Ejemplo de Configuración de las Funciones de Seguridad de Capa 2 en los Switches de Configuración Fija de Capa 3 de Cisco Catalyst

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de algunas de las funciones de seguridad de Capa 2, tales como seguridad de puerto, snooping de DHCP, inspección de Address Resolution Protocol (ARP) dinámico y Protección de origen IP, que se pueden implementar en los switches de configuración fija Cisco Catalyst Layer 3.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco Catalyst 3750 Series Switch con la versión 12.2(25)SEC2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede utilizar con estos hardware:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Switches Cisco Catalyst serie 3560-E
- Switches Cisco Catalyst serie 3750-E

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Al igual que los routers, tanto los switches de capa 2 como de capa 3 tienen sus propios conjuntos de requisitos de seguridad de red. Los switches son susceptibles a muchos de los mismos ataques de Capa 3 que los routers. Sin embargo, los switches y la Capa 2 del modelo de referencia OSI en general, están sujetos a ataques de red de diferentes maneras. Estos incluyen:

- **Desbordamiento de tabla de memoria direccionable de contenido (CAM)**Las tablas de la Memoria direccionable de contenido (CAM) tienen un tamaño limitado. Si se ingresan suficientes entradas en la tabla CAM antes de que caduquen otras entradas, la tabla CAM se llena hasta el punto de que no se pueden aceptar nuevas entradas. Normalmente, un intruso de red inunda el switch con un gran número de direcciones MAC (Control de acceso a medios) de origen no válidas hasta que se completa la tabla CAM. Cuando esto ocurre, el switch inunda todos los puertos con tráfico entrante porque no puede encontrar el número de puerto para una dirección MAC determinada en la tabla CAM. El switch, en esencia, actúa como un concentrador. Si el intruso no mantiene la inundación de direcciones MAC de origen no válidas, el switch eventualmente desconecta las entradas de dirección MAC más antiguas de la tabla CAM y comienza a actuar como un switch de nuevo. El desbordamiento de la tabla CAM sólo inunda el tráfico dentro de la VLAN local, por lo que el intruso sólo ve el tráfico dentro de la VLAN local a la que está conectado.El ataque de desbordamiento de la tabla CAM se puede mitigar mediante la configuración de la seguridad del puerto en el switch. Esta opción proporciona la especificación de las direcciones MAC en un puerto de switch determinado o la especificación del número de direcciones MAC que puede aprender un puerto de switch. Cuando se detecta una dirección MAC no válida en el puerto, el switch puede bloquear la dirección MAC infractora o apagar el puerto. La especificación de las direcciones MAC en los puertos del switch es una solución demasiado inmanejable para un entorno de producción. Se puede administrar un límite del número de direcciones MAC en un puerto de switch. Una solución más escalable desde el punto de vista administrativo es la implementación de la seguridad dinámica de los puertos en el switch. Para implementar la seguridad de puerto dinámico, especifique un número máximo de direcciones MAC que se

aprenderán.

- **Suplantación de dirección de control de acceso a medios (MAC)**Los ataques de suplantación de Media Access Control (MAC) implican el uso de una dirección MAC conocida de otro host para intentar hacer que el switch de destino reenvíe las tramas destinadas al host remoto al atacante de red. Cuando se envía una única trama con la dirección Ethernet de origen del otro host, el atacante de red sobrescribe la entrada de la tabla CAM para que el switch reenvíe los paquetes destinados al host al atacante de red. Hasta que el host envía tráfico, no recibe tráfico alguno. Cuando el host envía tráfico, la entrada de la tabla CAM se reescribe una vez más para que se traslade de vuelta al puerto original.Utilice la función de seguridad de puertos para mitigar los ataques de suplantación de MAC. La seguridad de puerto proporciona la capacidad de especificar la dirección MAC del sistema conectado a un puerto determinado. Esto también proporciona la capacidad de especificar una acción que realizar si se produce una violación de la seguridad de puerto.
- **Suplantación de protocolo de resolución de direcciones (ARP)**ARP se utiliza para asignar direcciones IP a direcciones MAC en un segmento de red de área local donde residen los hosts de la misma subred. Normalmente, un host envía una solicitud ARP de broadcast para encontrar la dirección MAC de otro host con una dirección IP determinada, y una respuesta ARP viene del host cuya dirección coincide con la solicitud. El host solicitante luego almacena en memoria caché esta respuesta ARP. Dentro del protocolo ARP, se hace otra provisión para que los hosts realicen respuestas ARP no solicitadas. Las respuestas ARP no solicitadas se denominan ARP Gratuitous (GARP). Un atacante puede explotar maliciosamente GARP para falsificar la identidad de una dirección IP en un segmento LAN. Esto se utiliza normalmente para simular la identidad entre dos hosts o todo el tráfico hacia y desde un gateway predeterminado en un ataque de "man-in-the-middle" (hombre en el medio).Cuando se crea una respuesta ARP, un atacante de red puede hacer que su sistema parezca ser el host de destino buscado por el remitente. La respuesta ARP hace que el remitente almacene la dirección MAC del sistema del atacante de red en la memoria caché ARP. El switch también almacena esta dirección MAC en su tabla CAM. De esta manera, el atacante de red ha insertado la dirección MAC de su sistema tanto en la tabla CAM del switch como en la memoria caché ARP del remitente. Esto permite al atacante de red interceptar tramas destinadas al host que está simulando.Los temporizadores de espera en el menú de configuración de la interfaz se pueden utilizar para mitigar los ataques de suplantación ARP estableciendo el tiempo que una entrada permanecerá en la memoria caché ARP. Sin embargo, los temporizadores de retención por sí mismos son insuficientes. Se requiere la modificación del tiempo de vencimiento de la memoria caché ARP en todos los sistemas extremos, así como las entradas ARP estáticas. Otra solución que se puede utilizar para mitigar diversas vulnerabilidades de red basadas en ARP es el uso de snooping DHCP junto con la inspección dinámica ARP. Estas funciones de Catalyst validan los paquetes ARP en una red y permiten la intercepción, registro y descarte de paquetes ARP con direcciones MAC inválidas a vinculaciones de direcciones IP.La indagación DHCP filtra los mensajes DHCP confiables para proporcionar seguridad. Luego, estos mensajes se utilizan para generar y mantener una tabla de enlace de indagación DHCP. La indagación DHCP considera que los mensajes DHCP que se originan en cualquier puerto orientado al usuario que no es un puerto del servidor DHCP no son de confianza. Desde la perspectiva de la indagación DHCP, estos puertos no confiables orientados al usuario no deben enviar respuestas de tipo de servidor DHCP, como DHCPOFFER, DHCPACK o DHCPNAK. La tabla de enlace de snooping DHCP contiene la dirección MAC, la dirección IP, el tiempo de concesión, el tipo de enlace, el número de VLAN y la información de interfaz que corresponde a las interfaces locales no

confiables de un switch. La tabla de enlace de snooping DHCP no contiene información sobre los hosts interconectados con una interfaz de confianza. Una interfaz no fiable es una interfaz configurada para recibir mensajes desde fuera de la red o del firewall. Una interfaz de confianza es una interfaz configurada para recibir sólo mensajes desde dentro de la red. La tabla de enlace de indagación DHCP puede contener enlaces de dirección MAC dinámica y estática a dirección IP.La inspección ARP dinámica determina la validez de un paquete ARP basándose en las vinculaciones de dirección MAC a dirección IP válidas almacenadas en una base de datos de indagación DHCP. Además, la inspección ARP dinámica puede validar los paquetes ARP en función de las listas de control de acceso (ACL) configurables por el usuario. Esto permite la inspección de paquetes ARP para hosts que utilizan direcciones IP configuradas estáticamente. La inspección dinámica de ARP permite el uso de listas de control de acceso por puerto y VLAN (PACL) para limitar los paquetes ARP para direcciones IP específicas a direcciones MAC específicas.

- **Inicio de protocolo de configuración dinámica de host (DHCP)**Un ataque de inanición de DHCP funciona mediante la difusión de solicitudes DHCP con direcciones MAC simuladas. Si se envían suficientes solicitudes, el atacante de red puede agotar el espacio de direcciones disponible para los servidores DHCP durante un período de tiempo. El atacante de red puede entonces configurar un servidor DHCP no autorizado en su sistema y responder a las nuevas solicitudes DHCP de los clientes en la red. Con la colocación de un servidor DHCP no autorizado en la red, un atacante de red puede proporcionar a los clientes direcciones y otra información de red. Debido a que las respuestas DHCP suelen incluir la información predeterminada del gateway y del servidor DNS, el atacante de red puede suministrar su propio sistema como la gateway predeterminada y el servidor DNS. Esto da lugar a un ataque de intermediarios. Sin embargo, el agotamiento de todas las direcciones DHCP no es necesario para introducir un servidor DHCP no autorizado.Las funciones adicionales de la familia de switches Catalyst, como la indagación DHCP, se pueden utilizar para ayudar a proteger contra un ataque de inanición de DHCP. La indagación DHCP es una función de seguridad que filtra los mensajes DHCP no confiables y genera y mantiene una tabla de enlace de indagación DHCP. La tabla de enlace contiene información como la dirección MAC, la dirección IP, el tiempo de concesión, el tipo de enlace, el número de VLAN y la información de interfaz que corresponde a las interfaces locales no confiables de un switch. Los mensajes no fiables son aquellos recibidos desde fuera de la red o del firewall. Las interfaces de switch no confiables son aquellas configuradas para recibir dichos mensajes desde fuera de la red o del firewall.Otras funciones del switch Catalyst, como IP source guard, pueden proporcionar una defensa adicional contra ataques como la inanición de DHCP y la suplantación de IP. Al igual que la indagación DHCP, la protección de origen IP está habilitada en puertos de capa 2 no confiables. Todo el tráfico IP se bloquea inicialmente, excepto los paquetes DHCP capturados por el proceso de indagación DHCP. Una vez que un cliente recibe una dirección IP válida del servidor DHCP, se aplica una PACL al puerto. Esto restringe el tráfico IP del cliente a las direcciones IP de origen configuradas en el enlace. Se filtra cualquier otro tráfico IP con una dirección de origen distinta de las direcciones del enlace.

Configurar

En esta sección, se le presenta la información para configurar las funciones de seguridad de puerto, detección DHCP, inspección ARP dinámica y seguridad de IP Source Guard.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

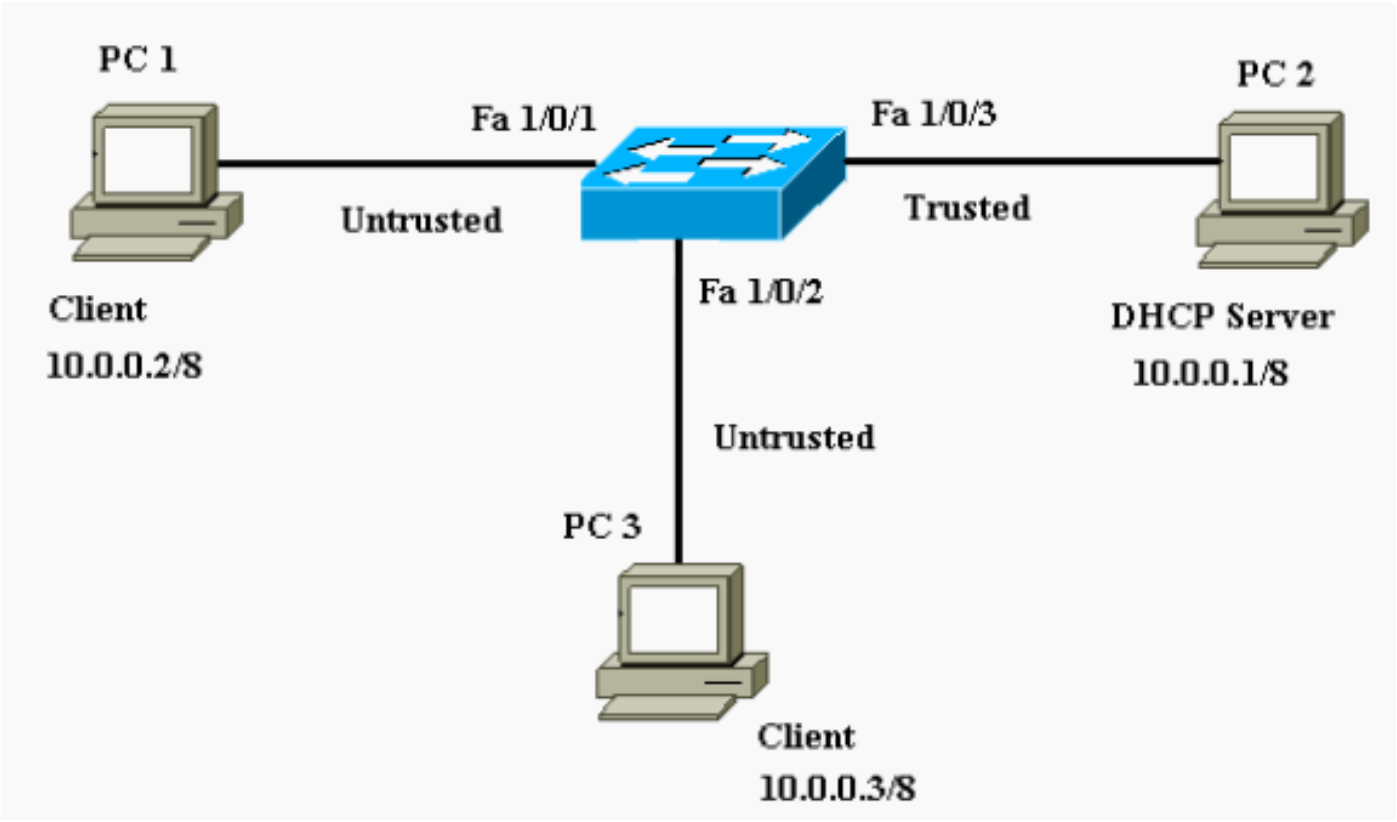
Las configuraciones del Catalyst 3750 Switch contienen lo siguiente:

- Seguridad de Puertos
- Detección de DHCP
- Dynamic ARP Inspection
- IP Source Guard

Diagrama de la red

En este documento, se utiliza esta configuración de red:

- PC 1 y PC 3 son clientes conectados al switch.
- PC 2 es un servidor DHCP conectado al switch.
- Todos los puertos del switch se encuentran en la misma VLAN (VLAN 1).
- El servidor DHCP se configura para asignar direcciones IP a los clientes en función de sus direcciones MAC.



Seguridad de Puertos

Puede utilizar la función de seguridad del puerto para limitar e identificar las direcciones MAC de las estaciones a las que se permite el acceso al puerto. Esto restringe la entrada a una interfaz. Cuando asigna direcciones MAC seguras a un puerto seguro, el puerto no reenvía paquetes con direcciones de origen fuera del grupo de direcciones definidas. Si limita el número de direcciones MAC seguras a una y asigna una única dirección MAC segura, la estación de trabajo conectada a ese puerto estará asegurada del ancho de banda completo del puerto. Si un puerto se configura como puerto seguro y se alcanza el número máximo de direcciones MAC seguras, cuando la dirección MAC de una estación que intenta acceder al puerto es diferente de cualquiera de las

direcciones MAC seguras identificadas, se produce una violación de la seguridad. Además, si una estación con una dirección MAC segura configurada o aprendida en un puerto seguro intenta acceder a otro puerto seguro, se marca una violación. De forma predeterminada, el puerto se apaga cuando se supera el número máximo de direcciones MAC seguras.

Nota: Cuando un Catalyst 3750 Switch se une a una pila, el nuevo switch recibe las direcciones seguras configuradas. El nuevo miembro de la pila descargará todas las direcciones seguras dinámicas de los demás miembros de la pila.

Consulte Pautas de Configuración para ver las pautas sobre cómo configurar la seguridad de puerto.

Aquí, se muestra la función de seguridad de puerto configurada en la interfaz FastEthernet 1/0/2. De forma predeterminada, el número máximo de direcciones MAC seguras para la interfaz es uno. Puede ejecutar el comando **show port-security interface** para verificar el estado de seguridad del puerto para una interfaz.

Seguridad de Puertos

```
Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
!--- Default port security configuration on the switch.
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#interface fastEthernet 1/0/2
Cat3750(config-if)#switchport port-security
Command rejected: FastEthernet1/0/2 is a dynamic port.
!--- Port security can only be configured on static
access ports or trunk ports. Cat3750(config-
if)#switchport mode access
!--- Sets the interface switchport mode as access.
Cat3750(config-if)#switchport port-security
!--- Enables port security on the interface.
Cat3750(config-if)#switchport port-security mac-address
0011.858D.9AF9
!--- Sets the secure MAC address for the interface.
Cat3750(config-if)#switchport port-security violation
shutdown
!--- Sets the violation mode to shutdown. This is the
default mode. Cat3750# !--- Connected a different PC (PC
4) to the FastEthernet 1/0/2 port !--- to verify the
port security feature. 00:22:51: %PM-4-ERR_DISABLE:
psecure-violation error detected on Fa1/0/2, putting
Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on
```

```
Interface FastEthernet1/0/2, changed state to down
00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2,
changed state to down !--- Interface shuts down when a
security violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2
FastEthernet1/0/2 is down, line protocol is down (err-
disabled)
!--- Output Suppressed. !--- The port is shown error-
disabled. This verifies the configuration. !--- Note:
When a secure port is in the error-disabled state, !---
you can bring it out of this state by entering !--- the
errdisable recovery cause psecure-violation global
configuration command, !--- or you can manually re-
enable it by entering the !--- shutdown and no shutdown
interface configuration commands.


Cat3750#show port-security interface fastEthernet 1/0/2
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0011.8565.4B75:1
Security Violation Count   : 1
```

Nota: Las mismas direcciones MAC no deben configurarse como direcciones MAC seguras y estáticas en diferentes puertos de un switch.

Cuando un teléfono IP se conecta a un switch a través del switchport configurado para la VLAN de voz, el teléfono envía paquetes CDP sin etiqueta y paquetes CDP de voz etiquetados. Por lo tanto, la dirección MAC del teléfono IP se detecta tanto en el PVID como en el VVID. Si no se configura el número adecuado de direcciones seguras, puede obtener un mensaje de error similar a este mensaje:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

Debe establecer el número máximo de direcciones seguras permitidas en el puerto en dos (para el teléfono IP) más el número máximo de direcciones seguras permitidas en la VLAN de acceso para resolver este problema.

Refiérase a Configuración de la Seguridad del Puerto para obtener más información.

Detección de DHCP

El snooping de DHCP actúa como un firewall entre hosts no confiables y servidores DHCP. El snooping de DHCP se utiliza para diferenciar entre las interfaces no confiables conectadas al usuario final y las interfaces de confianza conectadas al servidor DHCP u otro switch. Cuando un switch recibe un paquete en una interfaz no confiable y la interfaz pertenece a una VLAN que tiene la indagación DHCP habilitada, el switch compara la dirección MAC de origen y la dirección de hardware del cliente DHCP. Si las direcciones coinciden (el valor predeterminado), el switch

reenvía el paquete. Si las direcciones no coinciden, el switch descarta el paquete. El switch descarta un paquete DHCP cuando ocurre una de estas situaciones:

- Un paquete de un servidor DHCP, como un paquete DHCPOFFER, DHCPACK, DHCPNAK o DHCPLEASEQUERY, se recibe desde fuera de la red o del firewall.
- Se recibe un paquete en una interfaz no confiable y la dirección MAC de origen y la dirección de hardware del cliente DHCP no coinciden.
- El switch recibe un mensaje de broadcast DHCPRELEASE o DHCPDECLINE que tiene una dirección MAC en la base de datos de enlace de snooping DHCP, pero la información de la interfaz en la base de datos de enlace no coincide con la interfaz en la que se recibió el mensaje.
- Un agente de relé DHCP reenvía un paquete DHCP, que incluye una dirección IP de agente relay que no es 0.0.0.0, o el agente relay reenvía un paquete que incluye información de la opción 82 a un puerto no confiable.

Consulte Pautas de Configuración de Indagación DHCP para obtener instrucciones sobre cómo configurar la indagación DHCP.

Nota: Para que el snooping DHCP funcione correctamente, todos los servidores DHCP deben estar conectados al switch a través de interfaces de confianza.

Nota: En una pila de switches con switches Catalyst 3750, la indagación DHCP se administra en el maestro de la pila. Cuando un nuevo switch se une a la pila, el switch recibe la configuración de indagación DHCP del maestro de la pila. Cuando un miembro abandona la pila, todos los enlaces de indagación DHCP asociados con el switch caducan.

Nota: Para asegurarse de que el tiempo de arrendamiento en la base de datos es preciso, Cisco recomienda que habilite y configure NTP. Si se configura NTP, el switch escribe cambios de enlace en el archivo de enlace sólo cuando el reloj del sistema del switch está sincronizado con NTP.

Los servidores DHCP sospechosos pueden mitigarse mediante las funciones de snooping DHCP. El comando **ip dhcp snooping** se ejecuta para habilitar DHCP globalmente en el switch. Cuando se configuran con snooping DHCP, todos los puertos en la VLAN no son confiables para las respuestas DHCP. Aquí, sólo la interfaz FastEthernet 1/0/3 conectada al servidor DHCP está configurada como confiable.

Detección de DHCP

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1
!--- DHCP snooping is not active until DHCP snooping is
enabled on a VLAN. Cat3750(config)#no ip dhcp snooping
information option
!--- Disable the insertion and removal of the option-82
field, if the !--- DHCP clients and the DHCP server
reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip dhcp snooping
```

```
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit
(pps)
------------------------     -------     ---------------
-
FastEthernet1/0/3            yes         unlimited
!--- Displays the DHCP snooping configuration for the
switch. Cat3750#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
VLAN  Interface
------------------  ---------------  ----------  -------
------  ----  --------------------
00:11:85:A5:7B:F5     10.0.0.2        86391       dhcp-
snooping  1    FastEtheret1/0/1
00:11:85:8D:9A:F9     10.0.0.3        86313       dhcp-
snooping  1    FastEtheret1/0/2
Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

Refiérase a Configuración de Funciones DHCP para obtener más información.

Dynamic ARP Inspection

La inspección ARP dinámica es una función de seguridad que valida los paquetes ARP en una red. Intercepta, registra y descarta paquetes ARP con vinculaciones de dirección IP a MAC no válidas. Esta capacidad protege la red de ciertos ataques de intrusos.

La inspección ARP dinámica garantiza que sólo se retransmitan las solicitudes y respuestas ARP válidas. El switch realiza estas actividades:

- Intercepta todas las solicitudes y respuestas ARP en puertos no confiables
- Verifica que cada uno de estos paquetes interceptados tenga un enlace de dirección IP a MAC válido antes de que actualice la memoria caché ARP local o antes de que reenvíe el paquete al destino apropiado
- Descarta paquetes ARP no válidos

La inspección ARP dinámica determina la validez de un paquete ARP basándose en las vinculaciones de dirección IP a MAC válidas almacenadas en una base de datos de confianza, la base de datos de enlace de indagación DHCP. Esta base de datos se genera mediante la indagación DHCP si la indagación DHCP está habilitada en las VLAN y en el switch. Si el paquete ARP se recibe en una interfaz de confianza, el switch reenvía el paquete sin ninguna verificación. En las interfaces no confiables, el switch reenvía el paquete sólo si es válido.

En los entornos no DHCP, la inspección ARP dinámica puede validar los paquetes ARP contra las ACL ARP configuradas por el usuario para los hosts con direcciones IP configuradas estáticamente. Puede ejecutar el comando de configuración global **arp access-list** para definir una ACL ARP. Las ACL ARP tienen prioridad sobre las entradas en la base de datos de enlace de indagación DHCP. El switch utiliza las ACL sólo si ejecuta el comando de configuración global **ip arp inspection filter vlan** para configurar las ACL. El switch compara primero los paquetes ARP

con las ACL ARP configuradas por el usuario. Si la ACL ARP niega el paquete ARP, el switch también niega el paquete incluso si existe un enlace válido en la base de datos poblada por la indagación DHCP.

Consulte Pautas de Configuración de Inspección ARP Dinámica para ver las pautas sobre cómo configurar la inspección ARP dinámica.

El comando de configuración global **ip arp inspection vlan** se ejecuta para habilitar la inspección dinámica ARP por VLAN. Aquí, sólo la interfaz FastEthernet 1/0/3 conectada al servidor DHCP se configura como confiable con el comando **ip arp inspection trust**. El snooping DHCP debe estar habilitado para permitir los paquetes ARP que tienen direcciones IP asignadas dinámicamente. Vea la sección Indagación DHCP de este documento para obtener información de configuración de indagación DHCP.

Dynamic ARP Inspection

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1
!--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust
!--- Configures the interface connected to the DHCP
server as trusted. Cat3750#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match
Static ACL
 ----     -------------    ---------   ---------
----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
!--- Verifies the dynamic ARP inspection configuration.
Cat3750#
```

Consulte Configuración de la Inspección ARP Dinámica para obtener más información.

IP Source Guard

La protección de origen IP es una función de seguridad que filtra el tráfico basado en la base de datos de enlace de indagación DHCP y en los enlaces de origen IP configurados manualmente para restringir el tráfico IP en las interfaces de Capa 2 no enrutadas. Puede utilizar la protección de origen IP para evitar los ataques de tráfico causados cuando un host intenta utilizar la dirección IP de su vecino. La protección de origen de IP evita la suplantación de IP/MAC.

Puede habilitar la protección de origen IP cuando la indagación DHCP está habilitada en una interfaz no confiable. Después de que la protección de origen de IP esté habilitada en una interfaz, el switch bloquea todo el tráfico IP recibido en la interfaz, excepto los paquetes DHCP permitidos por la indagación DHCP. Se aplica una ACL de puerto a la interfaz. La ACL de puerto

permite solamente el tráfico IP con una dirección IP de origen en la tabla de enlace de origen IP y niega el resto del tráfico.

La tabla de enlace de origen IP tiene vinculaciones aprendidas por la indagación DHCP o configuradas manualmente (vinculaciones de origen IP estáticas). Una entrada en esta tabla tiene una dirección IP, su dirección MAC asociada y su número VLAN asociado. El switch utiliza la tabla de enlace de origen IP solamente cuando la protección de origen IP está habilitada.

Puede configurar la protección de origen IP con el filtrado de direcciones IP de origen o con el filtrado de direcciones IP y MAC de origen. Cuando la protección de origen de IP se habilita con esta opción, el tráfico IP se filtra en función de la dirección IP de origen. El switch reenvía el tráfico IP cuando la dirección IP de origen coincide con una entrada en la base de datos de enlace de snooping DHCP o con un enlace en la tabla de enlace de origen IP. Cuando la protección de origen de IP se habilita con esta opción, el tráfico IP se filtra en función de las direcciones IP y MAC de origen. El switch reenvía el tráfico solamente cuando las direcciones IP y MAC de origen coinciden con una entrada en la tabla de enlace de origen IP.

Nota: La protección de origen IP se soporta solamente en los puertos de Capa 2, que incluye el acceso y los puertos trunk.

Consulte Pautas de Configuración de IP Source Guard para obtener instrucciones sobre cómo configurar IP Source Guard.

Aquí, el protector de origen IP con filtrado IP de origen se configura en la interfaz FastEthernet 1/0/1 con el comando **ip verify source**. Cuando la protección de origen IP con el filtrado IP de origen está habilitada en una VLAN, la indagación DHCP debe estar habilitada en la VLAN de acceso a la que pertenece la interfaz. Ejecute el comando **show ip verify source** para verificar la configuración de IP source guard en el switch.

IP Source Guard

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1
!--- See the DHCP Snooping section of this document for
!--- DHCP snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source
!--- Enables IP source guard with source IP filtering.
Cat3750#show ip verify source
Interface  Filter-type  Filter-mode  IP-address
Mac-address        Vlan
---------  -----------  -----------  ---------------  --
---------------  -----
Fa1/0/1    ip           active       10.0.0.2
1
!--- For VLAN 1, IP source guard with IP address
filtering is configured !--- on the interface and a
binding exists on the interface. Cat3750#
```

Refiérase a Comprensión de IP Source Guard para obtener más información.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cómo asegurar redes con una VLAN privada y listas de control de acceso de VLAN
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems