Funciones de seguridad de la capa 2 en el ejemplo de configuración de los switches de configuración fija de la capa 3 del Cisco Catalyst

Contenido

Introducción

Este documento proporciona una configuración de muestra para algunas de las funciones de seguridad de la capa 2, tales como Seguridad de puerto, snooping del DHCP, examen del Address Resolution Protocol (ARP) dinámico y Protección de origen IP, que se pueden implementar en los switches de configuración fija de la capa 3 del Cisco Catalyst.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con estos hardwares:

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

Convenciones

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

Antecedentes

Similar al Routers, acode 2 y los switches de la capa 3 tienen sus propios conjuntos de los requisitos de seguridad de la red. El Switches es susceptible a muchos de los mismos ataques de la capa 3 que el Routers. Sin embargo, el Switches y acoda 2 del OSI Reference Model está generalmente conforme a los ataques a la red en las maneras diferentes. Estos incluyen:

- **Desbordamiento de la tabla del Content Addressable Memory (CAM)**Las tablas del Content Addressable Memory (CAM) se limitan de tamaño. Si bastantes entradas se ingresan en la tabla CAM antes de que se expiren otras entradas, la tabla CAM llena hasta la punta que ningunas nuevas entradas pueden ser validadas. Típicamente, un intruso de la red inunda el Switch con un gran número de Media Access Control (MAC) Address del origen no válido hasta la tabla CAM se llena. Cuando ocurre eso, el Switch inunda todos los puertos con el tráfico entrante porque no puede encontrar el número del puerto para un MAC Address determinado en la tabla CAM. El Switch, esencialmente, actúa como un concentrador. Si el intruso no mantiene la inundación de las direcciones MAC del origen no válido, el Switch mide el tiempo eventual hacia fuera de más viejas entradas de MAC Address de la tabla CAM y comienza a actuar como un Switch otra vez. Las inundaciones del desbordamiento de la tabla CAM solamente trafican dentro del VLA N local así que el intruso ve solamente el tráfico dentro del VLA N local con el cual él o ella está conectado.El ataque del desbordamiento de la tabla CAM puede ser atenuado configurando la Seguridad de puerto en el Switch. Esta opción prevé la especificación de las direcciones MAC en un puerto del switch determinado o la especificación del número de direcciones MAC que se puedan aprender por un puerto del switch. Cuando un MAC Address inválido se detecta en el puerto, el Switch puede bloquear el MAC address que ofende o apagar el puerto. La especificación de las direcciones MAC en los puertos del switch es una solución demasiado unmanageable lejana para un entorno de producción. Un límite del número de direcciones MAC en un puerto del switch es manejable. Más administrativo una solución escalable es la implementación de la Seguridad de puerto dinámico en el Switch. Para implementar la Seguridad de puerto dinámico, especifique un

número máximo de MAC Addresses que sea docto.

- **Spoofing del Media Access Control (MAC) Address**Los ataques de simulación del Media Access Control (MAC) implican el uso de un MAC address sabido de otro host de intentar hacer que la blanco conmuta las tramas delanteras destinadas para el host remoto al atacante de la red. Cuando una sola trama se envía con la dirección Ethernet de la fuente del otro host, el atacante de la red sobregraba la entrada de tabla CAM de modo que los paquetes del Switch adelante destinados para el host al atacante de la red. Hasta que el host envíe el tráfico, no recibe ningún tráfico. Cuando el host envía el tráfico, la entrada de tabla CAM se reescribe una vez más de modo que se mueva de nuevo al puerto original.Utilice la función de seguridad de puerto para atenuar los ataques de simulación MAC. La Seguridad de puerto proporciona la capacidad para especificar la dirección MAC del sistema conectado con un puerto determinado. Esto también proporciona la capacidad de especificar una acción para tomar si ocurre una infracción de Seguridad de puerto.
- **Spoofing del Address Resolution Protocol (ARP)**El ARP se utiliza para asociar el IP Addressing a las direcciones MAC en un segmento de la red de área local donde residen los host de la misma subred. Normalmente, un host envía una petición del broadcast ARP de encontrar la dirección MAC de otro host con un IP Address particular, y una respuesta ARP viene del host cuyo direccionamiento hace juego la petición. El host solicitante entonces oculta esta respuesta ARP. Dentro del Protocolo ARP, otra disposición se adopta para que los host realicen las respuestas ARP no solicitadas. Las respuestas ARP no solicitadas se llaman el ARP gratuito (GARP). El GARP se puede explotar malévolo por un atacante al spoof la identidad de una dirección IP en un segmento LAN. Esto se utiliza típicamente al spoof la identidad entre dos host o todo el tráfico a y desde un default gateway en un ataque “hombre-en--medio”.Cuando se hace a mano una respuesta ARP, un atacante de la red puede hacer que su sistema aparece ser la computadora principal de destino buscada por el remitente. La respuesta ARP hace al remitente salvar la dirección MAC del sistema del atacante de la red en memoria caché ARP. Esta dirección MAC también es salvada por el Switch en su tabla CAM. De esta manera, el atacante de la red ha insertado la dirección MAC de su sistema en la tabla CAM del Switch y memoria caché ARP del remitente. Esto permite que el atacante de la red intercepte las tramas destinadas para el host que él o ella es spoofing.Los temporizadores del asentamiento en el menú de la configuración de la interfaz se pueden utilizar para atenuar los ataques de simulación ARP fijando la longitud del tiempo que una entrada permanecerá en memoria caché ARP. Sin embargo, los temporizadores del asentamiento solo son escasos. La modificación del vencimiento de memoria caché ARP en todos los sistemas extremos se requiere así como las entradas ARP estáticas. Otra solución que se puede utilizar para atenuar la diversa red ARP-basada explota, es el uso del snooping del DHCP junto con la inspección ARP dinámica. Estas características del Catalyst validan los paquetes ARP en una red y permiten la interceptación, el registro, y el desecho de los paquetes ARP con el MAC Address inválido a los atascamientos de la dirección IP.El snooping del DHCP filtra confiaba en los mensajes DHCP para proporcionar la Seguridad. Entonces, estos mensajes se utilizan para construir y para mantener una tabla de vinculación del snooping del DHCP. El snooping del DHCP considera los mensajes DHCP que originan de cualquier puerto del usuario-revestimiento que no sea un puerto de servidor DHCP como untrusted. De una perspectiva del snooping del DHCP, estos puertos untrusted del usuario-revestimiento no deben enviar las respuestas del tipo de servidor DHCP, tales como DHCPOFFER, DHCPACK, o DHCPNAK. La tabla de vinculación del snooping del DHCP contiene el MAC address, el IP Address, el Tiempo de validez, el tipo obligatorio, el número VLAN, y la información de la interfaz que corresponde a las interfaces no confiables locales

de un Switch. La tabla de vinculación del snooping del DHCP no contiene la información sobre los host interconectados con una interfaz confiada en. Una interfaz no confiable es una interfaz configurada para recibir los mensajes desde fuera de la red o del Firewall. Una interfaz de confianza es una interfaz que se configura a los mensajes RO dentro de la red. La tabla de vinculación del snooping del DHCP puede contener dinámico y el Static MAC Address a los atascamientos del IP Address.La inspección ARP dinámica determina la validez de un paquete ARP basado en el MAC address válido a los atascamientos del IP Address salvados en una base de datos del snooping del DHCP. Además, la inspección ARP dinámica puede validar los paquetes ARP basados en el Listas de control de acceso (ACL) utilizador configurable. Esto permite el examen de los paquetes ARP para los host que utilizan estáticamente los IP Address configurados. La inspección ARP dinámica permite el uso de las listas de control de acceso por puerto y del VLA N (PACL) de limitar los paquetes ARP para los IP Addresses específicos a las direcciones MAC específicas.

- **Hambre del Protocolo de configuración dinámica de host (DHCP)**Un ataque del hambre del DHCP trabaja por el broadcast de los pedidos de DHCP con las direcciones MAC del spoofed. Si se envían bastantes solicitudes, el atacante de la red puede agotar el espacio de la dirección disponible para los servidores DHCP por un período de tiempo. El atacante de la red puede después configurar a un servidor DHCP rogue en su sistema y responder a los nuevos pedidos de DHCP de los clientes en la red. Con la colocación de un servidor DHCP rogue en la red, un atacante de la red puede proporcionar a los clientes con los direccionamientos y la otra información de red. Porque las respuestas DHCP incluyen típicamente el default gateway y la información del servidor DNS, el atacante de la red puede suministrar su propio sistema como el default gateway y el servidor DNS. Esto da lugar a un ataque del intermediario. Sin embargo, el extractor de todos los DHCP Address no se requiere para presentar a un servidor DHCP rogue.Las características adicionales en la familia de switches Catalyst, tal como el snooping del DHCP, se pueden utilizar para ayudar a guardar contra un ataque del hambre del DHCP. El snooping del DHCP es una función de seguridad que los mensajes DHCP untrusted y las estructuras de los filtros y mantienen una tabla de vinculación del snooping del DHCP. La tabla de vinculación contiene la información tal como el MAC address, el IP Address, el Tiempo de validez, el tipo obligatorio, el número VLAN y la información de la interfaz que corresponde a las interfaces no confiables locales de un Switch. Los mensajes untrusted son ésos recibidos desde fuera de la red o del Firewall. Las interfaces del switch untrusted son unas que se configuran para recibir tales mensajes desde fuera de la red o del Firewall.Otras características del switch de Catalyst, tales como Protección de origen IP, pueden proporcionar la defensa adicional contra los ataques tales como hambre y IP spoofing del DHCP. Similar al snooping del DHCP, habilitan a la Protección de origen IP en los puertos untrusted de la capa 2. Todo el tráfico IP se bloquea inicialmente, a excepción de los paquetes DHCP capturados por el proceso del snooping del DHCP. Una vez que un cliente recibe un IP Address válido del servidor DHCP, un PACL se aplica al puerto. Esto restringe IP del cliente el tráfico a esas dirección IP de origen configuradas en el atascamiento. Cualquier otro tráfico IP con una dirección de origen con excepción de los direccionamientos en el atascamiento se filtra.

Configurar

En esta sección, le presentan con la información para configurar la Seguridad de puerto, el snooping del DHCP, las funciones de seguridad dinámicas de la inspección ARP y de la

Protección de origen IP.

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

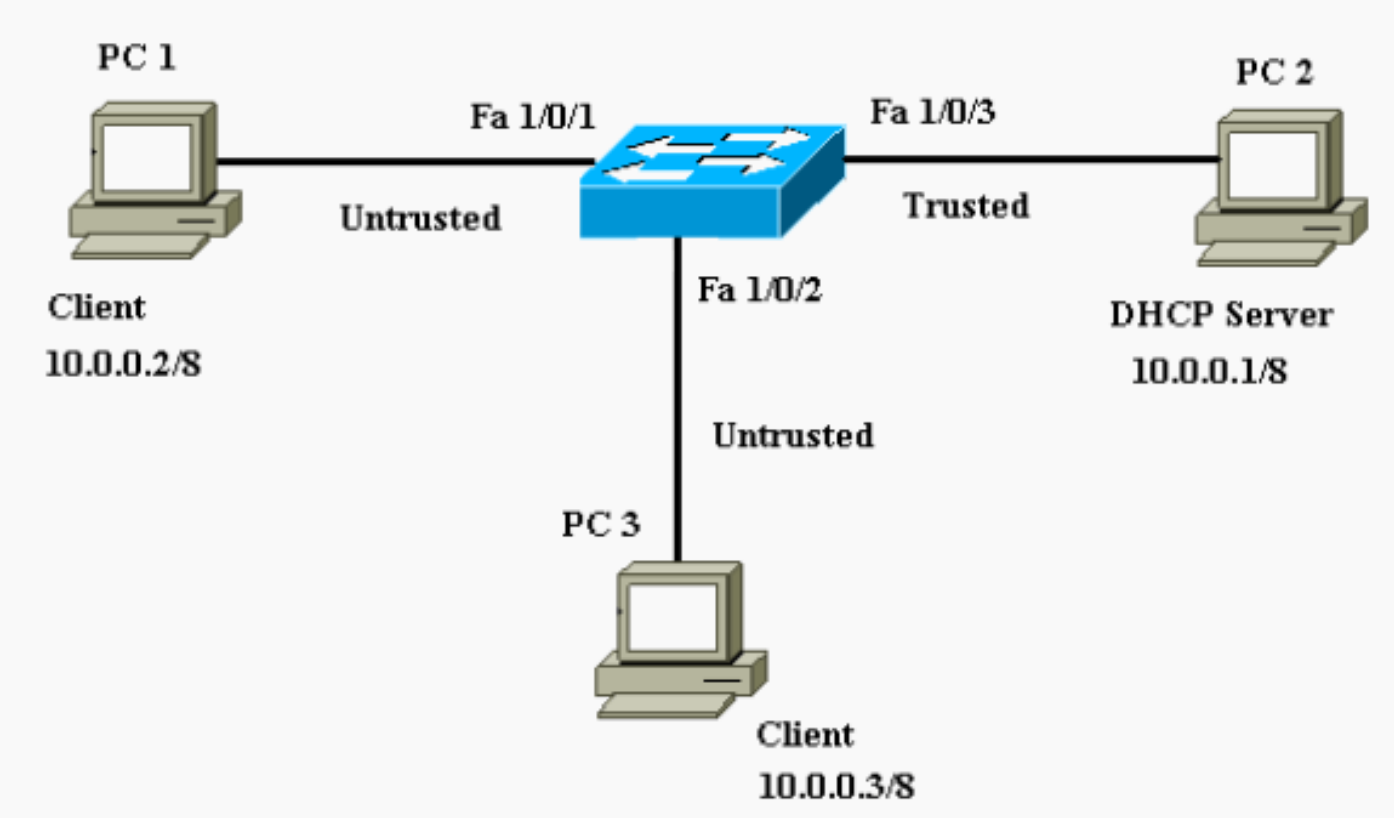
Las configuraciones del Catalyst 3750 Switch contienen éstos:

- Seguridad de Puertos
- Snooping del DHCP
- Dynamic ARP Inspection
- IP Source Guard

Diagrama de la red

En este documento, se utiliza esta configuración de red:

- El PC1 y el PC3 son clientes conectados con el Switch.
- El PC2 es servidor DHCP conectado con el Switch.
- Todos los puertos del Switch están en el mismo VLA N (VLA N 1).
- Configuran al servidor DHCP para asignar los IP Addresses a los clientes basados en sus direcciones MAC.



Seguridad de Puertos

Usted puede utilizar la función de seguridad de puerto para limitar y para identificar las direcciones MAC de las estaciones permitidas acceder el puerto. Esto restringe la entrada a una interfaz. Cuando usted asigna los MAC Address seguros a un puerto seguro, el puerto no remite los paquetes con las direcciones de origen fuera del grupo de direccionamientos definidos. Si usted limita el número de MAC Address seguros a uno y asigna un solo MAC Address seguro, el puesto de trabajo asociado a ese puerto se asegura el ancho de banda completa del puerto. Si se

configura un puerto mientras que un puerto seguro y el número máximo de MAC Address seguros se alcanza, cuando la dirección MAC de una estación que intente acceder el puerto es diferente de los MAC Address seguros identificados uces de los, una violación de seguridad ocurre. También, si una estación con un MAC Address seguro configurado o aprendido en un puerto seguro intenta acceder otro puerto seguro, se señala por medio de una bandera una infracción. Por abandono, el puerto apaga cuando el número máximo de MAC Address seguros se excede.

Nota: Cuando un Catalyst 3750 Switch se une a un stack, el nuevo Switch recibe los direccionamientos seguros configurados. Todos los direccionamientos seguros dinámicos son descargados por el nuevo miembro de pila de los otros miembros de pila.

Refiera a las pautas de configuración para las guías de consulta en cómo configurar la Seguridad de puerto.

Aquí, la función de seguridad de puerto se muestra configurada en el FastEthernet 1/0/2 interfaz. Por abandono, el número máximo de MAC Address seguros para la interfaz es una. Usted puede publicar el **comando interface de la Seguridad de puerto de la demostración** para verificar el estatus de la Seguridad de 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 se deben configurar que seguras y el Static MAC Address en diversos puertos de un Switch.

Cuando un teléfono del IP está conectado con un Switch a través del switchport configurado para el VLA N de la Voz, el teléfono envía los paquetes CDP untagged y los paquetes CDP marcados con etiqueta de la Voz. La dirección MAC del teléfono del IP se aprende tan en el PVID y el VVID. Si el número apropiado de direccionamientos seguros no se configura, usted puede conseguir 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:
```

Usted debe fijar el máximo no prohibido los direccionamientos seguros en el puerto a dos (para el teléfono del IP) más el número máximo de direccionamientos seguros permitidos en el VLA N del acceso para resolver este problema.

Refiera a configurar la Seguridad de puerto para más información.

Snooping del DHCP

El snooping del DHCP actúa como un Firewall entre los host no confiables y los servidores DHCP. Usted utiliza el snooping del DHCP para distinguir entre las interfaces no confiables conectadas con el usuario final y las interfaces confiadas en conectadas con el servidor DHCP u otro Switch. Cuando un Switch recibe un paquete en una interfaz no confiable y la interfaz pertenece a un VLA N que tenga snooping del DHCP habilitado, el Switch compara el MAC Address de origen y a la dirección de hardware del Cliente de DHCP. Si los direccionamientos hacen juego (el valor por defecto), el Switch adelante el paquete. Si los direccionamientos no hacen juego, el Switch cae el paquete. El Switch cae un paquete DHCP cuando ocurre una de estas situaciones:

- Un paquete de un servidor DHCP, tal como un DHCPOFFER, paquete DHCPACK, DHCPNAK, o DHCPLEASEQUERY, se recibe desde fuera de la red o del Firewall.
- Un paquete se recibe en una interfaz no confiable, y el MAC Address de origen y la dirección de hardware del Cliente de DHCP no corresponden con.
- El Switch recibe un mensaje de broadcast DHCPRELEASE o DHCPDECLINE que tenga un MAC address en la base de datos de etiquetas del snooping del DHCP, pero la información de la interfaz en la base de datos de etiquetas no corresponde con la interfaz en la cual el mensaje fue recibido.
- Un agente de relé DHCP adelante un paquete DHCP, que incluye un IP Address del Agente Relay que no sea 0.0.0.0, o el Agente Relay adelante un paquete que incluye la información option-82 al puerto no confiable.

Refiera a las pautas de configuración del snooping del DHCP para las guías de consulta en cómo configurar el snooping del DHCP.

Nota: Para que el snooping del DHCP funcione correctamente, todos los servidores DHCP deben ser conectados con el Switch a través de las interfaces confiadas en.

Nota: En un stack del Switch con los Catalyst 3750 Switch, el snooping del DHCP se maneja en el master del stack. Cuando un nuevo Switch se une al stack, el Switch recibe la configuración del snooping del DHCP del master del stack. Cuando un miembro deja el stack, todos los atascamientos del snooping del DHCP se asociaron a la edad del Switch hacia fuera.

Nota: Para asegurarse de que el Tiempo de validez en la base de datos sea exacto, Cisco recomienda que usted habilita y configura el NTP. Si se configura el NTP, el Switch escribe los cambios del atascamiento al archivo obligatorio solamente cuando el reloj del sistema del Switch se sincroniza con el NTP.

Los servidores DHCP rogue pueden ser atenuados por las características del snooping del DHCP. El comando del **snooping DHCP del IP** se publica para habilitar el DHCP global en el Switch. Cuando están configurados con el snooping del DHCP, todos los puertos en el VLA N son untrusted para las respuestas DHCP. Aquí, solamente la interfaz FastEthernet 1/0/3 conectada con el servidor DHCP se configura según lo confiado en.

Snooping del 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.
```

Refiera a configurar las características del DHCP para más información.

Dynamic ARP Inspection

La inspección ARP dinámica es una función de seguridad que valida los paquetes ARP en una red. Intercepta, los registros, y desecha los paquetes ARP con las vinculaciones de dirección inválidas IP-a-MAC. Esta capacidad protege la red contra ciertos ataques del intermediario.

La inspección ARP dinámica se asegura de que solamente los pedidos ARP y las respuestas válidos estén retransmitidos. El Switch realiza estas actividades:

- Intercepta todos los pedidos ARP y respuestas en los puertos untrusted
- Verifica que cada uno de estos paquetes interceptados tenga una vinculación de dirección válida IP-a-MAC antes de que ponga al día memoria caché ARP local o antes de que él adelante el paquete al destino apropiado
- Cae los paquetes ARP inválidos

La inspección ARP dinámica determina la validez de un paquete ARP basado en las vinculaciones de dirección válidas IP-a-MAC salvadas en una base de datos confiada en, la base de datos de etiquetas del snooping del DHCP. Esta base de datos es construida por el snooping del DHCP si el snooping del DHCP se habilita en los VLA N y en el Switch. Si el paquete ARP se recibe en una interfaz de confianza, el Switch adelante el paquete sin cualquier controles. En las interfaces no confiables, el Switch adelante el paquete solamente si es válido.

En los entornos del NON-DHCP, la inspección ARP dinámica puede validar los paquetes ARP contra el usuario configurado ARP ACL para los host con estáticamente los IP Address configurados. Usted puede publicar el comando global configuration de la **lista de acceso arp** para definir un ARP ACL. El ARP ACL toma la precedencia sobre las entradas en la base de datos de etiquetas del snooping del DHCP. El Switch utiliza los ACL solamente si usted publica el comando global configuration **vlan del filtro del examen arp del IP** para configurar los ACL. El Switch primero compara los paquetes ARP al usuario configurado ARP ACL. Si el ARP ACL niega el paquete ARP, el Switch también niega el paquete incluso si un atascamiento válido existe en la base de datos poblada por el snooping del DHCP.

Refiera a las pautas de configuración dinámicas de la inspección ARP para las guías de consulta en cómo configurar la inspección ARP dinámica.

Publican el comando global configuration **vlan del examen arp del IP** para habilitar la inspección ARP dinámica sobre una base del por el VLAN. Aquí, solamente la interfaz FastEthernet 1/0/3 conectada con el servidor DHCP se configura según lo confiado en con el **comando trust del examen arp del IP**. El snooping del DHCP se debe habilitar para permitir los paquetes ARP que tienen dinámicamente IP Address asignados. Vea la sección del snooping del DHCP de este documento para la información de la configuración del snooping del 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#

Refiera a configurar la inspección ARP dinámica para más información.

IP Source Guard

La Protección de origen IP es una función de seguridad que los filtros trafican basado en la base de datos de etiquetas del snooping del DHCP y en los atascamientos manualmente configurados del IP de origen para restringir el tráfico IP en los interfaz de capa 2 NON-ruteados. Usted puede utilizar a la Protección de origen IP para prevenir los ataques del tráfico causados cuando un host intenta utilizar la dirección IP de su vecino. La Protección de origen IP previene el spoofing IP/MAC.

Usted puede habilitar a la Protección de origen IP cuando el snooping del DHCP se habilita en una interfaz no confiable. Después de que habiliten a la Protección de origen IP en una interfaz, el Switch bloquea todo el tráfico IP recibido en la interfaz, a excepción de los paquetes DHCP permitidos por el snooping del DHCP. Un puerto ACL se aplica a la interfaz. El puerto ACL permite solamente el tráfico IP con una dirección IP de origen en la tabla de vinculación del IP de origen y niega el resto del tráfico.

La tabla de vinculación del IP de origen tiene atascamientos que sean aprendidos por el snooping del DHCP o configurados manualmente (IP estático los atascamientos de la fuente). Una entrada en esta tabla tiene una dirección IP, su dirección MAC asociada, y su número VLAN asociado. El Switch utiliza la tabla de vinculación del IP de origen solamente cuando habilitan a la Protección de origen IP.

Usted puede configurar a la Protección de origen IP con la dirección IP de origen que filtra, o con la filtración IP y de la dirección MAC de la fuente. Cuando habilitan a la Protección de origen IP con esta opción, el tráfico IP se filtra sobre la base de la dirección IP de origen. Del Switch el tráfico IP adelante cuando la dirección IP de origen corresponde con una entrada en la base de datos de etiquetas del snooping del DHCP o un atascamiento en la tabla de vinculación del IP de origen. Cuando habilitan a la Protección de origen IP con esta opción, el tráfico IP se filtra sobre la base del IP de la fuente y de las direcciones MAC. El Switch adelante trafica solamente cuando el IP de la fuente y las direcciones MAC hacen juego una entrada en la tabla de vinculación del IP de origen.

Nota: Soportan a la Protección de origen IP solamente en los puertos de la capa 2, que incluye el acceso y los puertos troncales.

Refiera a las pautas de configuración de la Protección de origen IP para las guías de consulta en cómo configurar a la Protección de origen IP.

Aquí, configuran a la Protección de origen IP con la filtración IP de la fuente en el FastEthernet que 1/0/1 interfaz con el **IP verifica el comando source**. Cuando habilitan a la Protección de origen IP con la filtración IP de la fuente en un VLA N, el snooping del DHCP se debe habilitar en el VLA N del acceso al cual la interfaz pertenece. Publique el **IP de la demostración verifican el comando source** para verificar la configuración de la Protección de origen IP 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#
```

Refiera comprensión de la Protección de origen IP para más información.

Verificación

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

Troubleshooting

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