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. Estos son solo dos de los parámetros de configuración que se analizan en este capítulo.

Los switches funcionan en lugares de la capa de acceso donde los dispositivos de red cliente se conectan directamente a la red y donde los departamentos de TI quieren que los usuarios accedan de forma simple a esta. Es una de las áreas más vulnerables de la red, ya que está muy expuesta al usuario. Los switches se deben configurar para que sean resistentes a los ataques de todo tipo y, al mismo tiempo, protejan los datos de los usuarios y permitan que haya conexiones de alta velocidad. La seguridad de puertos es una de las características de seguridad que proporcionan los switches administrados por Cisco.

En este capítulo, se analizan algunas de las opciones de configuración básica de switch que se requieren para mantener un entorno LAN conmutado seguro y disponible.

Una vez que se enciende el switch Cisco, lleva a cabo 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 ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al 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, startup-config, que está almacenado en NVRAM.

En la ilustración, la variable de entorno BOOT se establece con el comando **boot system** del modo de configuración global. Observe que el IOS se ubica en una carpeta distinta y que se especifica la ruta de la carpeta. Use el comando **show bootvar** (**show boot** en versiones anteriores de IOS) para ver la configuración actual del archivo de arranque de IOS.

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 recuperarse de la pérdida o el olvido de una contraseña. Por ejemplo, el comando**dir** se puede usar para ver una lista de archivos dentro de un directorio específico, como se muestra en la ilustración.

**Nota**: observe que, en este ejemplo, el IOS se ubica en la raíz de la carpeta de la memoria flash.

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 se conectó 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. Éste 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 half-duplex. Si el LED del puerto es de color verde, el puerto está en modo full-duplex.
* **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.

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.

De manera predeterminada, el switch está configurado para que el control de la administración del switch se realice mediante la VLAN 1. Todos los puertos se asignan a la VLAN 1 de manera predeterminada. Por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

Tenga en cuenta que el propósito de esta configuración IP es solamente obtener acceso a la administración remota del switch; la configuración IP no permite que el switch enrute paquetes de capa 3.

**Paso 1. Configurar la interfaz de administración**

Se configura una dirección IP 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 IP, se usa el comando **ip address**. El comando **no shutdown** habilita la interfaz. En este ejemplo, la VLAN 99 se configuró con la dirección IP 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)# **interface***interface\_id*

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 IP 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 IP del gateway predeterminado. El gateway predeterminado es la dirección IP 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 configuró con una dirección IP y una máscara de subred y que está en condiciones de funcionamiento.

En la ilustración, se muestra la comunicación full-duplex y half-duplex.

La comunicación full-duplex mejora el rendimiento de una LAN conmutada. La comunicación full-duplex aumenta el ancho de banda eficaz al permitir que ambos extremos de una conexión transmitan y reciban datos simultáneamente. Esto también se conoce como “flujo de datos bidireccional”. Este método de optimización de rendimiento de la red requiere microsegmentación. Las LAN microsegmentadas se crean cuando un puerto de switch tiene solo un dispositivo conectado y funciona en modo full-duplex. Como resultado, se obtiene el dominio de colisiones de tamaño micro de un único dispositivo. Sin embargo, debido a que hay solamente un dispositivo conectado, en las LAN microsegmentadas no hay colisiones.

A diferencia de la comunicación full-duplex, la comunicación half-duplex es unidireccional. El envío y la recepción de datos no ocurren al mismo tiempo. La comunicación half-duplex genera problemas de rendimiento debido a que los datos fluyen en una sola dirección por vez, lo que a menudo provoca colisiones. Las conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs. La comunicación full-duplex reemplazó a la half-duplex en la mayoría del hardware.

Actualmente, la mayoría de las tarjetas NIC Ethernet y Fast Ethernet disponibles en el mercado proporciona capacidad full-duplex. Las NIC Gigabit Ethernet y de 10 Gb requieren conexiones full-duplex para funcionar. En el modo full-duplex, 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 full-duplex requieren un switch que admita la configuración full-duplex o una conexión directa entre dos dispositivos mediante un cable Ethernet.

En general, la eficacia de una configuración Ethernet compartida estándar basada en hubs es del 50% al 60% del ancho de banda indicado. Full-duplex ofrece el 100% de eficacia en ambas direcciones (transmisión y recepción). Como resultado, se obtiene un uso potencial del 200% del ancho de banda indicado.

**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. En la figura 1, el puerto F0/1 de los switches S1 y S2 se configura manualmente con la palabra clave **full** para el comando **duplex** y la palabra clave **100** para el comando**speed**.

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 half-duplex o full-duplex cuando se establecen en 10 Mb/s o 100 Mb/s, pero solo funcionan en el modo full-duplex 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 100BASE-FX, solo funcionan a una velocidad predefinida y siempre son full-duplex.

Use el verificador de sintaxis de la figura 2 para configurar el puerto F0/1 del switch S1.

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 característica auto-MDIX, se deben usar cables directos para conectarse a dispositivos como servidores, estaciones de trabajo o routers, y cables cruzados 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 routers y switches Cisco más modernos, el comando **mdix auto** del modo de configuración de interfaz 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.

Los comandos para habilitar auto-MDIX se muestran en la figura 1.

**Nota:** la característica auto-MDIX está habilitada de manera predeterminada en los switches Catalyst 2960 y Catalyst 3560, pero no está disponible en los switches más antiguos Catalyst 2950 y Catalyst 3550.

Para examinar la configuración de auto-MDIX de una interfaz específica, use el comando **show controllers ethernet-controller** con la palabra clave**phy**. Para limitar los resultados a las líneas que se refieren a auto-MDIX, use el filtro **include Auto-MDIX**. Como se muestra en la figura 2, el resultado indica On (Habilitada) u Off (Deshabilitada) para la característica.

Use el verificador de sintaxis de la figura 3 para configurar la interfaz FastEthernet 0/1 de S2 con auto-MDIX.

En la figura 1, se describen algunas de las opciones del comando **show** que son útiles para verificar las características configurables comunes de un switch.

En la figura 2, se muestra un resultado abreviado del comando **show running-config**. Use este comando para verificar que el switch se haya configurado correctamente. Como se observa en el resultado de S1, se muestra cierta información clave:

* Interfaz Fast Ethernet 0/18 configurada con la VLAN 99 de administración
* VLAN 99 configurada con la dirección IP 172.17.99.11 255.255.255.0
* Gateway predeterminado establecido en 172.17.99.1

El comando **show interfaces** es otro comando de uso frecuente que muestra información estadística y de estado sobre las interfaces de red del switch. El comando **show interfaces** se usa habitualmente cuando se configuran y se controlan los dispositivos de red.

En la figura 3, se muestra el resultado del comando **show interfaces fastEthernet 0/18**. En la primera línea de la ilustración, se indica que la interfaz FastEthernet 0/18 está “up/up”, lo que significa que está en funcionamiento. Más abajo en el resultado, se muestra que el modo dúplex es full y la velocidad es de 100 Mb/s.

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. En la figura 1, se indica la línea de resumen para revisar el estado de una interfaz.

El primer parámetro (FastEthernet0/1 is up) se refiere a la capa de hardware y, básicamente, refleja si la interfaz recibe la señal de detección de portadora del otro extremo. El segundo parámetro (line protocol is up) se refiere a la capa de enlace de datos y refleja si se reciben los keepalives del protocolo de capa de enlace de datos.

Sobre la base del resultado del comando **show interfaces**, los posibles problemas se pueden reparar de la siguiente manera:

* Si la interfaz está activa y el protocolo de línea está inactivo, hay un problema. Puede haber una incompatibilidad en el tipo de encapsulación, la interfaz en el otro extremo puede estar inhabilitada por errores o puede haber un problema de hardware.
* Si el protocolo de línea y la interfaz están inactivos, hay un cable que no está conectado o existe algún otro problema de interfaz. Por ejemplo, en una conexión directa, el otro extremo de la conexión puede estar administrativamente inactivo.
* Si la interfaz se encuentra administrativamente inactiva, se inhabilitó manualmente en la configuración activa (se emitió el comando **shutdown**).

En la figura 2, se muestra un ejemplo del resultado del comando **show interfaces**. En el ejemplo, se muestran los contadores y las estadísticas de la interfaz FastEthernet0/1.

Algunos errores de medios no son lo suficientemente graves para provocar una falla en el circuito, pero sí provocan problemas en el rendimiento de la red. En la figura 3, se explican algunos de estos errores frecuentes, los cuales se pueden detectar mediante el comando **show interfaces**.

“Input errors” indica la suma de todos los errores en los datagramas que se recibieron en la interfaz que se analiza. Estos incluyen 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. 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 causa del exceso de fragmentos de colisión suele ser una NIC en mal funcionamiento, pero este puede deberse a los mismos problemas que causan el exceso de colisiones.
* **Giants:** las tramas Ethernet más largas que la longitud máxima permitida se denominan “giants” (fragmentos gigantes). Los fragmentos gigantes se deben a los mismos problemas que causan los fragmentos de colisión.
* **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 comunes incluyen interferencia eléctrica, conexiones flojas o dañadas o el uso del tipo de cable incorrecto. Si aparecen muchos errores de CRC, hay demasiado ruido en el enlace, y se debe examinar el cable para conocer la longitud y detectar daños. También se deben buscar y eliminar las fuentes del ruido, si es posible.

“Output errors” indica 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 half-duplex son completamente normales y no debe preocuparse por estas, siempre que esté satisfecho con el funcionamiento half-duplex. Sin embargo, nunca debe haber colisiones en una red correctamente diseñada y configurada que use la comunicación full-duplex. Se recomienda especialmente usar full-duplex, a menos que tenga un equipo más antiguo o heredado que requiera half-duplex.
* **Late collisions**: las colisiones tardías se refieren a las colisiones que ocurren después de que se transmitieron 512 bits (el preámbulo) 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 full-duplex y el otro para half-duplex. Las colisiones tardías se verían en la interfaz que está configurada para half-duplex. En ese caso, debe configurar los mismos parámetros de dúplex en ambos extremos. Una red diseñada y configurada correctamente nunca debería tener colisiones tardías.

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.

Para poder resolver estos problemas, si no cuenta con una conexión o tiene una conexión defectuosa entre un switch y otro dispositivo, siga este proceso general:

Para revisar el estado de la interfaz, use el comando **show interfaces**.

Si la interfaz está inactiva, realice lo siguiente:

* Verifique que se usen los cables adecuados. Además, revise los cables y los conectores para detectar daños. Si se sospecha que hay un cable defectuoso o incorrecto, reemplácelo.
* Si la interfaz continúa inactiva, el problema puede deberse a una incompatibilidad en la configuración de velocidad. En general, la velocidad de una interfaz se negocia automáticamente; por lo tanto, incluso si se configura manualmente, la interfaz que se conecta debe negociar automáticamente conforme a ello. Si se produce una incompatibilidad de velocidad debido a una configuración incorrecta o a un problema de hardware o de software, esto podría provocar que la interfaz quede inactiva. Establezca manualmente la misma velocidad en ambos extremos de la conexión si se sospecha que hay un problema.

Si la interfaz está activa pero aún hay problemas de conectividad, realice lo siguiente:

* Mediante el comando **show interfaces**, busque indicios de ruido excesivo. Los indicios pueden incluir un aumento en los contadores de fragmentos de colisión, de fragmentos gigantes y de errores de CRC. Si hay un exceso de ruido, primero busque el origen del ruido y, si es posible, elimínelo. Además, verifique qué tipo de cable se utiliza y que el cable no supere la longitud máxima. Para los cables de cobre, se recomienda que utilice, por lo menos, la categoría 5.
* Si no hay problemas de ruido, verifique si hay un exceso de colisiones. Si hay colisiones o colisiones tardías, verifique la configuración de dúplex en ambos extremos de la conexión. Al igual que la configuración de velocidad, la configuración de dúplex por lo general se negocia automáticamente. Si pareciera haber una incompatibilidad de dúplex, configúrelo manualmente en ambos extremos de la conexión. Se recomienda usar full-duplex si ambos extremos lo admiten.

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. 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.

En la figura 1, un atacante puede controlar los paquetes mediante Wireshark. Se puede dirigir un flujo de Telnet para que capture el nombre de usuario y la contraseña.

En la figura 2, el atacante puede capturar el nombre de usuario y la contraseña del administrador desde la sesión de Telnet de texto no cifrado.

En la figura 3, se muestra la vista de Wireshark de una sesión de SSH. El atacante puede hacer un seguimiento de la sesión mediante la dirección IP del dispositivo administrador.

Sin embargo, en la figura 4, el nombre de usuario y la contraseña están cifrados.

Para habilitar SSH en un switch Catalyst 2960, el switch debe usar una versión del software IOS que incluya características y capacidades criptográficas (cifradas). En la figura 5, use el comando **show version** en el switch para ver qué IOS se ejecuta actualmente en el dispositivo y el nombre de archivo de IOS que incluye la combinación “k9” que admite características y capacidades criptográficas (cifradas).

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* 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. Cisco recomienda un tamaño de módulo mínimo de 1024 bits (consulte la configuración de muestra en la figura 1). 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 nombre de usuario y una contraseña con el comando del modo de configuración global**username***nombre-de-usuario***secret***contraseña*. 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**.

Use el verificador de sintaxis de la figura 2 para configurar SSH en el switch S1.

En las computadoras, se usa un cliente SSH, como PuTTY, para conectarse a un servidor SSH. Para los ejemplos de las figuras 1 a 3, se configuró lo siguiente:

* Se habilitó SSH en el switch S1.
* Interfaz VLAN 99 (SVI) con la dirección IP 172.17.99.11 en el switch S1.
* PC1 con la dirección IP 172.17.99.21.

En la figura 1, la computadora inicia una conexión SSH a la dirección IP de la VLAN SVI de S1.

En la figura 2, se solicita al usuario que introduzca un nombre de usuario y una contraseña. Con la configuración del ejemplo anterior, se introduce el nombre de usuario **admin** y la contraseña **ccna**. Después de introducir la combinación correcta, el usuario se conecta a la CLI del switch Catalyst 2960 mediante SSH.

Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando **show ip ssh**. En el ejemplo, se habilitó la versión 2 de SSH. Para revisar las conexiones SSH al dispositivo, use el comando **show ssh** (consulte la figura 3).

La seguridad básica del switch no evita los ataques malintencionados. La seguridad es un proceso en capas que, básicamente, nunca está completo. Cuanto más consciente sea el equipo de profesionales de redes de una organización sobre los ataques de seguridad y los peligros que presentan, mejor. Algunos tipos de ataques de seguridad se describen aquí, pero los detalles sobre cómo funcionan algunos de estos ataques exceden el ámbito de este curso. Encontrará información más detallada en los cursos de tecnologías WAN y de seguridad de CCNA.

**Saturación de direcciones MAC**

La tabla de direcciones MAC de un switch contiene las direcciones MAC relacionadas con cada puerto físico y la VLAN asociada para cada puerto. Cuando un switch de la Capa 2 recibe una trama, el switch busca en la tabla de direcciones MAC la dirección MAC de destino. Todos los modelos de switches Catalyst utilizan una tabla de direcciones MAC para la conmutación en la Capa 2. A medida que llegan las tramas a los puertos del switch, se registran las direcciones MAC de origen en la tabla de direcciones MAC. Si la dirección MAC tiene una entrada en la tabla, el switch reenvía la trama al puerto correspondiente. Si la dirección MAC no existe en la tabla de direcciones MAC, el switch satura todos los puertos con la trama, excepto el puerto en el cual se la recibió.

El comportamiento de un switch de saturar direcciones MAC para las direcciones desconocidas se puede usar para atacar un switch. Este tipo de ataque se denomina “ataque de desbordamiento de la tabla de direcciones MAC”. En ocasiones, los ataques de desbordamiento de la tabla de direcciones MAC se denominan “ataques de saturación MAC” y “ataques de desbordamiento de la tabla CAM”. En las ilustraciones, se muestra cómo funciona este tipo de ataque.

En la figura 1, el host A envía tráfico al host B. El switch recibe las tramas y busca la dirección MAC de destino en la tabla de direcciones MAC. Si el switch no puede encontrar una MAC de destino en la tabla de direcciones MAC, este copia la trama y satura todos los puertos del switch con esta (la difunde), excepto el puerto en el cual se la recibió.

En la figura 2, el host B recibe la trama y envía una respuesta al host A. A continuación, el switch descubre que la dirección MAC del host B está ubicada en el puerto 2 y registra esa información en la tabla de direcciones MAC.

El host C también recibe la trama que va del host A al host B, pero debido a que la dirección MAC de destino de la trama es el host B, el host C la descarta.

Como se muestra en la figura 3, cualquier trama que envíe el host A (o cualquier otro host) al host B se reenvía al puerto 2 del switch y no se difunde por todos los puertos.

Las tablas de direcciones MAC poseen límite de tamaño. Los ataques de saturación MAC usan esta limitación para sobrecargar al switch con direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch esté completa.

Como se muestra en la figura 4, un atacante en el host C puede enviar tramas al switch con direcciones MAC de origen y destino falsas y generadas aleatoriamente. El switch actualiza la tabla de direcciones MAC con la información de las tramas falsas. Cuando la tabla de direcciones MAC está llena de direcciones MAC falsas, el switch entra en un modo que se conoce como modo “fail-open”. En este modo, el switch transmite todas las tramas a todas las máquinas en la red. Como resultado, el atacante puede ver todas las tramas.

Algunas herramientas de ataques de red pueden generar hasta 155 000 entradas de MAC por minuto en un switch. El tamaño máximo de la tabla de direcciones MAC varía en función del switch.

Como se muestra en la figura 5, mientras la tabla de direcciones MAC en el switch esté llena, el switch difunde todas las tramas recibidas por cada puerto. En este ejemplo, las tramas enviadas del host A al host B también se difunden por el puerto 3 del switch, y el atacante en el host C las puede ver.

Una forma de mitigar los ataques de desbordamiento de la tabla de direcciones MAC es configurar la seguridad de puertos.

DHCP es el protocolo que asigna automáticamente una dirección IP válida de un pool de DHCP a un host. En esta industria, el protocolo DHCP se usa hace casi tanto tiempo como TCP/IP como protocolo principal para asignar direcciones IP a los clientes. Se pueden realizar dos tipos de ataques DHCP a una red conmutada: los ataques de agotamiento de DHCP y los de suplantación de identidad de DHCP.

En los ataques de agotamiento de DHCP, un atacante satura el servidor de DHCP con solicitudes de DHCP para utilizar todas las direcciones IP disponibles que el servidor de DHCP puede emitir. Una vez que se emiten estas direcciones IP, el servidor no puede emitir más direcciones; esta situación produce un ataque por denegación de servicio (DoS), ya que los nuevos clientes no pueden obtener acceso a la red. Un ataque DoS es cualquier ataque que se usa para sobrecargar dispositivos y servicios de red específicos con tráfico ilegítimo, lo que impide que el tráfico legítimo llegue a esos recursos.

En los ataques de suplantación de identidad de DHCP, un atacante configura un servidor de DHCP falso en la red para emitir direcciones de DHCP para los clientes. El motivo común de este ataque es obligar a los clientes a que usen servidores de Sistema de nombres de dominios (DNS) o de Servicio de nombres Internet de Windows (WINS) falsos y hacer que los clientes usen al atacante, o una máquina controlada por el atacante, como gateway predeterminado.

El agotamiento de DHCP se suele utilizar antes de un ataque de suplantación de identidad de DHCP para denegar el servicio al servidor de DHCP legítimo, lo que facilita la introducción de un servidor de DHCP falso en la red.

Para mitigar los ataques de DHCP, se usan las características de detección de DHCP y de seguridad de puertos de los switches Cisco Catalyst. Estas características se abarcan más adelante en otro tema.

El protocolo de descubrimiento de Cisco (CDP, Cisco Discovery Protocol) es un protocolo propiedad de Cisco que puede configurarse en todos los dispositivos de Cisco. CDP detecta otros dispositivos de Cisco conectados directamente, lo que permite que los dispositivos configuren su conexión de forma automática. En algunos casos, esto simplifica la configuración y la conectividad.

De manera predeterminada, la mayoría de los routers y switches Cisco poseen CDP habilitado en todos los puertos. La información de CDP se envía en difusiones periódicas sin cifrar. Esta información se actualiza localmente en la base de datos de CDP de cada dispositivo. Debido a que CDP es un protocolo de capa 2, los routers no propagan los mensajes CDP.

CDP contiene información sobre el dispositivo, como la dirección IP, la versión de software del IOS, la plataforma, las capacidades y la VLAN nativa. Los atacantes pueden usar esta información para encontrar la forma de atacar la red, generalmente mediante ataques por denegación de servicio (DoS).

En la ilustración, se muestra una parte de una captura de Wireshark en la que se muestra el contenido de un paquete CDP. En particular, la versión de software IOS de Cisco descubierta por CDP permite que el atacante determine si existen vulnerabilidades de seguridad específicas para esa versión de IOS. Además, debido a que CDP no se autentica, los atacantes pueden crear paquetes CDP falsos y enviarlos a un dispositivo de Cisco conectado directamente.

Se recomienda inhabilitar el uso de CDP en los dispositivos o los puertos que no necesitan usarlo mediante el comando **no cdp run** del modo de configuración global. CDP se puede inhabilitar por puerto.

**Ataques de Telnet**

El protocolo Telnet es inseguro, y los atacantes lo pueden usar para acceder de manera remota a un dispositivo de red de Cisco. Existen herramientas que permiten que los atacantes inicien un ataque de decodificación de contraseñas por fuerza bruta contra las líneas vty del switch.

**Ataque de contraseña de fuerza bruta**

La primer fase de un ataque de contraseña de fuerza bruta comienza con el uso de contraseñas comunes por parte del atacante y de un programa diseñado para intentar establecer una sesión de Telnet mediante todas las palabras del diccionario. Si la contraseña no se descifra en la primera fase, comienza una segunda fase. En la segunda fase del ataque de fuerza bruta, el atacante usa un programa que genera combinaciones de caracteres secuenciales para poder adivinar la contraseña. Si dispone del tiempo suficiente, un ataque de contraseña de fuerza bruta puede decodificar casi todas las contraseñas utilizadas.

Para mitigar los ataques de contraseña de fuerza bruta, use contraseñas seguras y cámbielas con frecuencia. Una contraseña segura debe tener una combinación de mayúsculas y minúsculas, y debe incluir números y símbolos (caracteres especiales). El acceso a las líneas vty también se puede limitar mediante una lista de control de acceso (ACL).

**Ataque DoS por Telnet**

Telnet también se puede usar para iniciar un ataque DoS. En un ataque DoS por Telnet, el atacante explota un defecto del software del servidor Telnet que se ejecuta en el switch, el cual hace que el servicio de Telnet no esté disponible. Este tipo de ataque impide que un administrador acceda de manera remota a las funciones de administración del switch. Esto se puede combinar con otros ataques directos a la red como parte de un esfuerzo coordinado para impedir que el administrador de red acceda a dispositivos clave durante la infracción.

En general, las vulnerabilidades en el servicio de Telnet que permiten que ocurran los ataques de DoS se enfrentan mediante parches de seguridad incluidos en las revisiones más recientes de IOS de Cisco.

**Nota:** se recomienda usar SSH en lugar de Telnet para las conexiones de administración remota.

La defensa de la red contra ataques requiere vigilancia y capacitación. Las siguientes son prácticas recomendadas para proteger una red:

* Desarrolle una política de seguridad escrita para la organización.
* Desactive los servicios y puertos que no se utilicen.
* Utilice contraseñas seguras y cámbielas con frecuencia.
* Controle el acceso físico a los dispositivos.
* Evite usar sitios web HTTP estándar inseguros, especialmente para las pantallas de inicio de sesión; en lugar de esto, use HTTPS, que es más seguro.
* Realice copias de respaldo y pruébelas periódicamente.
* Capacite a los empleados sobre los ataques de ingeniería social y desarrolle políticas para validar identidades por teléfono, mediante correo electrónico y personalmente.
* Cifre y proteja con contraseñas los datos confidenciales.
* Implemente hardware y software de seguridad, como firewalls.
* Mantenga el software actualizado mediante la instalación semanal o mensual de parches de seguridad, si es posible.

Estos métodos son solo un punto de partida para la administración de la seguridad. Las organizaciones deben mantenerse alerta en todo momento para defenderse de estas amenazas en constante evolución. Use herramientas de seguridad de red para medir la vulnerabilidad de la red actual.

Las herramientas de seguridad de red ayudan al administrador de red a probar una red para detectar debilidades. Algunas herramientas permiten que el administrador asuma el rol de atacante. Mediante una de estas herramientas, el administrador puede iniciar un ataque contra la red y analizar los resultados para determinar cómo ajustar las políticas de seguridad a fin de mitigar esos tipos de ataques. Las auditorías de seguridad y los pruebas de penetración son dos funciones básicas que llevan a cabo las herramientas de seguridad de red.

El administrador puede iniciar manualmente las técnicas de prueba de seguridad de red. Otras pruebas están automatizadas en gran medida. Sin importar el tipo de prueba, el personal que configura y lleva a cabo las pruebas de seguridad debe tener un amplio conocimiento de seguridad y de redes. Esto incluye conocimientos en las siguientes áreas:

* Seguridad de la red
* Firewalls
* Sistemas de prevención de intrusiones
* Sistemas operativos
* Programación
* Protocolos de red (como TCP/IP)

Las herramientas de seguridad de red permiten que los administradores de red realicen auditorías de seguridad en una red. Una auditoría de seguridad revela el tipo de información que puede recopilar un atacante con un simple monitoreo del tráfico de la red.

Por ejemplo, las herramientas de auditoría de seguridad de red permiten que un administrador sature la tabla de direcciones MAC con direcciones MAC ficticias. A esto le sigue una auditoría de los puertos del switch a medida que este satura con tráfico todos los puertos. Durante la auditoría, las asignaciones de direcciones MAC legítimas vencen y se reemplazan por las asignaciones de direcciones MAC ficticias. Esto determina qué puertos están comprometidos y no están configurados correctamente para evitar este tipo de ataque.

El tiempo es un factor importante para realizar la auditoría de manera correcta. Los diferentes switches admiten distintas cantidades de direcciones MAC en sus tablas MAC. Puede resultar difícil determinar el número ideal de direcciones MAC suplantadas que se deben enviar al switch. Los administradores de red también deben enfrentar el período de vencimiento de la tabla de direcciones MAC. Si las direcciones MAC suplantadas comienzan a vencerse en el momento en que se realiza la auditoría de red, las direcciones MAC válidas comienzan a completar la tabla de direcciones MAC, lo que limita la cantidad de datos que pueden monitorearse con una herramienta de auditoría de red.

Las herramientas de seguridad de red también se pueden usar para realizar pruebas de penetración en la red. La prueba de penetración es un ataque simulado contra la red para determinar qué tan vulnerable sería en un ataque real. Esto permite que un administrador de red identifique debilidades en la configuración de los dispositivos de red y realice cambios para que los dispositivos sean más resistentes a los ataques. Los administradores pueden llevar a cabo una gran cantidad de ataques, y la mayoría de los conjuntos de herramientas vienen acompañados por documentación completa que detalla la sintaxis necesaria para ejecutar el ataque deseado.

Debido a que las pruebas de penetración pueden tener efectos adversos en la red, se llevan a cabo bajo condiciones muy controladas, respetando los procedimientos registrados que se detallan en una política de seguridad de red completa. Lo ideal es una red sin conexión que imite la red de producción real y funcione como banco de pruebas. El personal de redes puede usar la red del banco de pruebas para realizar pruebas de penetración en la red.

**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, este 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.

El snooping DHCP es una función que determina cuáles son los puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, incluidos los paquetes de oferta de DHCP y de acuse de recibo de DHCP; los puertos no confiables solo pueden recibir solicitudes. Los puertos confiables de los hosts se alojan en el servidor de DHCP o pueden ser un enlace hacia dicho servidor. Si un dispositivo no autorizado en un puerto no confiable intenta enviar un paquete de oferta de DHCP a la red, el puerto se desactiva. Esta función puede unirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP

Como se muestra en las figuras 1 y 2, los puertos no confiables son aquellos que no están configurados explícitamente como confiables. Se construye una tabla enlazada de DHCP para los puertos no confiables. Cada entrada contiene una dirección MAC cliente, una dirección IP, un tiempo de arrendamiento, un número de VLAN y una ID de puerto registrados como clientes que realizan solicitudes de DHCP. Se utiliza entonces la tabla para filtrar el tráfico de DHCP subsiguiente. Desde la perspectiva de la detección de DHCP, los puertos de acceso no confiables no deben enviar mensajes de servidor de DHCP.

Estos pasos describen la forma en que se configura la detección de DHCP en un switch Catalyst 2960:

**Paso 1.** Habilite la detección de DHCP mediante el comando **ip dhcp snooping** del modo de configuración global.

**Paso 2.** Habilite la detección de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan***número*.

**Paso 3.** Defina los puertos como confiables en el nivel de la interfaz mediante la identificación de los puertos confiables con el comando **ip dhcp snooping trust**.

**Paso 4.** (Optativo) Limite la velocidad a la que un atacante puede enviar solicitudes de DHCP falsas de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate*velocidad***.

**Seguridad del puerto**

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. En la figura 1, se resumen estos puntos.

**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* 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 direcciones MAC seguras persistentes mediante el comando **switchport port-security mac-address sticky***dirección-mac* del modo de configuración de interfaz, 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.

En la figura 2, se muestran las características de las direcciones MAC seguras persistentes.

Observe que la característica de seguridad de puertos no funciona hasta que se habilita la seguridad de puertos en la interfaz mediante el comando **switchport port-security**.

Existe una violación de seguridad cuando se produce cualquiera de estas situaciones:

* Se agregó la cantidad máxima de direcciones MAC seguras a la tabla de direcciones para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.
* Una dirección aprendida o configurada en una interfaz segura puede verse en otra interfaz segura de la misma VLAN.

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 de violación (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 hay un puerto seguro en estado inhabilitado por errores, se lo puede sacar de dicho estado mediante la introducción de los comandos **shutdown** y **no shutdown** del modo de configuración de interfaz.

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**}.

En la figura 1, se resume la configuración predeterminada de seguridad de puerto en un switch Cisco Catalyst.

En la figura 2, se muestran los comandos de CLI de Cisco IOS necesarios para configurar la seguridad de puertos en el puerto Fast Ethernet F0/18 del switch S1. Observe que el ejemplo no especifica un modo de violación. En este ejemplo, el modo de violación es shutdown, el modo predeterminado.

En la figura 3, se muestra cómo habilitar las direcciones MAC seguras persistentes para la seguridad de puertos en el puerto Fast Ethernet 0/19 del switch S1. Como se mencionó anteriormente, la cantidad máxima de direcciones MAC seguras se puede configurar de forma manual. En este ejemplo, la sintaxis del comando de Cisco IOS se utiliza para establecer en 10 la cantidad máxima de direcciones MAC para el puerto 0/19. De manera predeterminada, el modo de violación se establece en shutdown.

**Verificar la seguridad de 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 de puerto**

Para mostrar la configuración de seguridad de puertos para el switch o la interfaz especificada, use el comando **show port-security [interface***ID-de-interfaz***]**. El resultado de la configuración de la seguridad del puerto dinámico se muestra en la figura 1. De manera predeterminada, se permite una dirección MAC en este puerto.

El resultado que se muestra en la figura 2 muestra los valores de la configuración de seguridad del puerto persistente. La cantidad máxima de direcciones se estableció en 10, como se configuró.

**Nota:** la dirección MAC se identifica como sticky MAC (MAC persistente).

Las direcciones MAC persistentes se agregan a la tabla de direcciones MAC y a la configuración en ejecución. Como se muestra en la figura 3, la dirección MAC persistente de la PC2 se agregó a la configuración en ejecución para S1.

**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**. Como se muestra en la figura 4, las direcciones MAC seguras se indican junto con los tipos.

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 envía ni se recibe tráfico en ese puerto. En la consola (figura 1), se muestra una serie de mensajes relacionados con la seguridad del puerto.

**Nota:** el estado del enlace y del protocolo del puerto cambia a down (inactivo).

El LED del puerto cambia a color naranja. El comando **show interfaces**identifica el estado del puerto como **err-disabled** (figura 2). El resultado del comando **show port-security interface** ahora muestra el estado del puerto como **secure-shutdown**. Debido a que el modo de violación de seguridad de puertos está establecido en shutdown, el puerto que experimenta la violación de seguridad pasa al estado de inhabilitación por errores.

El administrador debe determinar la causa de la violación de seguridad antes de volver a habilitar el puerto. Si hay un dispositivo no autorizado conectado a un puerto seguro, el puerto no se debe volver a habilitar hasta que se elimine la amenaza de seguridad. Para volver a habilitar el puerto, use el comando**shutdown** del modo de configuración de interfaz (figura 3). Luego, use el comando**no shutdown** del modo de configuración de interfaz para que el puerto funcione.

Es importante tener la hora correcta dentro de las redes. Se requieren marcas de tiempo correctas para hacer un seguimiento preciso de los eventos de red, como las violaciones de seguridad. Además, la sincronización de relojes es fundamental para la interpretación correcta de los eventos dentro de los archivos de datos syslog, así como para los certificados digitales.

El protocolo NTP se usa para sincronizar los relojes de los sistemas de computación de las redes de datos conmutadas por paquetes de latencia variable. NTP permite que los dispositivos de red sincronicen la configuración de la hora con un servidor NTP. Un grupo de clientes NTP que obtienen información de fecha y hora de un único origen tiene una configuración de tiempo más coherente.

Un método seguro para proporcionar sincronización a la red es que los administradores implementen sus propios relojes maestros de red privada, sincronizados en UTC, mediante satélite o radio. Sin embargo, si los administradores de red no desean implementar sus propios relojes maestros debido al costo o a otros motivos, existen otros orígenes de reloj disponibles en Internet. NTP puede obtener la hora correcta de un origen de hora interno o externo, incluidos los siguientes:

* Reloj maestro local
* Reloj maestro en Internet
* GPS o reloj atómico

Los dispositivos de red se pueden configurar como servidor NTP o cliente NTP. Para permitir que un servidor horario NTP sincronice el reloj del software, use el comando **ntp server***dirección-IP* del modo de configuración global. En la figura 1, se muestra un ejemplo de configuración. El router R2 está configurado como cliente NTP, mientras que el router R1 funciona como servidor NTP autoritativo.

Para configurar un dispositivo con un reloj maestro NTP con el que los peers se puedan sincronizar, use el comando **ntp master [***capa***]** del modo de configuración global. El valor de capa es un número que va de 1 a 15 e indica el número de capa NTP que informa el sistema. Si el sistema está configurado como reloj maestro NTP y no se especifica ningún número de capa, se establece la capa 8 de manera predeterminada. Si el reloj maestro NTP no llega a ningún reloj con un número de capa más bajo, el sistema informa que está sincronizado en el número de capa configurado, y otros sistemas estarán dispuestos a sincronizarse con él mediante NTP.

En la figura 2, se muestra la verificación de NTP. Para mostrar el estado de las asociaciones NTP, use el comando **show ntp associations** del modo EXEC privilegiado. Este comando indica la dirección IP de cualquier dispositivo peer sincronizado a este peer, los peers configurados de forma estática y el número de capa. El comando **show ntp status** del modo EXEC de usuario se puede utilizar para mostrar información como el estado de la sincronización de NTP, el peer con el que el dispositivo está sincronizado y las capas NTP en las que funciona el dispositivo.

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 ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al 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.

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 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 full-duplex 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 del switch es un requisito para evitar los ataques como la saturación de direcciones MAC y la suplantación de identidad de DHCP. Los puertos de switch se deben configurar para permitir que ingresen solo las tramas con direcciones MAC de origen específicas. Se deben rechazar las direcciones MAC de origen desconocidas, y se debe desactivar el puerto para evitar otros ataques.

La seguridad de puertos es solo uno de los métodos de defensa contra los riesgos que puede sufrir la red. Existen 10 prácticas recomendadas que representan los métodos más seguros para una red:

* Desarrolle una política de seguridad escrita para la organización.
* Desactive los servicios y puertos que no se utilicen.
* Utilice contraseñas seguras y cámbielas con frecuencia.
* Controle el acceso físico a los dispositivos.
* Evite usar sitios web HTTP estándar inseguros, especialmente para las pantallas de inicio de sesión. En lugar de esto, use HTTPS, que es más seguro.
* Realice copias de respaldo y pruébelas periódicamente.
* Capacite a los empleados sobre los ataques de ingeniería social y desarrolle políticas para validar identidades por teléfono, mediante correo electrónico y personalmente.
* Cifre los datos confidenciales y protéjalos con una contraseña segura.
* Implemente hardware y software de seguridad, como firewalls.
* Mantenga el software IOS actualizado mediante la instalación semanal o mensual de parches de seguridad, si es posible.

Estos métodos son solo un punto de partida para la administración de la seguridad. Las organizaciones deben mantenerse alerta en todo momento para defenderse de estas amenazas en constante evolución.