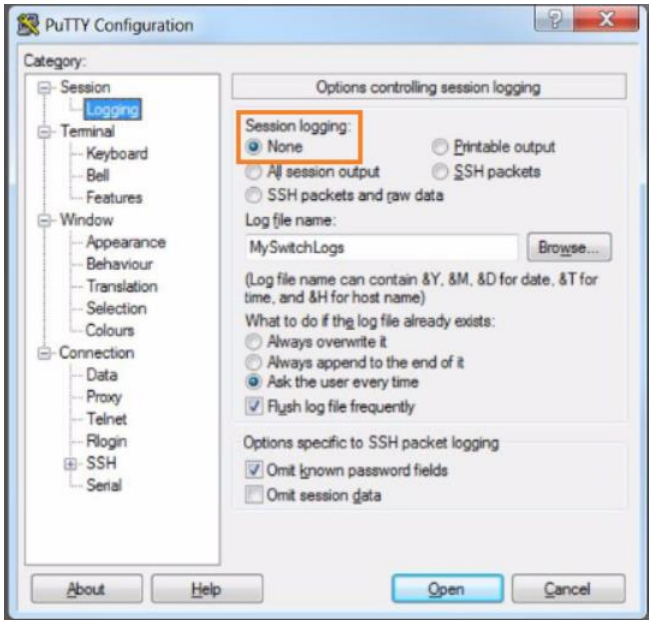
- Ingrese al modo de configuración global en el dispositivo.

- 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.


PuTTY Configuration
Category:
Session
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Options controlling session logging
Session logging:
None
Printable output
All session output
SSH packets
SSH packets and raw data
Log file name:
MySwitchLogs
Browse...
(Log file name can contain &Y, &M, &D for date, &T for time, and &H for host name)
What to do if the log file already exists:
Always overwrite it
Always append to the end of it
Ask the user every time
Flush log file frequently
Options specific to SSH packet logging
Omit known password fields
Omit session data
About
Help
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Options controlling session logging
Session logging:
None
Printable output
All session output
SSH packets
SSH packets and raw data
Log file name:
MySwitchLogs
Browse...
(Log file name can contain &Y, &M, &D for date, &T for time, and &H for host name)
What to do if the log file already exists:
Always overwrite it
Always append to the end of it
Ask the user every time
Flush log file frequently
Options specific to SSH packet logging
Omit known password fields
Omit session data
About
Help
Open
Cancel

2.3.1.1 Direcciones IP

El uso de direcciones IP es el principal medio para permitir que los dispositivos se ubiquen entre sí y para establecer la comunicación completa en Internet. Cada terminal en una red se debe configurar con direcciones IP.

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.

Nota: en este curso, IP refiere a los protocolos IPv4 e IPv6. IPv6 es la versión más reciente de IP y el reemplazo para el protocolo IPv4 más común.

Con la dirección IPv4, también se necesita una máscara de subred. Una máscara de subred IPv4 es un valor de 32 bits que separa la porción de red de la dirección de la porción de host. Combinada con la dirección IPv4, la máscara de subred determina la subred particular a la pertenece el dispositivo.

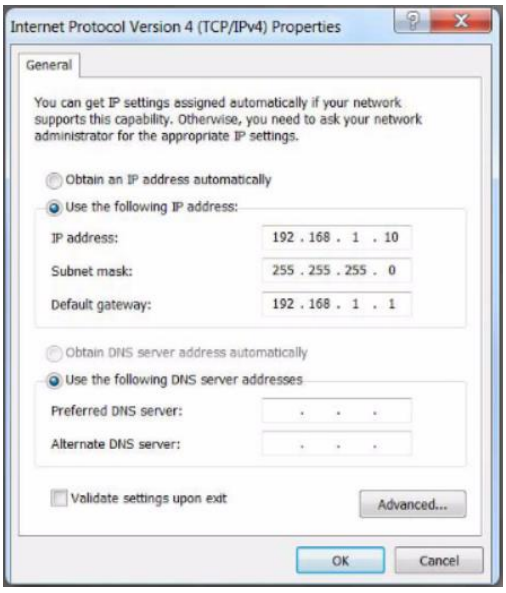
El ejemplo de la figura 2 muestra la dirección IPv4 (192.168.1.10), la máscara de subred (255.255.255.0) y el gateway predeterminado (192.168.1.1) asignados a un host. La dirección de gateway predeterminado es la dirección IP del router que el host utilizará para acceder a las redes remotas, incluso a Internet.

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.

Los switches de la capa 2 de Cisco IOS cuentan con puertos físicos para conectar dispositivos. Estos puertos no son compatibles con las direcciones IP de la capa 3. En consecuencia, los switches tienen una o más interfaces virtuales de switch (SVI). Son interfaces virtuales porque no hay hardware físico en el dispositivo asociado a ellas. Una SVI se crea 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, fácil de instalar. La SVI predeterminada es interfaz VLAN1.

Nota: Un switch de capa 2 no necesita una dirección IP. La dirección IP asignada a la SVI se utiliza para acceder al switch de forma remota. No se necesita una dirección IP para que el switch realice estas operaciones.



2.3.2.1 Configuración manual de direcciones IP para terminales

Para que un terminal se comunique a través de la red, se debe configurar con una dirección IPv4 y una máscara de subred únicas. La información de dirección IP se puede introducir en los terminales en forma manual o automáticamente mediante el Protocolo de configuración dinámica de host (DHCP).

Para configurar una dirección IPv4 de forma manual en un host de Windows, abra **Panel de Control > Centro de redes y recursos compartidos > Cambiar configuración del adaptador** y seleccione el adaptador. Luego, haga clic con el botón secundario y seleccione **Propiedades** para que aparezcan las **Propiedades de conexión de área local**, como se muestra en la figura 1.

Resalte el protocolo de Internet versión 4 (TCP/IPv4) y haga clic en **Propiedades** para abrir la ventana de **Propiedades del protocolo de Internet versión 4 (TCP/IPv4)**, como se muestra en la figura 2. Configure la información de la dirección IPv4 y la máscara de subred, y el gateway predeterminado.

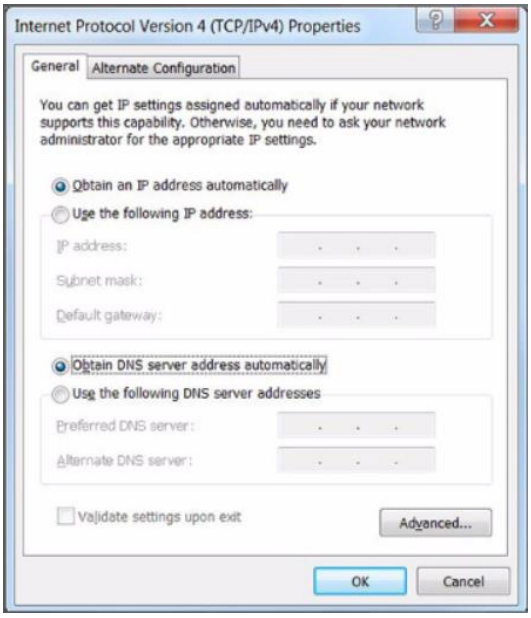
Nota: La dirección del servidor DNS es la dirección IPv4 del servidor del sistema de nombres de dominio (DNS), que se utiliza para traducir direcciones IP a direcciones web, como www.cisco.com.

2.3.2.2 Configuración automática de direcciones IP para terminales

En general, las PC utilizan DHCP de forma predeterminada para la configuración automática de direcciones IPv4. DHCP es una tecnología que se utiliza en casi todas las redes. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo.

En una red, DHCP permite la configuración automática de direcciones IPv4 para cada terminal con DHCP habilitado. Para configurar el protocolo DHCP en una PC con Windows, solo debe seleccionar “Obtener una dirección IP automáticamente” y “Obtener la dirección del servidor DNS automáticamente”. Su PC buscará un servidor DHCP y se le asignarán los ajustes de dirección necesarios para comunicarse en la red.

Es posible mostrar los ajustes de configuración IP en una PC con Windows usando el comando **ipconfig**cuando el sistema se lo solicite. El resultado muestra la información de dirección IPv4, máscara de subred y gateway que se recibió del servidor DHCP.



2.3.2.3 Configuración de la interfaz virtual de switch

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI. Para configurar una SVI en un switch, utilice el comando de configuración global **interface vlan 1**. La Vlan 1 no es una interfaz física real, sino una virtual. A continuación, asigne una dirección IPv4 mediante el comando **ip address** *ip-address subnet-mask* de la configuración de interfaz. Finalmente, habilite la interfaz virtual con el comando de configuración de interfaz **no shutdown**.

Una vez que se configuran estos comandos, el switch tiene todos los elementos IPv4 listos para la comunicación a través de la red. Usando el comando show ip interface brief podemos ver si las interfaces están caídas o no y si están conectadas a un dispositivo.

(Aclarar el funcionamiento de la vlan).

2.3.3.1 Verificación de la asignación de direcciones de interfaz

Del mismo modo que se usan comandos y utilidades como **ipconfig** para verificar la configuración de red de un host de PC, se deben utilizar los comandos para verificar los ajustes de interfaces y dirección de los dispositivos intermediarios, como switches y routers.

Haga clic en el botón Reproducir en la figura para ver una demostración en vídeo sobre el comando **show ip interface brief**. Este comando es útil para verificar la condición de las interfaces de switch.

El comando **ping** puede utilizarse para probar la conectividad de otro dispositivo en la red o un sitio web en Internet.