Configuración del switch

Los switches se usan para conectar varios dispositivos en la misma red. En una red diseñada correctamente, los switches LAN son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red.

Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar. Sin embargo, los switches Cisco ejecutan Cisco IOS y se pueden configurar manualmente para satisfacer mejor las necesidades de la red. Esto incluye el ajuste de los requisitos de velocidad, de ancho de banda y de seguridad de los puertos.

Además, los switches Cisco se pueden administrar de manera local y remota. Para administrar un switch de forma remota, este se debe configurar con una dirección IP y un gateway predeterminado.

Secuencia de arranque de un switch

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.

El cargador de arranque busca la imagen de Cisco IOS en el switch de la siguiente manera: el switch intenta arrancar automáticamente mediante la información de la variable de entorno BOOT. Si no se establece esta variable, el switch intenta cargar y ejecutar el primer archivo ejecutable que puede mediante una búsqueda recursiva y en profundidad en todo el sistema de archivos flash. Cuando se realiza una búsqueda en profundidad de un directorio, se analiza por completo cada subdirectorio que se encuentra antes de continuar la búsqueda en el directorio original.

En los switches de la serie Catalyst 2960, el archivo de imagen generalmente se encuentra en un directorio que tiene el mismo nombre que el archivo de imagen (excepto la extensión de archivo .bin). Luego, el sistema operativo IOS inicia las interfaces mediante los comandos del IOS de Cisco que se encuentran en el archivo de configuración de arranque, que se almacena en NVRAM.

Recuperación tras un bloqueo del sistema

El cargador de arranque proporciona acceso al switch si no se puede usar el sistema operativo debido a la falta de archivos de sistema o al daño de estos. El cargador de arranque tiene una línea de comandos que proporciona acceso a los archivos almacenados en la memoria flash.

Se puede acceder al cargador de arranque mediante una conexión de consola con los siguientes pasos:

Paso 1: Conecte una computadora al puerto de consola del switch con un cable de consola. Configure el software de emulación de terminal para conectarse al switch.

Paso 2. Desconecte el cable de alimentación del switch.

Paso 3. Vuelva a conectar el cable de alimentación al switch, espere 15 segundos y, a continuación, presione y mantenga presionado el botón **Mode** (Modo) mientras el LED del sistema sigue parpadeando con luz verde.

Paso 4: Continúe oprimiendo el botón **Modo** hasta que el LED del sistema se torne ámbar por un breve instante y luego verde, después suelte el botón **Modo**.

Paso 5: Aparece la petición de entrada **switch:** del cargador de arranque en el software de emulación de terminal en la computadora.

La línea de comandos de boot loader admite comandos para formatear el sistema de archivos flash, volver a instalar el software del sistema operativo y recuperar una contraseña perdida u olvidada. Por ejemplo, el comando **dir** se puede usar para ver una lista de archivos dentro de un directorio específico, como se muestra en la figura.

```
Switch# dir flash:
Directory of flash:/

   2 -rwx  11607161  Mar 1  2013  03:10:47  +00:00  c2960-lanbasek9-mz.150-2.SE.bin
   3 -rwx      1809  Mar 1  2013  00:02:48  +00:00  config.text
   5 -rwx      1919  Mar 1  2013  00:02:48  +00:00  private-config.text
   6 -rwx     59416  Mar 1  2013  00:02:49  +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#
```

Los switches Cisco Catalyst tienen varios indicadores luminosos LED de estado. Puede usar los LED del switch para controlar rápidamente la actividad y el rendimiento del switch. Los diferentes modelos y conjuntos de características de los switches tienen diferentes LED, y la ubicación de estos en el panel frontal del switch también puede variar.
En la ilustración, se muestran los LED y el botón Mode de un switch Cisco Catalyst 2960. El botón Mode se utiliza para alternar entre el estado del puerto, el modo dúplex del puerto, la velocidad del puerto y el estado de alimentación por Ethernet (PoE [si se admite]) de los LED del puerto. A continuación, se describe el propósito de los indicadores LED y el significado de los colores:

- **LED del sistema:** muestra si el sistema recibe alimentación y funciona correctamente. Si el LED está apagado, significa que el sistema no está encendido. Si el LED es de color verde, el sistema funciona normalmente. Si el LED es de color ámbar, el sistema recibe alimentación pero no funciona correctamente.

- **LED del sistema de alimentación redundante (RPS):** muestra el estado del RPS. Si el LED está apagado, el RPS está apagado o no está conectado correctamente. Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo. Si el LED parpadea y es de color verde, el RPS está conectado pero no está disponible porque está proporcionando alimentación a otro dispositivo. Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla. Si el LED parpadea y es de color ámbar, la fuente de alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.

- **LED de estado del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo de estado del puerto. Este es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, no hay enlace, o el puerto estaba administrativamente inactivo. Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos. Si el LED alterna entre verde y ámbar, hay una falla en el enlace. Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación). Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.

- **LED de modo dúplex del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo dúplex del puerto. Al seleccionarlo, los LED del puerto que están apagados están en modo semidúplex. Si el LED del puerto es de color verde, el puerto está en modo dúplex completo.

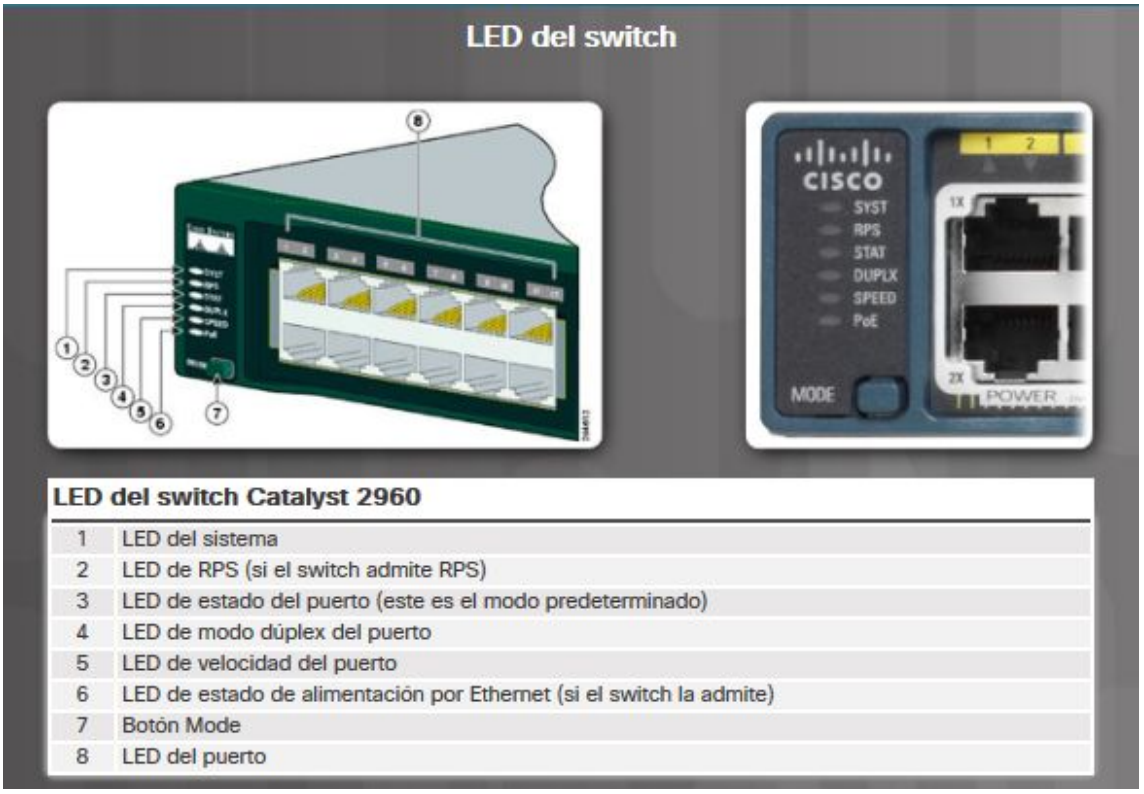
- **LED de velocidad del puerto:** indica que se seleccionó el modo de velocidad del puerto. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, el puerto funciona a 10 Mb/s. Si el LED es de color verde, el puerto funciona a 100 Mb/s. Si el LED parpadea y es de color verde, el puerto funciona a 1000 Mb/s.

- **LED de modo de alimentación por Ethernet**: si se admite alimentación por Ethernet, hay un LED de modo de PoE. Si el LED está apagado, indica que no se seleccionó el modo de alimentación por Ethernet, que a ninguno de los puertos se le negó el suministro de alimentación y ninguno presenta fallas. Si el LED parpadea y es de color ámbar, no se seleccionó el modo de alimentación por Ethernet, pero al menos a uno de los puertos se le negó el suministro de alimentación o uno de ellos presenta una falla de alimentación por Ethernet. Si el LED es de color verde, indica que se seleccionó el modo de alimentación por Ethernet, y los LED del puerto muestran colores con diferentes significados

- Si el LED del puerto está apagado, la alimentación por Ethernet está desactivada.

- Si el LED del puerto es de color verde, la alimentación por Ethernet está activada.

- Si el LED del puerto alterna entre verde y ámbar, se niega la alimentación por Ethernet, ya que, si se suministra energía al dispositivo alimentado, se excede la capacidad de alimentación del switch. Si el LED parpadea y es de color ámbar, la alimentación por Ethernet está desactivada debido a una falla. Si el LED es de color ámbar, se inhabilitó la alimentación por Ethernet para el puerto.



LED del switch Catalyst 2960	
1	LED del sistema
2	LED de RPS (si el switch admite RPS)
3	LED de estado del puerto (este es el modo predeterminado)
4	LED de modo dúplex del puerto
5	LED de velocidad del puerto
6	LED de estado de alimentación por Ethernet (si el switch la admite)
7	Botón Mode
8	LED del puerto

Preparación para la administración básica de un switch

Para el acceso a la administración remota de un switch, este se debe configurar con una dirección IP y una máscara de subred. Recuerde que para administrar un switch desde una red remota, se lo debe configurar con un gateway predeterminado. Este es un proceso muy similar a la configuración de la información de dirección IP en los dispositivos host. En la ilustración, se debe asignar una dirección IP a la interfaz virtual del switch (SVI) de S1. La SVI es una interfaz virtual, no un puerto físico del switch.

SVI es un concepto relacionado con las VLAN. Las VLAN son grupos lógicos numerados a los que se pueden asignar puertos físicos. Los parámetros de configuración aplicados a una VLAN también se aplican a todos los puertos asignados a esa VLAN.

Configuración del acceso a la administración básica de un switch con IPv4

Paso 1: Configuración de la interfaz de administración
Se configura una dirección IPv4 y una máscara de subred en la SVI de administración del switch desde el modo de configuración de interfaz VLAN. Como se muestra en la figura 1, el comando **interface vlan 99** se usa para ingresar al modo de configuración de interfaz. Para configurar la dirección IPv4, se usa el comando **ip address**. El comando **no shutdown** habilita la interfaz. En este ejemplo, la VLAN 99 se configuró con la dirección IPv4 172.17.99.11.

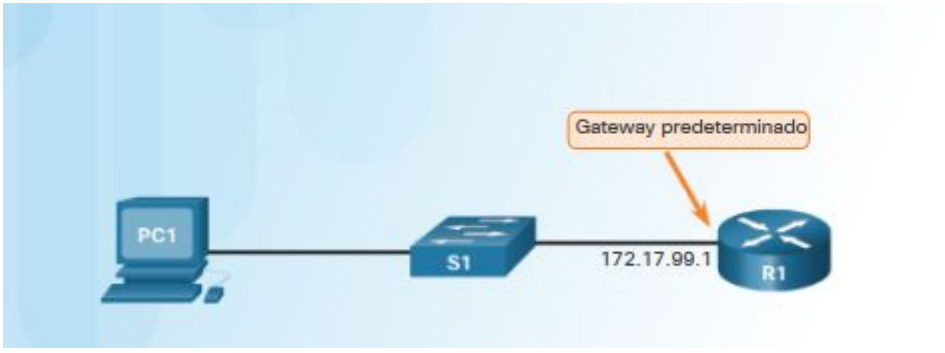
La SVI para la VLAN 99 no se muestra como "up/up" hasta que se cree la VLAN 99 y haya un dispositivo conectado a un puerto del switch asociado a la VLAN 99. Para crear una VLAN con la id_de_vlan 99 y asociarla a una interfaz, use los siguientes comandos:
S1(config)# **vlan** *id_de_vlan*
S1(config-vlan)# **name** *nombre_de_vlan*
S1(config-vlan)# **exit**
S1(config)# **interfaz** *id_de_interfaz*
S1(config-if)# **switchport access vlan** *id_de_vlan*

Paso 2: Configuración del gateway predeterminado
Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado. El gateway predeterminado es el router al que está conectado el switch. El switch reenvía los paquetes IP con direcciones IP de destino fuera de la red local al gateway predeterminado. Como se muestra en la figura 2, R1 es el gateway predeterminado para S1. La interfaz en R1 conectada al switch tiene la dirección IPv4 172.17.99.1. Esta es la dirección de gateway predeterminado para S1.

Para configurar el gateway predeterminado del switch, use el comando **ip default-gateway**. Introduzca la dirección IPv4 del gateway predeterminado. El gateway predeterminado es la dirección IPv4 de la interfaz del router a la que está conectado el switch. Use el comando **copy running-config startup-config** para realizar una copia de seguridad de la configuración.

Paso 3: Verificar la configuración

Como se muestra en la figura 3, el comando **show ip interface brief** es útil para determinar el estado de las interfaces virtuales y físicas. El resultado que se muestra confirma que la interfaz VLAN 99 se ha configurado con una dirección IPv4 y una máscara de subred.



Comunicación dúplex

La comunicación en dúplex completo mejora el rendimiento de una LAN conmutada. La comunicación en dúplex completo aumenta el ancho de banda eficazmente al permitir que ambos extremos de una conexión transmitan y reciban datos simultáneamente. Esto también se conoce como comunicación bidireccional.

A diferencia de la comunicación en dúplex completo, la comunicación en semidúplex es unidireccional. El envío y la recepción de datos no ocurren al mismo tiempo. La comunicación en semidúplex genera

problemas de rendimiento debido a que los datos fluyen en una sola dirección por vez, lo que a menudo provoca colisiones. Las conexiones semidúplex suelen verse en los dispositivos de hardware más antiguos, como los hubs.La comunicación en dúplex completo reemplazó al semidúplex en la mayoría del hardware.

Las NIC Gigabit Ethernet y de 10 Gb requieren conexiones dúplex completo para funcionar. En el modo dúplex completo, el circuito de detección de colisiones de la NIC se encuentra inhabilitado. Las tramas enviadas por los dos dispositivos conectados no pueden colisionar, dado que estos utilizan dos circuitos independientes en el cable de red. Las conexiones dúplex completo requieren un switch que admita la configuración dúplex completo o una conexión directa entre dos dispositivos mediante un cable Ethernet.

Configuración de puertos de switch en la capa física

Dúplex y velocidad

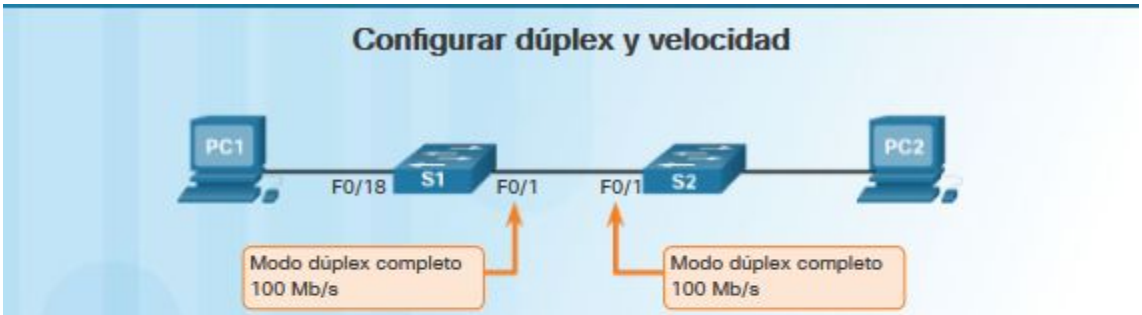
Los puertos de switch se pueden configurar manualmente con parámetros específicos de dúplex y de velocidad. Use el comando **duplex** del modo de configuración de interfaz para especificar manualmente el modo dúplex de un puerto de switch. Use el comando **speed** del modo de configuración de interfaz para especificar manualmente la velocidad de un puerto de switch.

La configuración predeterminada de dúplex y velocidad para los puertos de switch en los switches Cisco Catalyst 2960 y 3560 es automática. Los puertos 10/100/1000 funcionan en el modo semidúplex o dúplex completo cuando se establecen en 10 Mb/s o 100 Mb/s, pero solo funcionan en el modo dúplex completo cuando se establecen en 1000 Mb/s (1 Gb/s).

La autonegociación es útil cuando se desconoce la configuración de dúplex y de velocidad del dispositivo que se conecta al puerto o cuando es posible que dicha configuración cambie. Al conectarse a dispositivos conocidos, como servidores, estaciones de trabajo dedicadas o dispositivos de red, se recomienda establecer manualmente la configuración de dúplex y de velocidad.

Cuando se realiza la resolución de problemas de puertos de switch, se debe verificar la configuración de dúplex y de velocidad.

Nota: si la configuración para el modo dúplex y la velocidad de puertos del switch presenta incompatibilidades, se pueden producir problemas de conectividad. Una falla de autonegociación provoca incompatibilidades en la configuración.
Todos los puertos de fibra óptica, como los puertos 1000BASE-SX, solo funcionan a una velocidad predefinida y siempre son dúplex completo.



Comandos de IOS de un switch Cisco

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

Auto-MDIX

Hasta hace poco, se requerían determinados tipos de cable (cruzado o directo) para conectar dispositivos. Las conexiones switch a switch o switch a router requerían el uso de diferentes cables Ethernet. Mediante el uso de la característica automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX) en una interfaz, se elimina este problema. Al habilitar la característica auto-MDIX, la interfaz detecta automáticamente el tipo de conexión de cable requerido (directo o cruzado) y configura la conexión conforme a esa información. Al conectarse a los switches sin la función auto-MDIX, los cables directos deben utilizarse para conectar a dispositivos como servidores, estaciones de trabajo o routers. Los cables cruzados se deben utilizar para conectarse a otros switches o repetidores.

Con la característica auto-MDIX habilitada, se puede usar cualquier tipo de cable para conectarse a otros dispositivos, y la interfaz se ajusta de manera automática para proporcionar comunicaciones satisfactorias. En los switches Cisco más modernos, el comando del modo de configuración de interfaz **mdix auto** habilita la característica. Cuando se usa auto-MDIX en una interfaz, la velocidad y el modo dúplex de la interfaz se deben establecer en **auto** para que la característica funcione correctamente.

Verificación de la configuración de puertos de un switch

Para validar los parámetros configurados o preestablecidos en un switch Cisco es necesario utilizar el comando show, este comando acompañado con otras instrucciones permite evaluar diversos requisitos del switch.

Comandos de verificación

Comandos de IOS de un switch Cisco	
Muestra el estado y la configuración de la interfaz.	S1# show interfaces [interface-id]
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 [interface-id]
Muestra la tabla de direcciones MAC.	S1# show mac-address-table OR S1# show mac address-table

Problemas de la capa de acceso a la red

El resultado del comando **show interfaces** se puede usar para detectar problemas frecuentes de los medios. Una de las partes más importantes de este resultado es la visualización del estado del protocolo de línea y de enlace de datos.

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up Hardware is Fast Ethernet, address is
0022.91c4.0e01 (bia 0022.91c4.0e01) MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<se omitió el resultado>
  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
<Se omitió el resultado>
```

Los errores de entrada que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Runt frames:** las tramas de Ethernet más cortas que la longitud mínima permitida de 64 bytes se denominan “runt frames” (fragmentos de colisión). La NIC en mal funcionamiento son la causa habitual de las tramas excesivas de fragmentos de colisión, pero también pueden deberse a colisiones.

- **Giants**: las tramas Ethernet más grandes que el tamaño máximo permitido se denominan gigantes.

- **Errores de CRC:** en las interfaces Ethernet y seriales, los errores de CRC generalmente indican que hay errores en los medios o en los cables. Las causas más comunes incluyen interferencia

eléctrica, conexiones flojas o dañadas o cableado incorrecto. Si aparecen muchos errores de CRC, hay demasiado ruido en el enlace, y se debe examinar el cable. También se deben buscar y eliminar las fuentes de ruido.

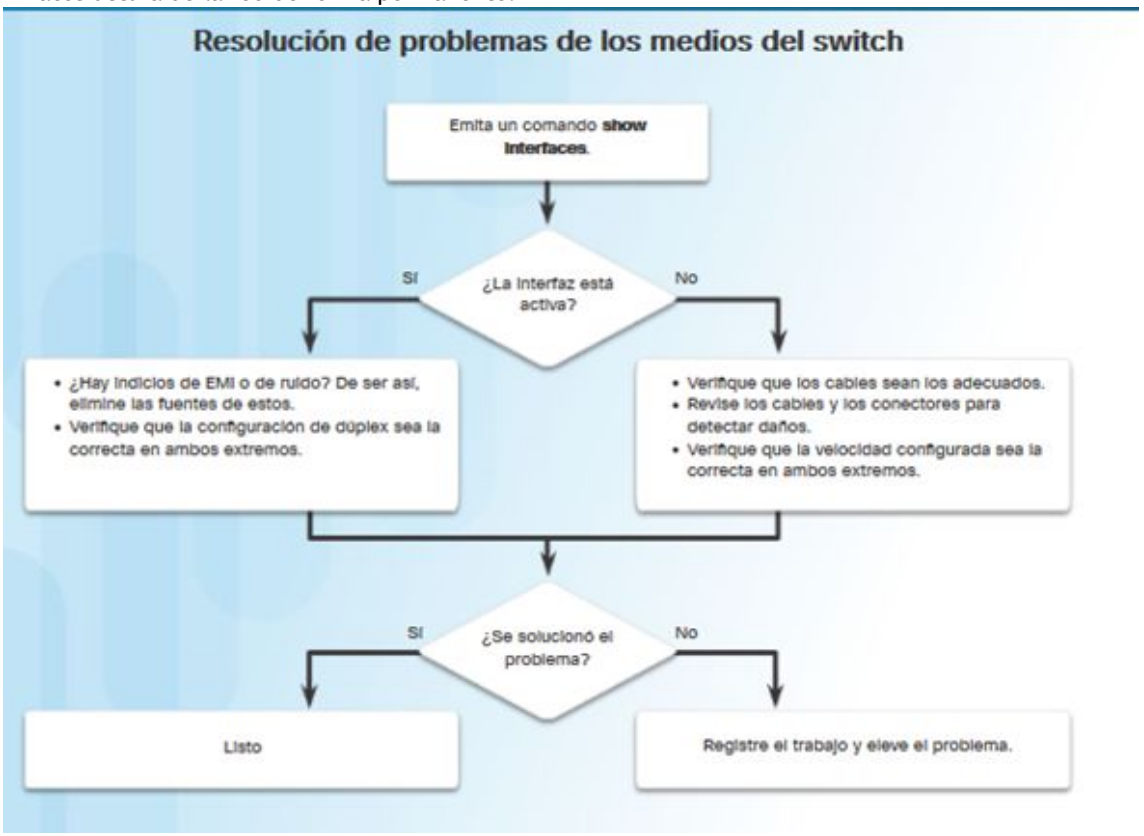
"Output errors" es la suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza. Los errores de salida que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Collisions**: las colisiones en las operaciones en semidúplex son normales. Sin embargo, nunca debe observar colisiones en una interfaz configurada para la comunicación en dúplex completo.

- **Late collisions**: las colisiones tardías se refieren a las colisiones que ocurren después de que se transmitieron 512 bits de la trama. La longitud excesiva de los cables es la causa más frecuente de las colisiones tardías. Otra causa frecuente es la configuración incorrecta de dúplex. Por ejemplo, el extremo de una conexión puede estar configurado para dúplex completo y el otro para semidúplex. Las colisiones tardías se verían en la interfaz que está configurada para semidúplex. En ese caso, debe configurar los mismos parámetros de dúplex en ambos extremos. Una red diseñada y configurada correctamente nunca debería tener colisiones tardías.

Resolución de problemas de la capa de acceso a la red

La mayoría de los problemas que afectan a las redes conmutadas se produce durante la implementación inicial. En teoría, una vez instaladas, las redes continúan funcionando sin problemas. Sin embargo, los cables se dañan, la configuración cambia, y se conectan al switch nuevos dispositivos que requieren cambios de configuración en este. Se requiere el mantenimiento y la resolución de problemas de infraestructura de la red de forma permanente.



Funcionamiento de SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. El SSH debe reemplazar a Telnet para las conexiones de administración. Telnet es un

protocolo más antiguo que usa la transmisión no segura de texto no cifrado de la autenticación de inicio de sesión (nombre de usuario y contraseña) y de los datos transmitidos entre los dispositivos que se comunican. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro cuando se autentica un dispositivo (nombre de usuario y contraseña) y también para los datos transmitidos entre los dispositivos que se comunican. SHH se asigna al puerto TCP 22. Telnet se asigna al puerto TCP 23.
Para habilitar SSH en un switch Catalyst 2960, el switch debe usar una versión del software IOS que incluya características y capacidades criptográficas (cifradas)

Configuración de SSH

Antes de configurar SSH, el switch debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

Paso 1: Verificar la compatibilidad con SSH
Use el comando **show ip ssh** para verificar que el switch admita SSH. Si el switch no ejecuta un IOS que admita características criptográficas, este comando no se reconoce.

Paso 2: Configurar el dominio IP
Configure el nombre de dominio IP de la red mediante el comando **ip domain-name** *nombre-de-dominio* comando del modo de configuración global. En la figura 1, el valor de *"nombre-de-dominio* es **cisco.com**.

Paso 3: Generar pares de claves RSA
No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando **ip ssh version 2** del modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando **crypto key generate rsa** del modo de configuración global para habilitar el servidor SSH en el switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. La configuración de ejemplo en la figura 1 utiliza un tamaño de módulo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más en generarlo y utilizarlo.

Nota: para eliminar el par de claves RSA, use el comando **crypto key zeroize rsa** del modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Paso 4: Configurar la autenticación de usuario
El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un par de nombres de usuario y contraseñas con el comando **username** *Nombre de usuario* **secret** *Contraseña* comando del modo de configuración global. En el ejemplo, se asignó la contraseña **ccna** al usuario **admin**.

Paso 5: Configurar las líneas vty
Habilite el protocolo SSH en las líneas vty mediante el comando **transport input ssh** del modo de configuración de línea. El switch Catalyst 2960 tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al switch a que acepte solo las conexiones SSH. Use el comando **line vty** del modo de configuración global y, luego, el comando **login local** del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6: Habilitar la versión 2 de SSH
De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de **show ip ssh** se muestra que se admite la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilite la versión de SSH mediante el comando de configuración global **ip ssh version 2**.

Asegurar los puertos sin utilizar

Deshabilitar puertos en desuso

Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Por ejemplo, si un switch Catalyst 2960 tiene 24 puertos y hay tres conexiones Fast Ethernet en uso, es aconsejable inhabilitar los 21 puertos que no se utilizan. Navegue hasta todos los puertos que no se utilizan y emita el comando **shutdown** de Cisco IOS. Si, más adelante, se debe reactivar un puerto, se puede habilitar con el comando **no shutdown** La figura muestra el resultado parcial para esta configuración.
Realizar cambios de configuración a varios puertos de un switch es sencillo. Si se debe configurar un rango de puertos, use el comando **interface range**.

Switch(config)# **interface range** *escriba el módulo/primer-número - último-número*
El proceso de habilitación e inhabilitación de puertos puede llevar mucho tiempo, pero mejora la seguridad de la red y vale la pena el esfuerzo.

Seguridad de puertos: funcionamiento

Seguridad de puertos

Se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para la producción. Una forma de proteger los puertos es mediante la implementación de una característica denominada “seguridad de puertos”. La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto.
Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC, cualquier intento adicional de conexión de las direcciones MAC desconocidas genera una violación de seguridad.

Tipos de direcciones MAC seguras

Existen varias maneras de configurar la seguridad de puerto. El tipo de dirección segura se basa en la configuración e incluye lo siguiente:

- **Direcciones MAC seguras estáticas**: son direcciones MAC que se configuran manualmente en un puerto mediante el comando **switchport port-security mac-address** *dirección-mac* (comando del modo de configuración de interfaz) Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch.
- **Direcciones MAC seguras dinámicas:** son direcciones MAC detectadas dinámicamente y se almacenan solamente en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.
- **Direcciones MAC seguras persistentes:** son direcciones MAC que pueden detectarse de forma dinámica o configurarse de forma manual, y que después se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución.

Direcciones MAC seguras persistentes

Para configurar una interfaz a fin de convertir las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes y agregarlas a la configuración en ejecución, debe habilitar el aprendizaje por persistencia. El aprendizaje por persistencia se habilita en una interfaz mediante el comando **switchport port-security mac-address sticky** del modo de configuración de interfaz.

Cuando se introduce este comando, el switch convierte todas las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes, incluso las que se detectaron dinámicamente antes de que se habilitara el aprendizaje por persistencia. Todas las direcciones MAC seguras persistentes se agregan a la tabla de direcciones y a la configuración en ejecución.

Las direcciones MAC seguras persistentes también se pueden definir manualmente. Cuando se configuran las direcciones MAC seguras persistentes con el comando de configuración de interfaz **switchport port-security mac-address sticky** *dirección-mac* todas las direcciones especificadas se agregan a la tabla de direcciones y a la configuración en ejecución.

Si se guardan las direcciones MAC seguras persistentes en el archivo de configuración de inicio, cuando el switch se reinicia o la interfaz se desactiva, la interfaz no necesita volver a aprender las direcciones. Si no se guardan las direcciones seguras persistentes, estas se pierden.

Si se inhabilita el aprendizaje por persistencia mediante el comando **no switchport port-security mac-address sticky** del modo de configuración de interfaz, las direcciones MAC seguras persistentes siguen formando parte de la tabla de direcciones, pero se eliminan de la configuración en ejecución.

Seguridad de puertos: modos de violación de seguridad

Se puede configurar una interfaz para uno de tres modos de violación, con la acción específica que se debe realizar si se produce una violación. La figura muestra los tipos de tráficos de datos que se envían cuando se configura en el puerto uno de los siguientes modos de violación de seguridad.

- **Protect (Proteger):** cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. No hay ninguna notificación de que se produjo una violación de seguridad.

- **Restrict (Restringir):** cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. En este modo, hay una notificación de que se produjo una violación de seguridad.

- **Shutdown** (Desactivar): en este modo (predeterminado), una violación de seguridad de puerto produce que la interfaz se inhabilite de inmediato por errores y que se apague el LED del puerto. Aumenta el contador de violaciones. Cuando un puerto seguro está en el estado inhabilitado por errores, se lo puede sacar de este estado si se introduce el comando de modo de configuración de interfaz **shutdown** seguido por el comando **no shutdown**.

Para cambiar el modo de violación en un puerto de switch, use el comando del modo de configuración de interfaz **switchport port-security violation** {**protect** | **restrict** | **shutdown**}.

Seguridad de puertos: verificación

Verificar la seguridad del puerto
Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Verificar los parámetros de seguridad del puerto
Para mostrar la configuración de seguridad de puertos para el switch o la interfaz especificada, use el comando **show port-security interface** [*interface-id*].

Verificar las direcciones MAC seguras
Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz especificada con la información de vencimiento para cada una, use el comando **show port-security address**.

Puertos en estado de inhabilitación por errores

Cuando se configura un puerto con seguridad de puertos, una violación puede provocar que el puerto se inhabilite por errores. Cuando un puerto se inhabilita por errores, se desactiva eficazmente, y no se envia ni se recibe tráfico en ese puerto.

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.

La variable de entorno BOOT determina el archivo de Cisco IOS específico que se carga. Una vez que se carga Cisco IOS, utiliza los comandos que encuentra en el archivo startup-config para inicializar y configurar las interfaces. 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.