



Materiales para el instructor Capítulo 5: Configuración de un switch



CCNA Routing and Switching Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™



Materiales del instructor: Guía de planificación del capítulo 5

Esta presentación en PowerPoint se divide en dos partes:

1. Guía de planificación para el instructor
 - Información para ayudarlo a familiarizarse con el capítulo
 - Ayuda a la enseñanza
2. Presentación de la clase del instructor
 - Diapositivas opcionales que puede utilizar en el aula
 - Comienza en la diapositiva n.º 11

Nota: Elimine la Guía de planificación de esta presentación antes de compartirla con otras personas.



Routing and Switching Essentials 6.0

Guía de planificación

Capítulo 5: Configuración de un switch



Cisco | Networking Academy®
Mind Wide Open™



Capítulo 5: Actividades

¿Qué actividades se relacionan con este capítulo?

N.º de página	Tipo de actividad	Nombre de la actividad	¿Opcional?
5.0.1.2	Actividad de clase	Todos de pie	Opcional
5.1.1.6	Práctica de laboratorio	Configuración básica del switch	Recomendado
5.1.2.2	Verificador de sintaxis	Configuración de puertos de switch en la capa física	Recomendado
5.1.2.3	Verificador de sintaxis	Habilitación de auto-MDIX	Recomendado
5.2.1.4	Packet Tracer	Configuración de SSH	Recomendado
5.2.2.8	Packet Tracer	Configuración de seguridad de puertos de switch	Recomendado
5.2.2.9	Packet Tracer	Resolución de problemas de seguridad de puertos de switch	Recomendado
5.2.2.10	Práctica de laboratorio	Configuración de características de seguridad de switch	Opcional
5.3.1.1	Actividad de clase	Trío de switches	Opcional
5.3.1.2	Packet Tracer	Desafío de integración de habilidades	Recomendado

La contraseña utilizada en las actividades de Packet Tracer en este capítulo es: **PT_ccna5**



Capítulo 5: Evaluación

- Los estudiantes deben completar el capítulo 5 "Evaluación" después de completar el capítulo 5.
- Los cuestionarios, las prácticas de laboratorio, los Packet Tracers y otras actividades se pueden utilizar para evaluar informalmente el progreso de los estudiantes.



Capítulo 5: Prácticas recomendadas

Antes de enseñar el capítulo 5, el instructor debe:

- Completar el capítulo 5: "Evaluación".
- Los objetivos de este capítulo son:
 - Configurar los parámetros iniciales en un switch Cisco.
 - Configurar los puertos de un switch para cumplir con los requisitos de red.
 - Configurar la interfaz virtual de administración en un switch.
 - Configurar la característica de seguridad de puertos para restringir el acceso a la red.



Capítulo 5: Prácticas recomendadas (cont.)

Sección 5.1

- Demuestre la secuencia de arranque de un switch.
- Cargue IOS 12 y 15 en un switch y edite la variable de entorno BOOT para cargar de IOS 12 a IOS 15. Demuestre los resultados del comando.
- Analice el propósito de los archivos en `dir flash:`
- Proporcione acceso a switches 2960 para que los estudiantes pueden practicar con el botón Mode (Modo) y los indicadores LED.
- Demuestre cómo se agrega un cable de consola y cómo se configura un switch en Packet Tracer.



Capítulo 5: Prácticas recomendadas (cont.)

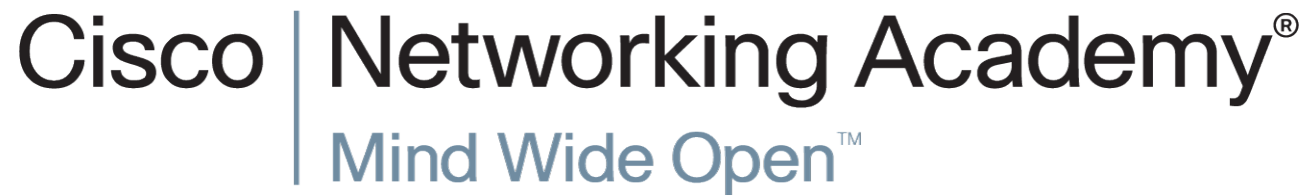
Sección 5.2

- Demuestre la comparación entre Telnet y SSH con Wireshark.
- Cree varias tipologías de Packet Tracer con fines demostración.
- Demuestre las características de seguridad de puertos y modos de infracción mediante Packet Tracer.
- Recomendación: Los estudiantes deben registrar notas sobre los "comandos show" y los resultados.



Capítulo 5: Ayuda adicional

- Para obtener ayuda adicional sobre las estrategias de enseñanza, incluidos los planes de lección, las analogías para los conceptos difíciles y los temas de debate, visite la Comunidad CCNA en <https://www.netacad.com/group/communities/community-home>.
- Prácticas recomendadas de todo el mundo para enseñar CCNA Routing and Switching.
<https://www.netacad.com/group/communities/ccna-blog>
- Si tiene planes o recursos de lección que desee compartir, súbalos a la Comunidad CCNA, a fin de ayudar a otros instructores.
- Los estudiantes pueden inscribirse en **Packet Tracer Know How 1: Packet Tracer 101** (autoinscripción)





Capítulo 5: Configuración de un switch



Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™



Capítulo 5: Secciones y objetivos

5.1 Configuración básica de un switch

- Configurar los parámetros iniciales en un switch Cisco.
- Configurar los puertos de un switch para cumplir con los requisitos de red.

5.2 Seguridad de switches: Administración e implementación

- Configurar la interfaz virtual de administración en un switch.
- Configurar la característica de seguridad de puertos para restringir el acceso a la red.



5.1 Configuración básica de un switch



Cisco | Networking Academy®
Mind Wide Open™



Configurar un switch con parámetros iniciales

Secuencia de arranque de un switch

1. Prueba de autodiagnóstico al encender (POST).
2. Se ejecuta el software del cargador de arranque.
3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel.
4. El cargador de arranque inicializa el sistema de archivos flash.
5. El cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.



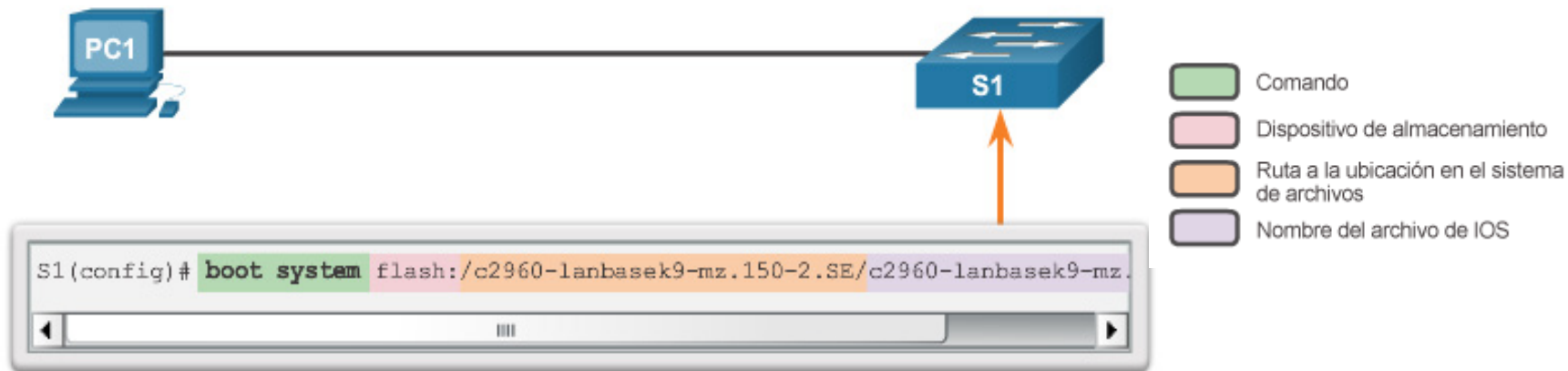
Configurar un switch con parámetros iniciales

Secuencia de arranque de un switch (continuación)

Para encontrar una imagen del Cisco IOS adecuada, el switch realiza los siguientes pasos:

- Paso 1.** Intenta arrancar automáticamente con la información de la variable de entorno BOOT.
- Paso 2.** Si esta variable no está establecida, el switch realiza una búsqueda integral en todo el sistema de archivos flash. Si puede, el switch carga y ejecuta el primer archivo ejecutable.
- Paso 3.** A continuación, el sistema operativo IOS inicializa las interfaces mediante los comandos de Cisco IOS que se encuentran en el archivo de configuración y en la configuración de arranque, almacenados en la memoria NVRAM.

Nota: El comando **boot system** se puede utilizar para establecer la variable de entorno BOOT. Use el comando **show boot** para ver la configuración actual del archivo de arranque de IOS.





Configurar un switch con parámetros iniciales

Recuperación tras un bloqueo del sistema

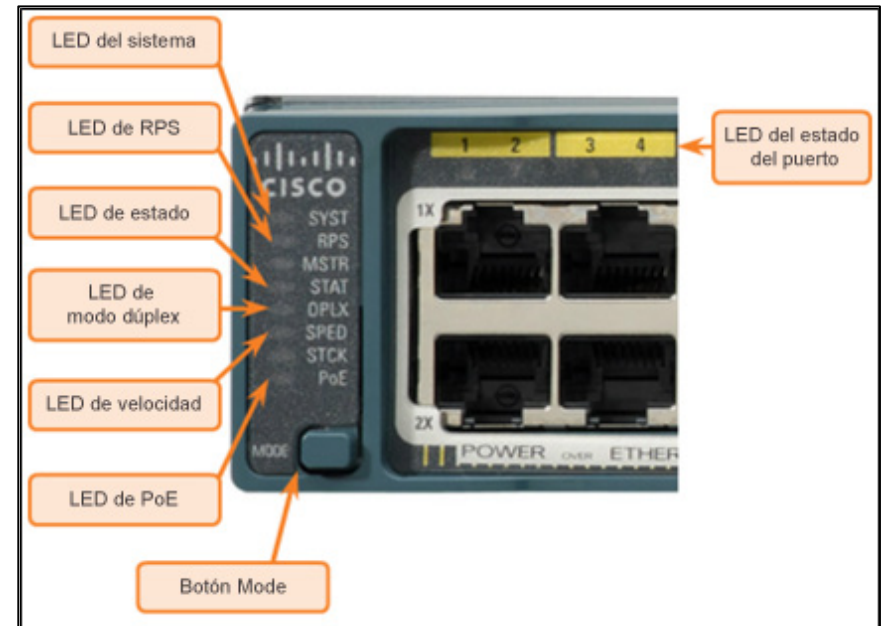
- El cargador de arranque también se puede utilizar para administrar el switch si el IOS no se puede cargar.
- Se puede acceder al cargador de arranque mediante una conexión de consola con los siguientes pasos:
 1. Conecte una PC al puerto de consola del switch con un cable de consola. Desconecte el cable de alimentación del switch.
 2. Vuelva a conectar el cable de alimentación al switch y mantenga presionado el botón Mode (Modo).
 3. El LED del sistema emite brevemente una luz color ámbar y después verde sólido. Suelte el botón Mode.
- Aparece la petición **switch:** del cargador de arranque en el software de emulación de terminales en la PC.



Configurar un switch con parámetros iniciales

Indicadores LED de un switch

- Cada puerto en los switches Cisco Catalyst tiene indicadores luminosos LED de estado.
- Estos LED reflejan la actividad de los puertos de manera predeterminada, pero también pueden proporcionar otra información sobre el switch mediante el botón Mode.
- Los siguientes modos están disponibles en los switches Cisco Catalyst 2960:
 - LED del sistema
 - LED del sistema de alimentación redundante (RPS)
 - LED de estado del puerto
 - LED de modo dúplex del puerto
 - LED de velocidad del puerto
 - LED de modo de alimentación por Ethernet





Configurar un switch con parámetros iniciales

Preparación para la administración básica de un switch

Para administrar un switch Cisco en forma remota, se lo debe configurar para que acceda a la red.

- Para conectar una PC al puerto de consola de un switch para su configuración, se utiliza un cable de consola.
- La información de IP (dirección, máscara de subred, gateway) se debe asignar a una interfaz virtual de switch (SVI).
- Si el switch se administra desde una red remota, también se debe configurar un gateway predeterminado.
- Si bien esta configuración de IP permite la administración remota y el acceso remoto al switch, no permite que el switch enrute paquetes de capa 3.



Configurar un switch con parámetros iniciales

Configurar el acceso a la administración de un switch

Configurar interfaz de administracion de switch

Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface vlan 99
Configura la dirección IP de la interfaz de administración.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Habilita la interfaz de administración.	S1(config-if)# no shutdown
Vuelva al modo EXEC privilegiado.	S1(config-if)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

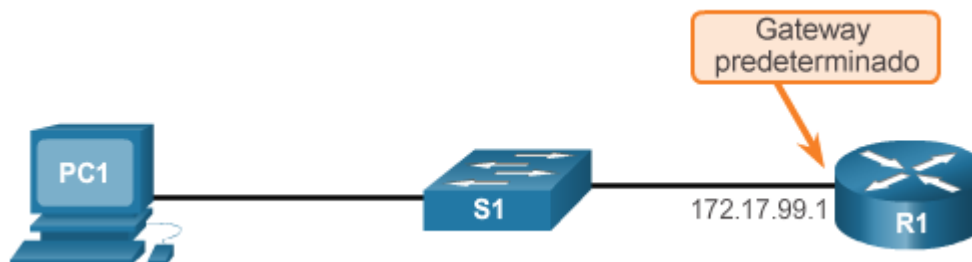


Configurar un switch con parámetros iniciales

Configurar el acceso a la administración de un switch (continuación)

Configuración del gateway predeterminado de un switch

Comandos de IOS de un switch Cisco	
Ingresa al modo de configuración global.	<code>S1# configure terminal</code>
Configure el gateway predeterminado para el switch.	<code>S1(config)# ip default-gateway 172.17.99.1</code>
Vuelva al modo EXEC privilegiado.	<code>S1(config)# end</code>
Guarda la configuración en ejecución en la configuración de inicio.	<code>S1# copy running-config startup-config</code>

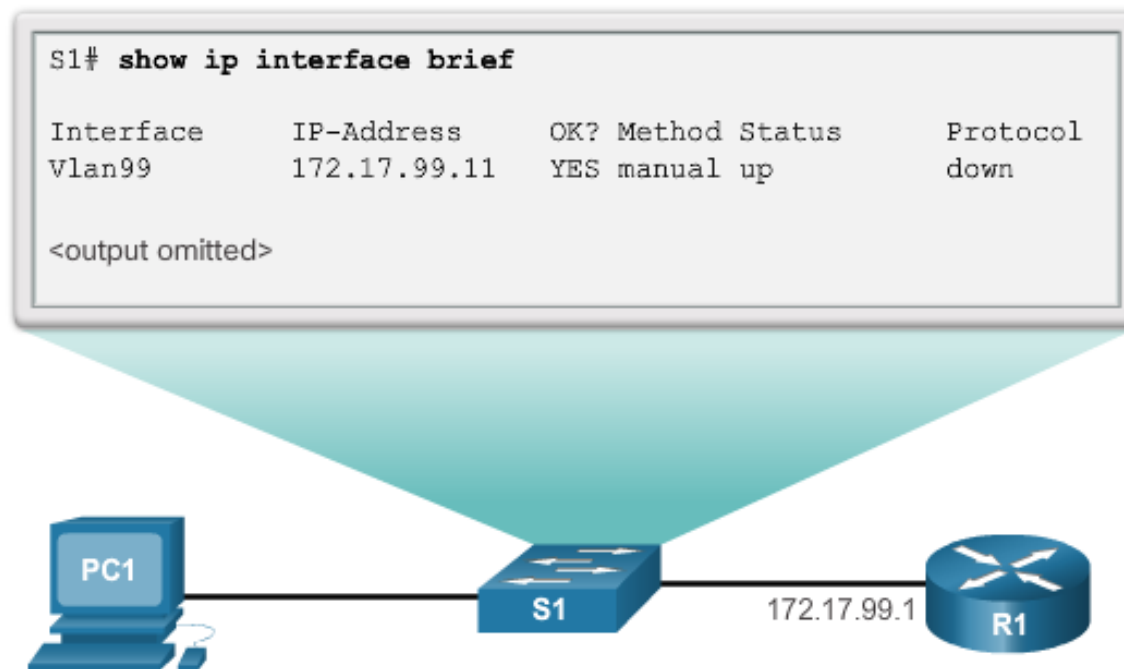




Configurar un switch con parámetros iniciales

Configurar el acceso a la administración de un switch (continuación)

Verificación de la configuración de la interfaz de administración de un switch

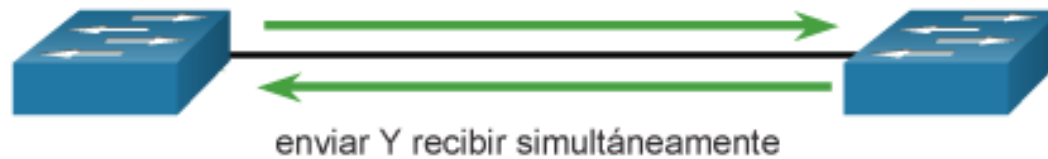




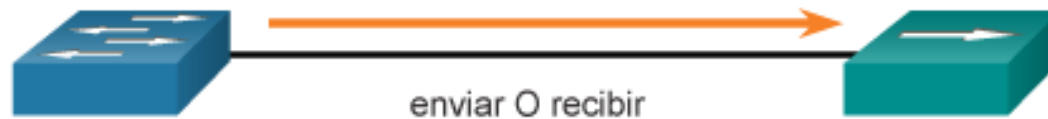
Configurar los puertos de un switch

Comunicación en dúplex

Comunicación dúplex completo



Comunicación dúplex medio





Configurar los puertos de un switch

Configurar los puertos de un switch en la capa física

Configurar dúplex y velocidad



Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	<code>S1# configure terminal</code>
Ingrese el modo de configuración de interfaz.	<code>S1(config)# interface FastEthernet 0/1</code>
Configura el modo dúplex de la interfaz.	<code>S1(config-if)# duplex full</code>
Configura la velocidad de la interfaz	<code>S1(config-if)# speed 100</code>
Vuelva al modo EXEC privilegiado.	<code>S1(config-if)# end</code>
Guarda la configuración en ejecución en la configuración de inicio.	<code>S1# copy running-config startup-config</code>



Configurar los puertos de un switch

Auto-MDIX

- Antes se requerían determinados tipos de cable (cruzados o directos) para conectar dispositivos.
- La característica de interfaz cruzada automática dependiente del medio (auto-MDIX) elimina este problema.
- Cuando se habilita auto-MDIX, la interfaz detecta automáticamente la conexión y la configura como corresponde.
- Cuando se usa auto-MDIX en una interfaz, la velocidad y el modo dúplex de la interfaz se deben establecer en automático.



Configurar los puertos de un switch Auto-MDIX (continuación)

Configuración de auto-MDIX



Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	<code>S1# configure terminal</code>
Ingrese al modo de configuración de interfaz.	<code>S1(config)# interface fastethernet 0/1</code>
Configura la interfaz para autonegociar la comunicación dúplex con el dispositivo conectado.	<code>S1(config-if)# duplex auto</code>
Configura la interfaz para negociar automáticamente la velocidad con el dispositivo conectado.	<code>S1(config-if)# speed auto</code>
Habilita auto-MDIX en la interfaz.	<code>S1(config-if)# mdix auto</code>
Vuelva al modo EXEC privilegiado.	<code>S1(config-if)# end</code>
Guarda la configuración en ejecución en la configuración de inicio.	<code>S1# copy running-config startup-config</code>



Configurar los puertos de un switch

Auto-MDIX (continuación)

Verificación de auto-MDIX



```

S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
  Auto-MDIX      : On   [AdminState=1   Flags=0x00056248]
S1#

```



Configurar los puertos de un switch

Verificar la configuración de los puertos de un switch

Comandos de verificación

Comandos de IOS de un switch Cisco	
Muestra el estado y la configuración de la interfaz.	S1# show interfaces [<i>interface-id</i>]
Muestra la configuración de inicio actual.	S1# show startup-config
Muestra la configuración de funcionamiento actual.	S1# show running-config
Muestra información sobre el sistema de archivos flash.	S1# show flash
Muestra el estado del hardware y el software del sistema.	S1# show version
Muestra el historial de comandos introducidos.	S1# show history
Muestra información de IP de una interfaz.	S1# show ip [<i>interface-id</i>]
Muestra la tabla de direcciones MAC.	S1# show mac-address-table O S1# show mac address-table



Configurar los puertos de un switch

Problema en la capa de acceso a la red

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<output omitted>
```



Configurar los puertos de un switch

Problema en la capa de acceso a la red (continuación)

Problemas de la capa de acceso a la red

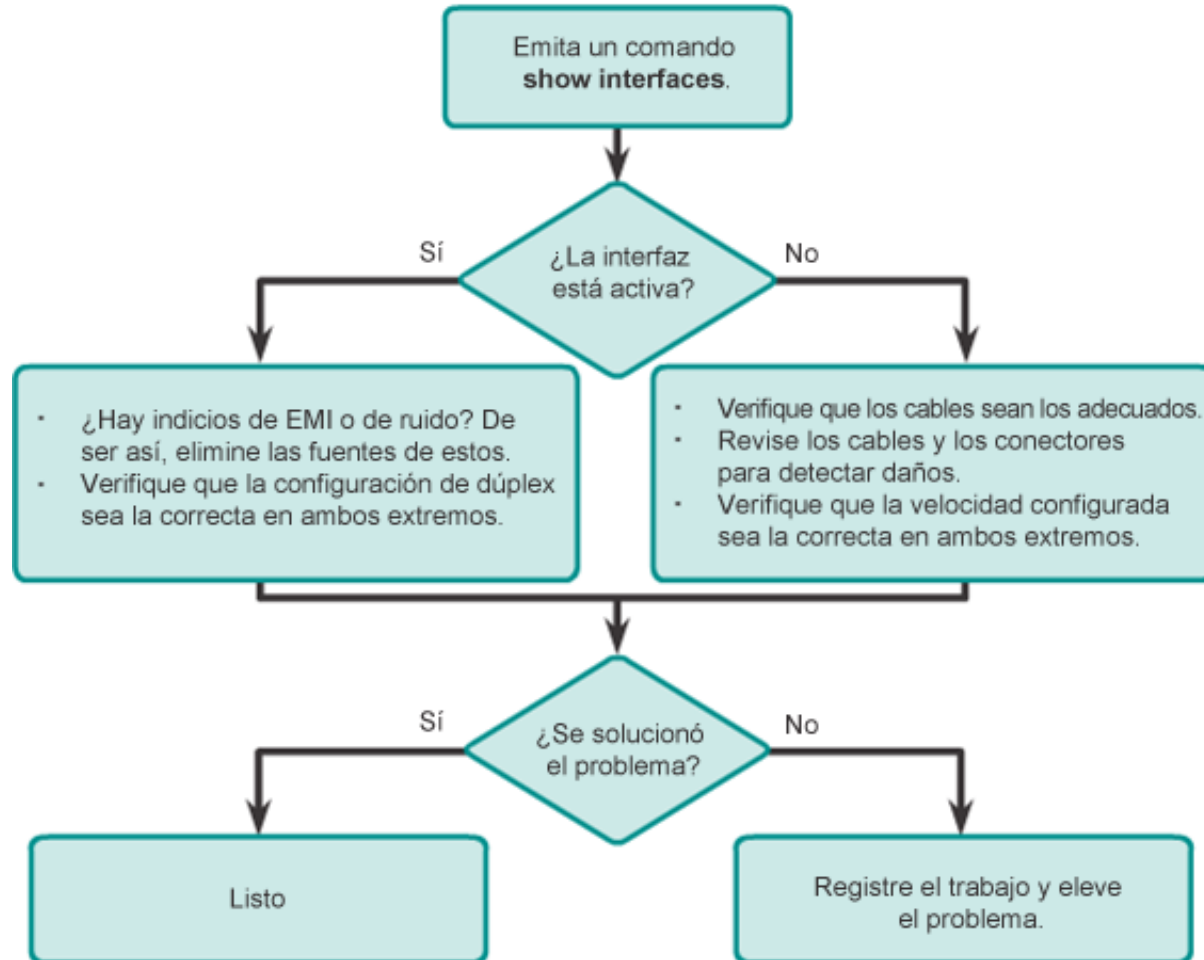
Tipo de error	Descripción
Errores de entrada	Cantidad total de errores. Incluye los recuentos de fragmentos de colisión, de fragmentos gigantes, de los que no están almacenados en buffer, de CRC, de tramas, de saturación y de ignorados.
Fragmentos de colisión	Paquetes que se descartan porque son más pequeños que el tamaño mínimo de paquete para el medio. Por ejemplo, cualquier paquete Ethernet de menos de 64 bits se considera insignificante.
Gigantes	Paquetes que se descartan porque son más grandes que el tamaño mayor de paquete para el medio. Por ejemplo, cualquier paquete Ethernet que supere los 1518 bits se considera un gigante.
CRC	Se generan errores de CRC cuando el checksum calculado no es igual al checksum recibido.
Errores de salida	La suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza.
Colisiones	Cantidad de mensajes retransmitidos debido a una colisión de Ethernet.
Colisiones tardías	Una colisión que ocurre después de que se transmitieron 512 bits de la trama.



Configurar los puertos de un switch

Solucionar problema en la capa de acceso a la red

Resolución de problemas de los medios del switch





5.2 Seguridad de switches: Administración e implementación



Cisco | Networking Academy®
Mind Wide Open™



Acceso remoto seguro

Funcionamiento de SSH

- Shell seguro (SSH) es un protocolo que proporciona una conexión segura (cifrada) a un dispositivo remoto basada en la línea de comandos.
- SSH debería reemplazar a Telnet para las conexiones de administración, debido a sus sólidas características de cifrado.
- SSH utiliza el puerto TCP 22 de manera predeterminada.
- Telnet utiliza el puerto TCP 23.
- Para habilitar SSH en switches Catalyst 2960, se requiere una versión del software de IOS que incluya características y capacidades criptográficas (cifradas).

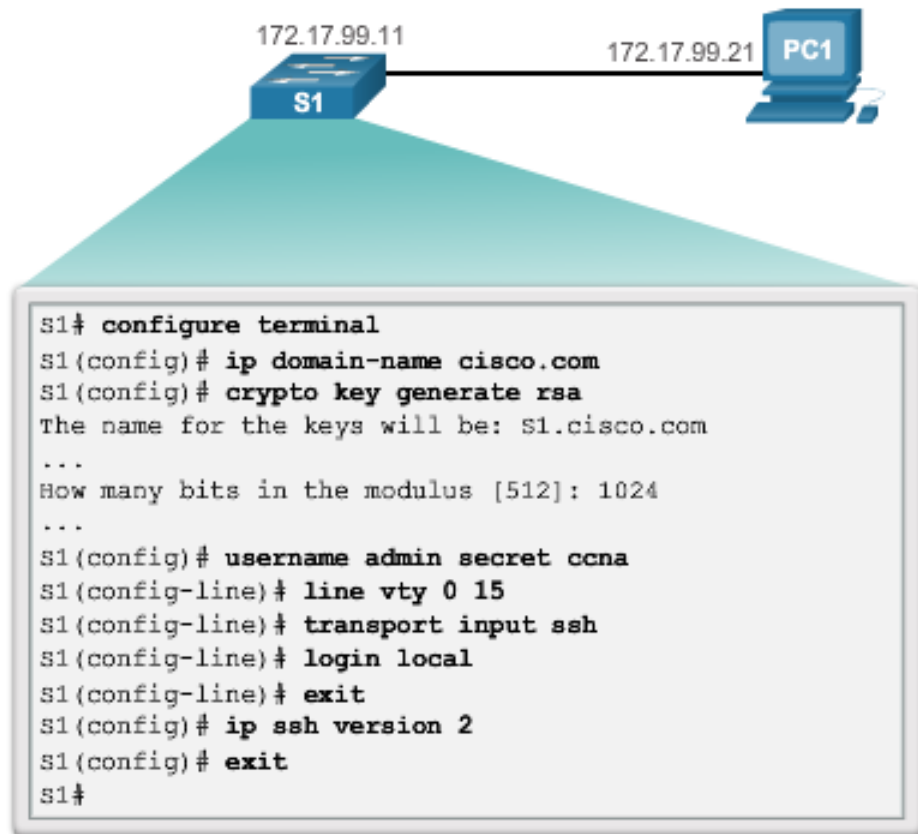


Acceso remoto seguro

Configuración de SSH

Configuración de SSH para la administración remota

1. **Verificar la compatibilidad con SHH: `show ip ssh`.**
2. **Configurar el dominio IP**
3. **Generar pares de claves RSA**
4. **Configurar la autenticación de usuario**
5. **Configurar las líneas vty**
6. **Habilitar la versión 2 de SSH.**

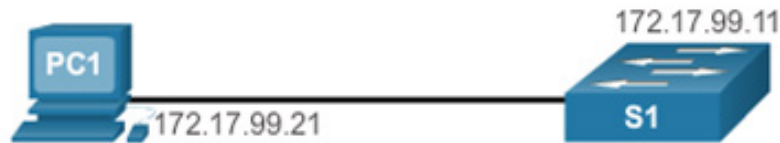




Acceso remoto seguro

Verificación de SSH

Conexión de SSH para la administración remota



```

172.17.99.11 - PuTTY
Login as: admin
Using keyboard-interactive
authentication.
Password:

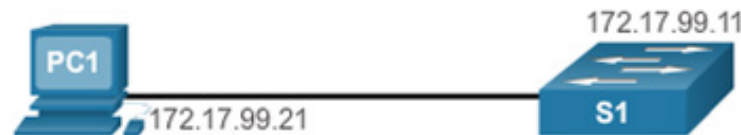
S1>enable
Password:
S1#
  
```



Acceso remoto seguro

Verificación de SSH (continuación)

Verificación del estado y la configuración de SSH



```

S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVN1QhI8GUOViuKNqVMOMtLg8Ud4qAilbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-sha1 Session started admin
0 2.0 OUT aes256-cbc hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
  
```



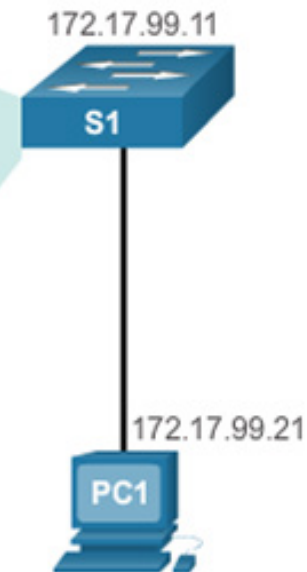
Seguridad de los puertos de un switch

Seguridad de los puertos sin utilizar

Deshabilitar puertos en desuso

Inhabilite los puertos sin utilizar con el comando **shutdown**.

```
S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 description web server
!
interface FastEthernet0/7
 shutdown
!
...
```





Seguridad de los puertos de un switch

Seguridad de puertos: Funcionamiento

- Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.
- Cualquier intento adicional de conexión por parte de direcciones MAC desconocidas generará una violación de seguridad.
- Las direcciones MAC seguras se pueden configurar de varias maneras:
 - Direcciones MAC seguras estáticas: se configuran manualmente y se agregan a la configuración en ejecución (**switchport port-security mac-address *dirección-mac***)
 - Direcciones MAC seguras dinámicas: se eliminan al reiniciarse el switch
 - Direcciones MAC seguras persistentes: se agregan a la configuración en ejecución y se obtienen en forma dinámica (comando del modo de configuración de interfaces **switchport port-security mac-address sticky**)



Seguridad de los puertos de un switch

Seguridad de puertos: Modos de violación de seguridad

- IOS considera que hay una violación de seguridad cuando:
 - Se agregó la cantidad máxima de direcciones MAC seguras a la tabla CAM para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.
- Cuando se detecta una violación, hay tres acciones posibles que se pueden realizar:
 - Proteger: no se recibe ninguna notificación
 - Restringir: se recibe una notificación sobre una violación de seguridad
 - Apagar
 - Comando del modo de configuración de interfaces `switchport port-security violation {protect | restrict | shutdown}`



Seguridad de los puertos de un switch

Seguridad de puertos: Modos de violación de seguridad (continuación)

Los modos de violación de seguridad incluyen los siguientes: Protect, Restrict y Shutdown.

Modos de violación de seguridad					
Modo de violación	Envía tráfico	Envía mensaje de syslog	Muestra mensaje de error	Incrementa el contador de violaciones	Desactiva el puerto
Proteger	No	No	No	No	No
Restringir	No	Sí	No	Sí	No
Apagar	No	No	No	Sí	Sí



Seguridad de los puertos de un switch

Seguridad de puertos: Configuración

Opciones predeterminadas de seguridad de puerto

Característica	Configuración predeterminada
Seguridad del puerto	Inhabilitada en un puerto.
Número máximo de direcciones MAC seguras	1
Modo de violación	Shutdown. El puerto se desactiva cuando se supera la cantidad máxima de direcciones MAC seguras.
Aprendizaje de direcciones sin modificación	Deshabilitado

Configurar la seguridad de los puertos dinámicos



Comandos de CLI de Cisco IOS

Especifica la interfaz que se debe configurar para la seguridad de puertos.	<code>S1(config)# interface fastethernet 0/18</code>
Establezca el modo de interfaz en acceso.	<code>S1(config-if)# switchport mode access</code>
Establezca la seguridad de puerto en la interfaz.	<code>S1(config-if)# switchport port-security</code>

Configurar la seguridad de puerto sin modificación



Comandos de CLI de Cisco IOS

Especifica la interfaz que se debe configurar para la seguridad de puertos.	<code>S1(config)# interface fastethernet 0/19</code>
Establezca el modo de interfaz en acceso.	<code>S1(config-if)# switchport mode access</code>
Establezca la seguridad de puerto en la interfaz.	<code>S1(config-if)# switchport port-security</code>
Establece la cantidad máxima de direcciones seguras permitidas en el puerto.	<code>S1(config-if)# switchport port-security maximum 10</code>
Habilita el aprendizaje por persistencia.	<code>S1(config-if)# switchport port-security mac-address sticky</code>



Seguridad de los puertos de un switch

Seguridad de puertos: Verificación

Verificación de dirección MAC: configuración dinámica

```
S1# show port-security interface fastethernet 0/18
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0025.83e6.4b01:1
Security Violation Count : 0
```

Verificación de dirección MAC: configuración persistente

```
S1# show port-security interface fastethernet 0/19
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 10
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```



Seguridad de los puertos de un switch

Seguridad de puertos: Verificación (continuación)

Verificación de MAC persistente: configuración en ejecución

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
```

Verificar las direcciones MAC seguras

```
S1# show port-security address
```

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0025.83e6.4b01	SecureDynamic	Fa0/18	-
1	0025.83e6.4b02	SecureSticky	Fa0/19	-



Seguridad de los puertos de un switch

Puertos en estado deshabilitado por errores

- Una violación de seguridad de puertos puede dejar a un switch en estado deshabilitado por errores.
- Un puerto en estado deshabilitado por errores se apaga por completo.
- El switch comunica estos eventos por medio de mensajes de consola.

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```



Seguridad de los puertos de un switch

Puertos en estado deshabilitado por errores (continuación)

Estado del puerto

```
S1# show interface fa0/18 status
Port Name      Status      Vlan Duplex  Speed  Type
Fa0/18         err-disabled 1    auto   auto   10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security      : Enabled
Port Status        : Secure-shutdown
Violation Mode     : Shutdown
Aging Time         : 0 mins
Aging Type         : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 000c.292b.4c75:1
Security Violation Count : 1
```

El comando **show interface** también indica si hay un puerto de switch en estado deshabilitado por errores.

Se debe emitir un comando de configuración de interfaces **shutdown** o **no shutdown** para volver a habilitar el puerto.

Cómo volver a habilitar un puerto inhabilitado por errores

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```



5.3 Resumen del capítulo



Cisco | Networking Academy®
Mind Wide Open™



Resumen del capítulo

Resumen

- Secuencia de arranque de un switches LAN Cisco.
- Modos LED de un switch LAN Cisco.
- Cómo acceder a un switch LAN Cisco y administrarlo de forma remota a través de una conexión segura.
- Modos dúplex en los puertos de un switch LAN Cisco.
- Seguridad de los puertos de un switch LAN Cisco, modos de violación de seguridad y acciones.
- Prácticas recomendadas para redes conmutadas.



Resumen del capítulo

Resumen

- Cuando se enciende un switch LAN Cisco por primera vez, realiza la siguiente secuencia de arranque:
 1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.
 2. A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.
 3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.
 4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.
 5. Por último, el cargador de arranque localiza y carga una imagen de software del sistema operativo de IOS en la memoria y delega el control del switch a IOS.
- Si faltan los archivos de Cisco IOS o estos están dañados, se puede usar el programa del cargador de arranque para volver a cargarlo o para recuperarse del problema.
- Una serie de LED en el panel frontal muestra el estado de funcionamiento del switch. Estos LED indican, por ejemplo, el estado de los puertos, el modo dúplex y la velocidad.



Resumen del capítulo

Resumen

- Se configura una dirección IP en la SVI de la VLAN de administración para permitir la configuración remota del dispositivo. Se debe configurar un gateway predeterminado que pertenezca a la red VLAN de administración en el switch mediante el comando **ip default-gateway**. Si el gateway predeterminado no se configura correctamente, no es posible la administración remota.
- Se recomienda usar Shell seguro (SSH) para proporcionar una conexión de administración segura (cifrada) a un dispositivo remoto, a fin de evitar la detección de nombres de usuario y contraseñas sin cifrar, lo cual es posible cuando se usan protocolos como Telnet.
- Una de las ventajas de los switches es que permiten la comunicación en dúplex completo entre los dispositivos, lo que duplica la velocidad de comunicación de forma eficaz. Si bien es posible especificar la configuración de dúplex y de velocidad de una interfaz de switch, se recomienda permitir que el switch configure estos parámetros automáticamente para evitar errores.
- La seguridad de puertos es solo uno de los métodos de defensa contra los riesgos que puede sufrir la red.



Sección 5.1

Términos y comandos

- Prueba de autodiagnóstico al encender (POST)
- Cargador de arranque
- Variable de entorno de BOOT
- **boot system**
- **show boot**
- Botón Mode
- LED del sistema
- switch del cargador de inicio:
- **dir flash:**
- LED del sistema
- LED del sistema de alimentación redundante (RPS)
- LED de estado del puerto
- LED de modo dúplex del puerto
- LED de velocidad del puerto
- LED de Alimentación por Ethernet (POE)
- Interfaz virtual de switch (SVI)
- VLAN
- Dúplex completo
- Semidúplex
- Auto-MDIX
- **interface vlan 99**
- **ip default-gateway**
- **show ip interface brief**
- **duplex auto**
- **speed auto**
- **mdix auto**
- **show interfaces**
- Errores de entrada
- Fragmentos de colisión
- Fragmentos gigantes
- Error de CRC
- Errores de salida
- Colisiones
- Colisiones tardías



Sección 5.2

Términos y comandos

- Secure Shell (SSH)
- `show ip ssh version 2`
- `crypto key generate rsa`
- `crypto key zeroize rsa`
- Username *nombre de usuario* secret *contraseña*
- `transport input ssh`
- `login local`
- `show ip ssh`
- Dirección MAC segura estática
- Dirección MAC segura dinámica
- Dirección MAC segura persistente
- `show port-security`
- `show port-security mac-address`
- `show port-security mac-address sticky`
- `show port-security interface`
- Proteger
- Restringir
- Apagar
- `switchport port-security violation {protect | restrict | shutdown}`
- Switchport port-security maximum #
- `show port-security interface id-de-interfaz`
- `show port-security address:`
- Secure-shutdown

