

Capítulo 2: Configuración de un sistema operativo de red

CCNA routing y switching

Introducción a redes v6.0



2.1 Entrenamiento intensivo sobre IOS

Sistema operativo

Los dispositivos Cisco utilizan el **sistema operativo de Interwork (IOS)** de Cisco.

- Aunque es utilizada por Apple, iOS es una marca registrada de Cisco en los EE. UU. y otros países y es utilizada por Apple en virtud de una licencia.

- Todos los dispositivos electrónicos necesitan un sistema operativo.
 - Windows, Mac y Linux para PC y computadoras portátiles
 - Apple iOS y Android para smartphones y tablets
 - Cisco IOS para los dispositivos de red (p. ej., switches, routers, puntos de acceso inalámbricos, firewall).

Shell del SO

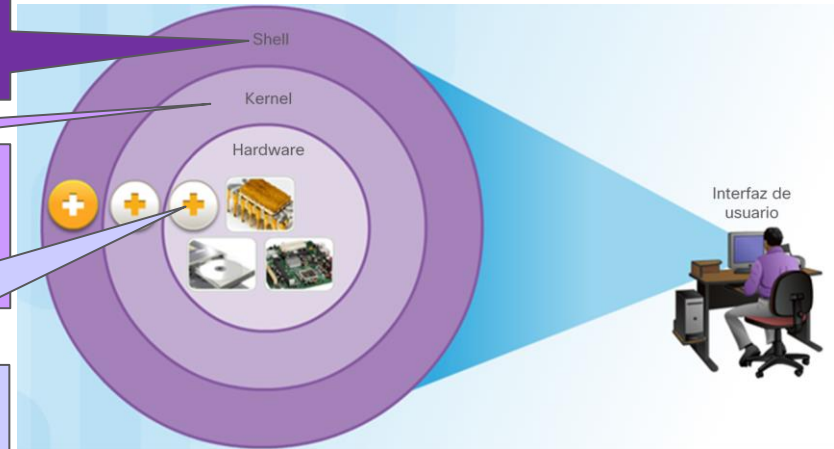
- El shell del SO es una interfaz de línea de comandos (CLI) o una interfaz gráfica de usuario (GUI) y permite que un usuario se interconecte con aplicaciones.

Núcleo del SO

- El núcleo del SO se comunica directamente con el hardware y administra la forma en que los recursos de hardware se utilizan para satisfacer requisitos de software.

Hardware

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



Propósito de los SO

- Mediante la utilización de una GUI, el usuario podrá hacer lo siguiente:
 - Utilice un mouse para hacer selecciones y ejecutar programas.
 - Introduzca texto y comandos de texto.

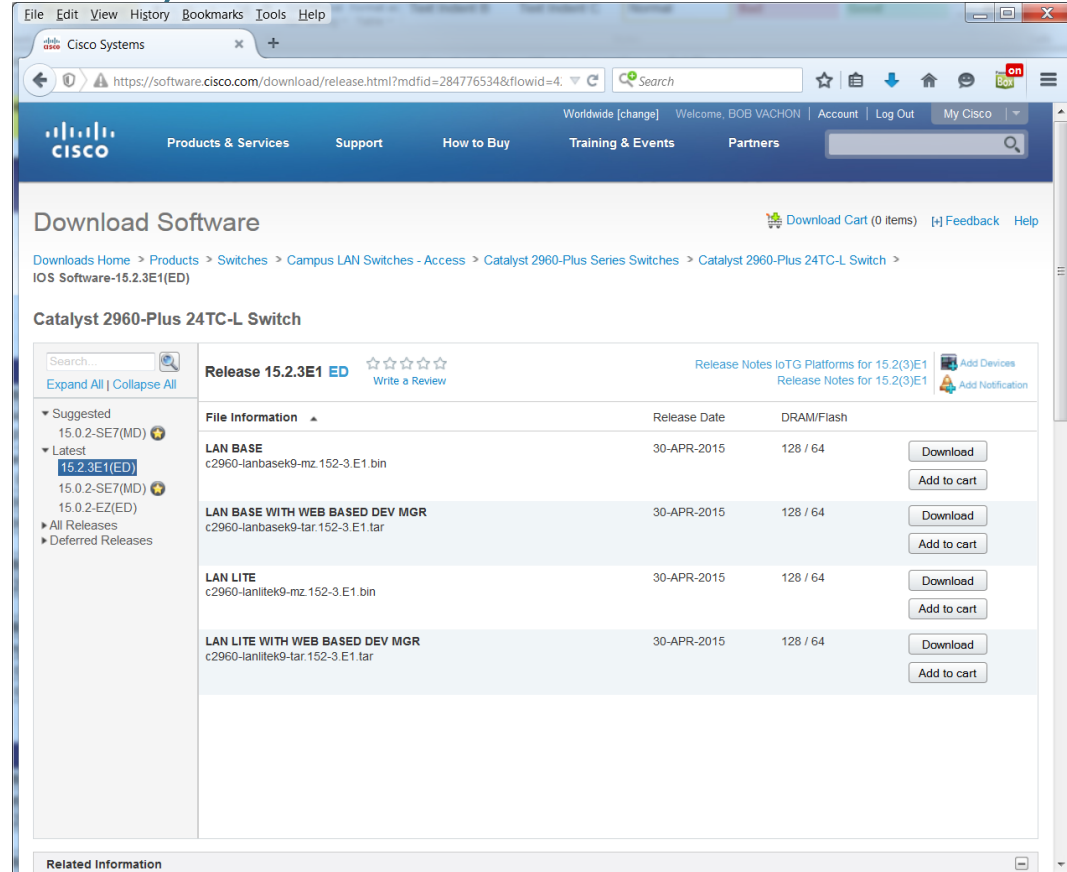
- Mediante la utilización de una CLI en un switch o router de Cisco IOS, el técnico en redes podrá hacer lo siguiente:
 - Utilice un teclado para ejecutar programas de red basados en la CLI.
 - Utilice un teclado para introducir texto y comandos basados en texto.

- 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

Propósito de los SO (continuación)

- Todos los dispositivos cuentan con un IOS predeterminado y conjunto de características. Es posible cambiar la versión o el conjunto de características del IOS.
- Los IOS pueden descargarse de cisco.com. Sin embargo, es necesario contar con una cuenta Cisco Connection Online (CCO).

Nota: El presente curso se centrará en Cisco IOS versión 15.x.



The screenshot shows the Cisco Software Download page for the Catalyst 2960-Plus 24TC-L Switch. The page displays the release 15.2.3E1(ED) with a table of software files for download. The table includes columns for File Information, Release Date, and DRAM/Flash size. Each row has 'Download' and 'Add to cart' buttons.

File Information	Release Date	DRAM/Flash
LAN BASE c2960-lanbasek9-mz.152-3.E1.bin	30-APR-2015	128 / 64
LAN BASE WITH WEB BASED DEV MGR c2960-lanbasek9-tar.152-3.E1.tar	30-APR-2015	128 / 64
LAN LITE c2960-lanlitek9-mz.152-3.E1.bin	30-APR-2015	128 / 64
LAN LITE WITH WEB BASED DEV MGR c2960-lanlitek9-tar.152-3.E1.tar	30-APR-2015	128 / 64

Métodos de acceso

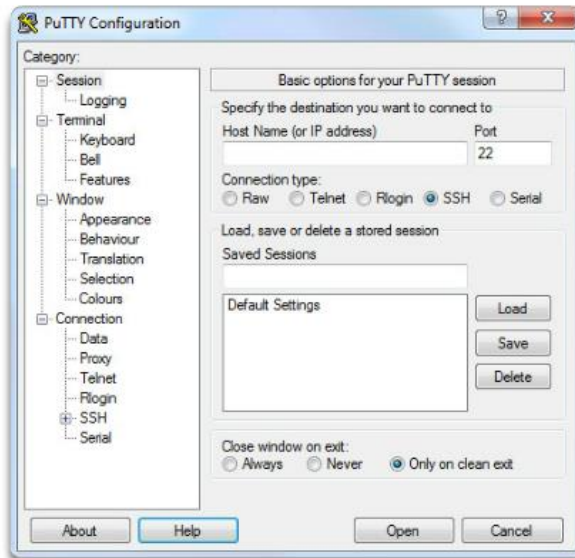
- Las tres formas más comunes de acceder al IOS son las siguientes:
 - **Puerto de consola:** puerto serial fuera de banda que se utiliza principalmente para propósitos de gestión como la configuración inicial del router.
 - **Shell seguro (SSH):** método en banda para establecer en forma remota y segura una sesión de CLI en una red. Se cifran la autenticación de usuario, las contraseñas y los comandos que se envían por la red. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.
 - **Telnet:** interfaces en banda para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.

Nota: El puerto AUX es un método más antiguo de establecer una sesión CLI en forma remota a través de una conexión por acceso telefónico a través de un módem.

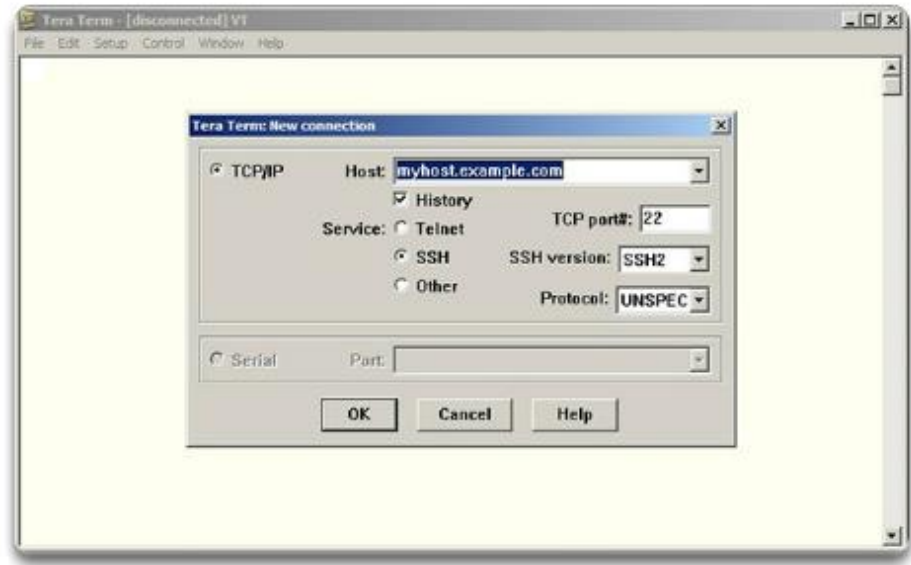
Programa de emulación de terminal

- Independientemente del método de acceso, se requerirá un programa de emulación de terminal. Entre los programas de emulación de terminal populares, se incluyen PuTTY, Tera Term, SecureCRT y OS X Terminal.

PuTTY



Tera Term



Modos de funcionamiento de Cisco IOS

- Los modos Cisco IOS utilizan una estructura de mando jerárquica.
- 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.



Modos de comando principales

- El modo EXEC del usuario permite solo una cantidad limitada de comandos de monitoreo básicos.
 - A menudo, se lo describe como un modo de “visualización solamente”.
 - En forma predeterminada, no se requiere autenticación para acceder al modo EXEC, pero debería obtenerse.
- El modo EXEC con privilegios permite la ejecución de comandos de administración y configuración.
 - A menudo, se lo describe como "modo enable" porque requiere el comando EXEC de usuario **enable**.
 - En forma predeterminada, no se requiere autenticación para acceder al modo EXEC, pero debería obtenerse.

Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC de usuario	<ul style="list-style-type: none">• 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 con privilegios	<ul style="list-style-type: none">• 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#

Modos de comandos de configuración

- El modo de configuración principal recibe el nombre de **configuración global** o, simplemente, **global config**.
 - Utilice el comando **configure terminal** para acceder.
 - Los cambios realizados afectan el funcionamiento del dispositivo.

- Desde el modo de configuración global, se puede acceder a modos de subconfiguración específicos. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS.
 - **Modo de interfaz:** para configurar una de las interfaces de red.
 - **Modo de línea:** para configurar la consola, AUX, Telnet o el acceso SSH.



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 con privilegios, ingrese el comando **enable**.
 - Para regresar al modo EXEC del usuario, use el comando **disable**.
- Pueden utilizarse diversos métodos para salir/abandonar los modos de configuración:
 - **Salida**: se utiliza para pasar de un modo específico al modo anterior más general, como del modo de interfaz al de global config.
 - **Final**: se puede utilizar para salir del modo de configuración global independientemente del modo de configuración en el que se encuentre.
 - **^ z**: funciona igual que **final**.



Navegación entre los modos de IOS (continuación)

- A continuación, encontrará un ejemplo de la navegación entre los modos de IOS:
 - Ingrese en el modo EXEC con privilegios con el comando **enable**.
 - Ingrese al modo global config mediante el comando **configure terminal**.
 - Ingrese al modo de sub-configuración de interfaz mediante el comando **interface fa0/1**.
 - Salga de cada modo mediante el comando **exit**.
 - El resto de la configuración muestra cómo puede salir de un modo de subconfiguración y regresar al modo EXEC con privilegios con la combinación de teclas **final** o **^Z**.



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 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 **ip protocols**)
 - 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 **Enter** (Introducir) para enviar el comando al intérprete de comandos.

Sintaxis de los comandos IOS

- Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulte la sintaxis de comandos
 - Consulte la tabla siguiente cuando analice la sintaxis de comandos.

Convención	Descripción
Negrita	El texto en negrita indica los comandos y las palabras clave que se introducen literalmente como se muestran.
<i>Cursiva</i>	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.

- Ejemplos:
 - **Descripción cadena:** se utiliza el comando para agregar una descripción a la interfaz. El argumento de *cadena* es texto ingresado por el administrador como **descripción** *Se conecta al switch de la oficina de la sede principal.*
 - **ping dirección-ip:** el comando es **ping** y el argumento definido por el usuario es la *dirección IP* del dispositivo de destino, como en el **ping** *10.10.10.5.*

Funciones de ayuda de IOS

- Ayuda contextual de IOS
 - La ayuda contextual proporciona una lista de comandos y los argumentos asociados con esos comandos en el contexto del modo actual.
 - Para acceder a la ayuda contextual, introduzca un signo de interrogación, ?, en cualquier petición de entrada.



Funciones de ayuda de IOS (continuación)

- Verificación de la sintaxis de los comandos IOS:
 - El intérprete de la línea de comando comprueba el comando ingresado de izquierda a derecha para establecer qué acción se solicita.
 - Si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente.
 - Si el intérprete encuentra un error, el IOS, en general, proporciona comentarios como "comando ambiguo", "comando incompleto" o "comando incorrecto".



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.

Demostración en vídeo: Teclas de acceso rápido y métodos abreviados

La CLI de IOS admite los siguientes métodos abreviados:

- **Fecha hacia abajo:** permite al usuario desplazarse por el historial de comandos.
- **Flecha hacia arriba:** permite al usuario desplazarse hacia atrás a través de los comandos.
- **Tab:** completa el resto del comando ingresado 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-Shift-6:** permite que el usuario interrumpa un proceso IOS (p. ej., ping).

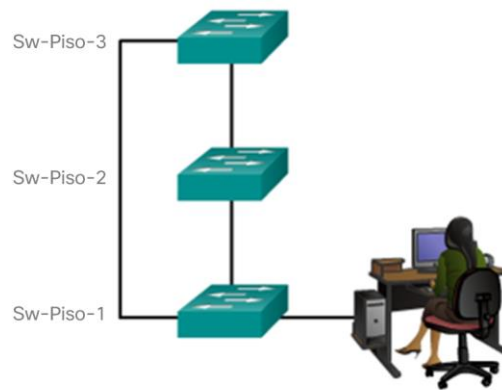


2.2 Configuración básica de dispositivos

Nombres de dispositivos

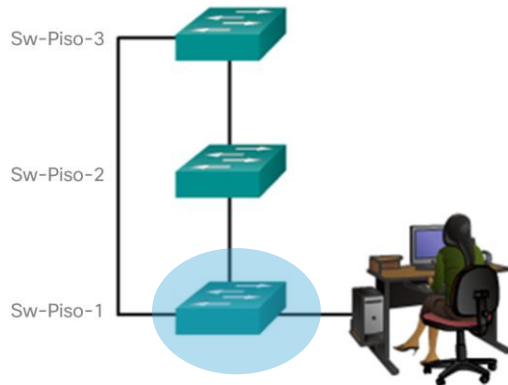
- El primer paso cuando se configura un switch es asignarle un nombre de dispositivo único o nombre de host.
- Los nombres de host aparecen en las peticiones de entrada de la CLI, pueden utilizarse en varios procesos de autenticación entre dispositivos y deben utilizarse en los diagramas de topologías.
- Sin nombre del host, es difícil identificar dispositivos de red para propósitos de configuración.

Los nombres de host permiten al administrador darle un nombre a un dispositivo, lo que facilita su identificación en una red.



Configuración de nombres del host

- Una vez que se ha identificado la convención de denominación, el próximo paso es aplicar los nombres a los dispositivos usando la CLI.
- El comando de configuración global *name* del **nombre de host** se utiliza para asignar un nombre.



```
Switch>  
Switch> enable  
Switch#  
Switch# configure terminal  
Switch(config)# hostname Sw-Floor-1  
Sw-Piso-1 (config) #
```

Limitación del acceso a los dispositivos

- **Paso 1:** Proteja los dispositivos de red para limitar físicamente su acceso; para ello, colóquelos en armarios de cableado y estantes bloqueados.
- **Paso 2:** Exija el uso de contraseñas seguras, dado que son la primera línea de defensa contra el acceso no autorizado a dispositivos de red.
- Limite el acceso administrativo de la siguiente manera.
- Utilice contraseñas fuertes de la manera recomendada.

Protección del 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

Otras tareas

- Encripte todas las contraseñas
- Proporcione notificación legal

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.

Para mayor comodidad, la mayor parte de las actividades de laboratorio y ejemplos en este curso usan las contraseñas simples pero débiles **cisco** o **class**.

Limitar el acceso a las configuraciones de dispositivos

Configuración de contraseñas

- Para proteger el acceso a EXEC con privilegios, utilice el comando de configuración global **enable secret password**.
- Para proteger el acceso a EXEC del usuario, configure la línea de consola de la siguiente manera:

Proteger el modo EXEC del usuario	Descripción
Switch(config)# line console 0	El comando ingresa el modo de configuración de la línea de consola
Switch(config-line)# contraseña contraseña	El comando especifica la contraseña de la línea de consola.
Switch(config-line)# login	El comando hace que el switch solicite la contraseña.

- Para proteger el acceso remoto a Telnet o SSH, configure la terminal virtual (VTY) de la siguiente manera:

Cómo proteger el acceso remoto	Descripción
Switch(config)# line vty 0 15	Los switches de Cisco en general admiten hasta 16 líneas VTY entrantes numeradas de 0 a 15.
Switch(config-line)# contraseña contraseña	El comando especifica la contraseña de la línea VTY.
Switch(config-line)# login	El comando hace que el switch solicite la contraseña.

Configuración de contraseñas (continuación)

Proteger EXEC con privilegios	<pre>Sw-Floor-1 (config) # enable secret class Sw-Floor-1 (config) # exit Sw-Floor-1 # Sw-Floor-1 # disable Sw-Floor-1 > enable Password: Sw-Floor-1 #</pre>
Proteger EXEC del usuario	<pre>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-Piso-1 (config) #</pre>
Cómo proteger el acceso remoto	<pre>Sw-Floor-1 (config) # line vty 0 15 Sw-Floor-1 (config-line) # password cisco Sw-Floor-1 (config-line) # login SW-Piso-1 (config-line) #</pre>

Cifrado de contraseñas

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

- Utilice el comando de global config **service password-encryption** para cifrar todas las contraseñas.
 - El comando aplica un cifrado débil a todas las contraseñas no cifradas.
 - Sin embargo, detiene "mirar por encima del hombro".

```
Sw-Floor-1(config)# service password-encryption
S1(config)# exit
S1# show running-config
<se omitió el resultado>
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
<Se omitieron resultados>
línea con 0

password 7 0822455D0A16
login
!
line vty 0 4

password 7 0822455D0A16
login
line vty 5 15

password 7 0822455D0A16
login!
```

Mensajes de aviso

- Los avisos son mensajes que se muestran cuando alguien intenta acceder a un dispositivo. Los avisos son una parte importante en un proceso legal en el caso de una demanda por el ingreso no autorizado a un dispositivo.
- Configurado mediante el comando **banner motd** *delimiter message delimiter* del modo de configuración global. El carácter delimitador puede ser cualquier carácter siempre que sea único y no aparezca en el mensaje (p. ej., # \$ % ^ & *).



Syntax Checker: Limitación del acceso a un switch

Cifre todas las contraseñas.

```
Sw-Floor-1(config)# service password-encryption  
Sw-Piso-1(config)#
```

Proteja el acceso a EXEC con privilegios con la contraseña Cla55.

```
Sw-Floor-1(config)# enable secret Cla55  
Sw-Piso-1(config)#
```

Proteja la línea de la consola. Utilice la contraseña Cisc0 y permita el inicio de sesión.

```
Sw-Floor-1(config)# line console 0  
Sw-Floor-1(config-line)# password Cisc0  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)# exit  
Sw-Piso-1(config)#
```

Proteja las primeras 16 líneas VTY. Utilice la contraseña Cisc0 y permita el inicio de sesión.

```
Sw-Floor-1(config)# line vty 0 15  
Sw-Floor-1(config-line)# password Cisc0  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)# end  
Sw-Floor-1#
```

Guardar el archivo de configuración en ejecución

- Los dispositivos Cisco usan un archivo de **configuración en ejecución** y un archivo de **configuración de inicio**.
- El archivo de configuración en ejecución se almacena en la RAM y contiene la configuración actual de un dispositivo Cisco IOS.
 - Los cambios de configuración se almacenan en este archivo.
 - Si se interrumpe la alimentación, se pierde la configuración en ejecución.
 - Utilice el comando **show startup-config** para mostrar el contenido.
- El archivo de configuración de inicio se almacena en la NVRAM y contiene la configuración que utilizará el dispositivo al reiniciar.
 - En general, la configuración en ejecución se guarda como la configuración de inicio.
 - Si se interrumpe la alimentación, no se pierde o borra.
 - Utilice el comando **show running-config** para mostrar el contenido.
- Utilice el comando **copy running-config startup-config** para guardar la nueva configuración en ejecución.



Modificación de la configuración en ejecución

- Si los cambios en la configuración no tienen el efecto deseado, pueden quitarse individualmente o el dispositivo puede reiniciarse a la última configuración guardada; para ello, utilice el comando del modo EXEC con privilegios **reload**.
 - El comando restaura 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 guardaron cambios no deseados en la configuración de inicio, es posible que deba borrar todas las configuraciones mediante el comando del modo EXEC con privilegios **erase startup-config**.



Guardar configuraciones

Captura de la configuración en un archivo de texto

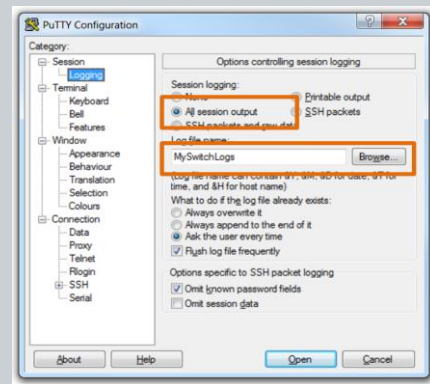
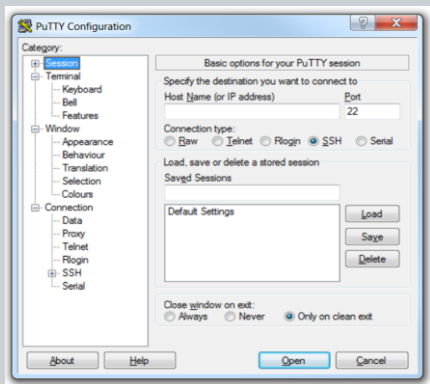
- Los archivos de configuración también pueden guardarse y archivar en un documento de texto para su posterior edición o reutilización. Por ejemplo, suponga que se configuró un switch y que se guardó la configuración en ejecución.

Conéctese al switch mediante PuTTY o Tera Term.

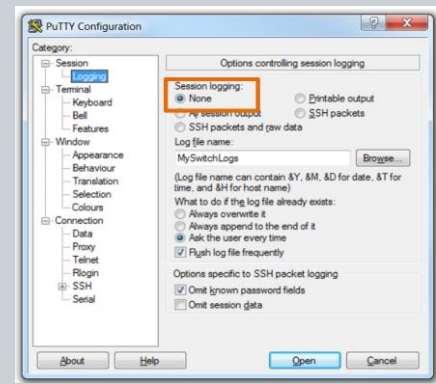
Habilite el inicio de sesión y asigne un nombre y ubicación de archivo donde guardar el archivo de registro.

Genere el texto que se capturará dado que 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; para ello, seleccione **None** (Ninguno) en la opción de inicio de sesión.



Ejecute el comando **show running-config** o **show startup-config** ante la petición de entrada de EXEC con privilegios.



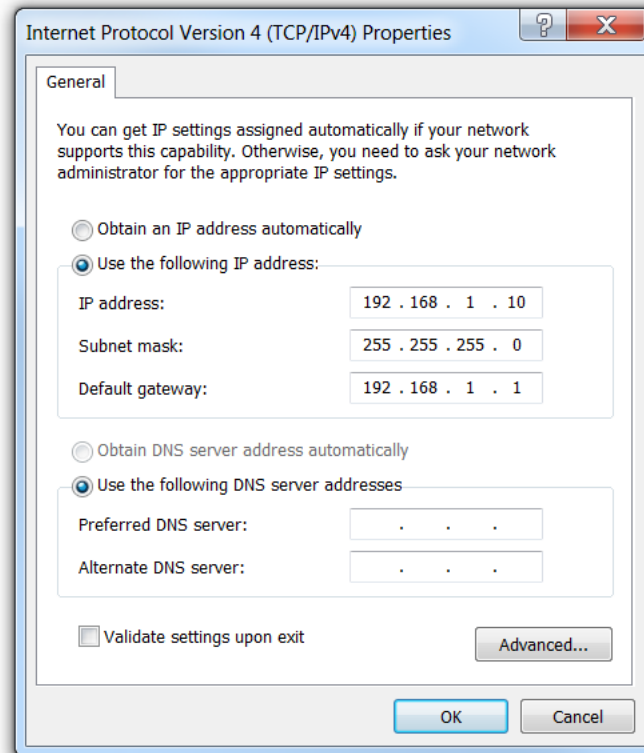
Captura de la configuración en un archivo de texto (continuación)

- El archivo de texto creado se puede utilizar como registro de cómo se implementa actualmente el dispositivo y puede utilizarse para restaurar la configuración. El archivo requerirá 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.

2.3 Esquemas de direcciones

Descripción general de direcciones IP

- Cada terminal de una red (p. ej., PC, computadoras portátiles, servidores, impresoras, teléfonos VoIP, cámaras de seguridad) requieren una configuración IP que conste de lo siguiente:
 - **IP Address (Dirección IP)**
 - **Máscara de subred**
 - **Gateway predeterminado** (opcional para algunos dispositivos)
- Las direcciones IPv4 se muestran en formato decimal punteado que consta de lo siguiente:
 - 4 números decimales 0 y 255
 - Separados por puntos decimales
 - P. ej., 192.168.1.10, 255.255.255.0, 192.168.1.1



Interfaces y puertos

- Los switches de la capa 2 de Cisco IOS cuentan con puertos físicos para conectar dispositivos. Sin embargo, estos puertos no son compatibles con las direcciones IP de la capa 3.
- Para conectarse en forma remota y administrar el switch de capa 2, debe configurarse con una interfaz virtual de switch (SVI) o más.
- Cada switch cuenta con una SVI de VLAN 1 predeterminada.

Nota: Un switch de capa 2 no necesita una dirección IP para funcionar. La dirección IP de la SVI solo se utiliza para la administración remota del switch.

Configurar direccionamiento IP

Configuración manual de direcciones IP para terminales

- Para configurar manualmente una dirección IP en un host de Windows:

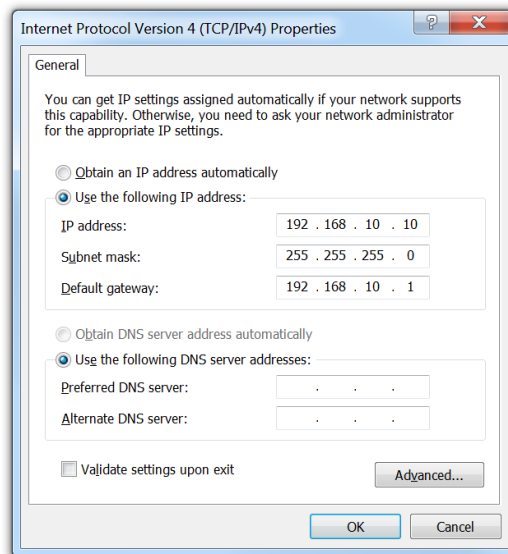
Abra el **Control Panel (Panel de control)** > **Network Sharing Center (Centro de compartición de redes)** > **Change adapter settings (Configuración del adaptador de cambios)** y haga clic en el adaptador.

Configure la información de la dirección IPv4, la máscara de subred y el gateway predeterminado, y luego haga clic en **OK (Aceptar)**.

Haga clic con el botón derecho en el adaptador y seleccione **Properties (Propiedades)** para mostrar la ventana Local Area Connection Properties (Propiedades de conexión de área local).

Resalte el protocolo de Internet versión 4 (TCP/IPv4) y haga clic en **Properties (Propiedades)** para abrir la ventana Protocol Version 4 (TCP/IPv4) Properties (Propiedades del protocolo de Internet versión 4 [TCP/IPv4]).

Haga clic en **Use the following IP address (Utilizar la dirección IP)** para configurar manualmente la configuración de la dirección IPv4.



Nota: La configuración manual de IPv4 de Windows 10 se proporciona como material suplementario al final de esta presentación.

Configuración automática de direcciones IP para terminales

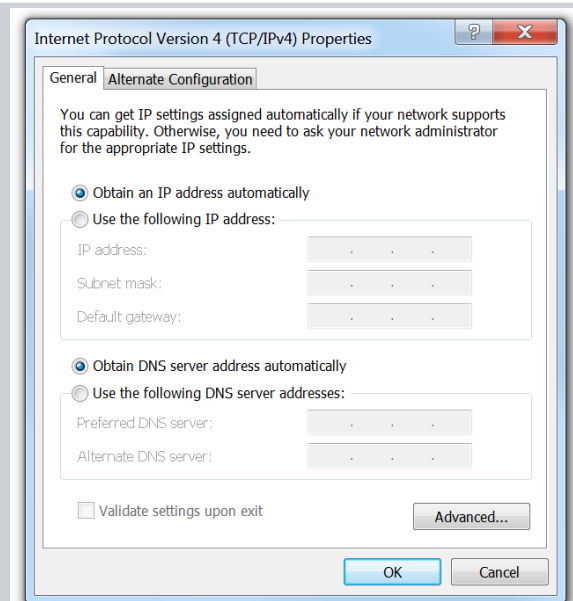
- Para asignar la configuración IP mediante el protocolo de configuración dinámica de host (DHCP):

Abra el **Control Panel (Panel de control) > Network Sharing Center (Centro de compartición de redes) > Change adapter settings (Configuración del adaptador de cambios)** y haga clic en el adaptador.

Haga clic en **Obtain an IP address automatically (Obtener una dirección IP automáticamente)** y haga clic en **OK (Aceptar)**.

Haga clic con el botón derecho en el adaptador y seleccione **Properties (Propiedades)** para mostrar la ventana Local Area Connection Properties (Propiedades de conexión de área local).

Resalte el protocolo de Internet versión 4 (TCP/IPv4) y haga clic en **Properties (Propiedades)** para abrir la ventana Protocol Version 4 (TCP/IPv4) Properties (Propiedades del protocolo de Internet versión 4 [TCP/IPv4]).



Interfaz virtual de switch

- Para administrar de forma remota un switch, también debe configurarse con una configuración IP:
 - Sin embargo, el switch no cuenta con una interfaz física de Ethernet que pueda configurarse.
 - En su lugar, debe configurar la **interfaz virtual de switch (SVI)** de VLAN 1.
- La SVI de VLAN 1 debe configurarse con lo siguiente:
 - **Dirección IP:** identifica únicamente al switch en la red.
 - **Máscara de subred:** identifica la porción de red y del host de la dirección IP.
 - **Enabled:** con el comando **no shutdown**.



Utilice el comando EXEC con privilegios **show ip interface brief** para verificar.

Verificación del direccionamiento de la interfaz

- Se verifica la configuración de IP en un host de Windows mediante el comando **ipconfig**.
- Para verificar los ajustes de las direcciones y las interfaces de dispositivos intermedios como switches y routers, utilice el comando EXEC con privilegios **show ip interface brief**.




Verificar conectividad

Prueba de conectividad integral

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

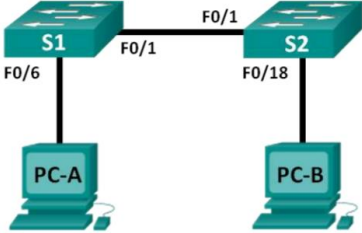


Práctica de laboratorio: Creación de una red simple

Cisco Networking Academy®Mind Wide Open™

Lab - Building a Simple Network

Topology



```
graph TD; S1[S1] --- F0/1 --- S2[S2]; S1 --- F0/6 --- PC-A[PC-A]; S2 --- F0/18 --- PC-B[PC-B];
```

Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

- Part 1: Set Up the Network Topology (Ethernet only)
- Part 2: Configure PC Hosts
- Part 3: Configure and Verify Basic Switch Settings

Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

2.4 Resumen del capítulo

Conclusión

Actividad de clase: Enséñeme

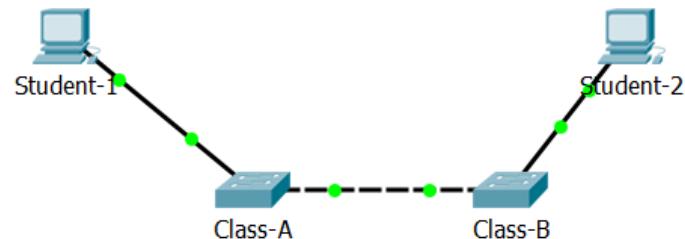


Packet Tracer: Desafío de integración de habilidades

Packet Tracer - Skills Integration Challenge

Addressing Table

Device	Interface	IP Address	Subnet Mask
	VLAN 1		255.255.255.0
	VLAN 1		255.255.255.0
	NIC		255.255.255.0
	NIC		255.255.255.0



Objectives

- Configure hostnames and IP addresses on two Cisco Internetwork Operating System (IOS) switches using the command-line interface (CLI).
- Use Cisco IOS commands to specify or limit access to the device configurations.
- Use IOS commands to save the running configuration.
- Configure two host devices with IP addresses.
- Verify connectivity between the two PC end devices.

Scenario

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

Capítulo 2: Configuración de un sistema operativo de red

- Explicar las características y funciones del software Cisco IOS.
- Configurar los parámetros iniciales en un dispositivo de red que utiliza el software Cisco IOS.
- Dado un esquema de asignación de direcciones IP, configurar los parámetros IP en las terminales para proporcionar conectividad completa en una red de pequeña o mediana empresa.

