Exemplo de Configuração de Recursos da Camada 2 em Switches de Configuração Fixa da Camada 3 Cisco Catalyst

Contents

Introduction

Este documento fornece um exemplo de configuração de alguns dos recursos de segurança da Camada 2, como segurança de portas, snooping de DHCP, inspeção de ARP (Address Resolution Protocol) dinâmica e proteção de origem de IP que podem ser implementados em switches de configuração fixa da Camada 3 Cisco Catalyst.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Catalyst 3750 Series Switch com a versão 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.

Produtos Relacionados

Esta configuração também pode ser utilizada com o seguinte hardware:

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

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Semelhante aos roteadores, os switches de Camada 2 e Camada 3 têm seus próprios conjuntos de requisitos de segurança de rede. Os switches são susceptíveis a muitos dos mesmos ataques de Camada 3 que os roteadores. No entanto, os switches e a camada 2 do modelo de referência OSI em geral estão sujeitos a ataques à rede de maneiras diferentes. Eles incluem:

- **Sobrecarga da tabela de memória endereçável de conteúdo (CAM - Content Addressable Memory)**As tabelas CAM (Content Addressable Memory, Memória endereçável de conteúdo) são limitadas em tamanho. Se entradas suficientes forem inseridas na tabela CAM antes de outras entradas expirarem, a tabela CAM preencherá até o ponto em que nenhuma entrada nova pode ser aceita. Normalmente, um invasor de rede inunda o switch com um grande número de endereços MAC (Media Access Control) de origem inválida até que a tabela CAM seja preenchida. Quando isso ocorre, o switch inunda todas as portas com tráfego de entrada porque não consegue encontrar o número de porta de um endereço MAC específico na tabela CAM. O switch, em essência, atua como um hub. Se o invasor não mantiver a inundação de endereços MAC de origem inválida, o switch eventualmente expirará entradas de endereços MAC mais antigas da tabela CAM e começará a agir como um switch novamente. O estouro da tabela CAM inunda apenas o tráfego dentro da VLAN local, de modo que o invasor veja apenas o tráfego dentro da VLAN local à qual está conectado.O ataque de estouro da tabela CAM pode ser atenuado pela configuração da segurança de porta no switch. Essa opção fornece a especificação dos endereços MAC em uma porta de switch específica ou a especificação do número de endereços MAC que podem ser aprendidos por uma porta de switch. Quando um endereço MAC inválido é detectado na porta, o switch pode bloquear o endereço MAC ofensivo ou desligar a porta. A especificação de endereços MAC em portas de switch é uma solução muito ingerenciável para um ambiente de produção. Um limite do número de endereços MAC em uma porta do switch é gerenciável. Uma solução administrativamente mais escalável é a implementação de segurança de porta dinâmica no switch. Para implementar a segurança de porta dinâmica, especifique um número máximo de endereços MAC que serão aprendidos.

- **Spoofing de endereço MAC (Media Access Control)**Os ataques de falsificação de Controle de Acesso ao Meio (MAC - Media Access Control) envolvem o uso de um endereço MAC conhecido de outro host para tentar fazer com que o switch de destino encaminhe quadros destinados ao host remoto para o invasor de rede. Quando um único quadro é enviado com o endereço Ethernet de origem do outro host, o invasor de rede substitui a entrada da tabela CAM para que o switch encaminhe pacotes destinados ao host para o invasor de rede. Até que o host envie tráfego, ele não recebe nenhum tráfego. Quando o host envia tráfego, a entrada da tabela CAM é regravada uma vez mais para que ela se mova de volta para a porta original.Use o recurso de segurança de porta para atenuar ataques de falsificação de MAC. A segurança de porta fornece a capacidade de especificar o endereço MAC do sistema conectado a uma porta específica. Isso também permite especificar uma ação a ser tomada se ocorrer uma violação de segurança de porta.
- **Spoofing do Address Resolution Protocol (ARP)**O ARP é usado para mapear o endereçamento IP para endereços MAC em um segmento de rede local onde os hosts da mesma sub-rede residem. Normalmente, um host envia uma solicitação ARP de broadcast para encontrar o endereço MAC de outro host com um endereço IP específico, e uma resposta ARP vem do host cujo endereço corresponde à solicitação. Em seguida, o host solicitante coloca em cache essa resposta ARP. Dentro do protocolo ARP, outro provisionamento é feito para que os hosts executem respostas ARP não solicitadas. As respostas ARP não solicitadas são chamadas de Gratuitous ARP (GARP). O GARP pode ser maliciosamente explorado por um invasor para falsificar a identidade de um endereço IP em um segmento de LAN. Normalmente, isso é usado para falsificar a identidade entre dois hosts ou todo o tráfego de e para um gateway padrão em um ataque "man-in-the-middle".Quando uma resposta ARP é criada, um invasor de rede pode fazer com que seu sistema pareça ser o host de destino procurado pelo remetente. A resposta de ARP faz com que o emissor armazene o endereço MAC do sistema do agressor no cache de ARP. Esse endereço MAC também é armazenado pelo switch em sua tabela CAM. Ao agir dessa forma, o agressor de rede inseriu o endereço MAC do seu próprio sistema na tabela CAM do switch e no cache de ARP do emissor. Isso permite que ele intercepte frames destinados ao host que está falsificando.Os temporizadores holddown no menu de configuração de interface podem ser usados para atenuar ataques de falsificação ARP definindo o período de tempo durante o qual uma entrada permanecerá no cache ARP. No entanto, os temporizadores de retenção por si só são insuficientes. É necessária a modificação do tempo de expiração do cache ARP em todos os sistemas finais, bem como entradas ARP estáticas. Outra solução que pode ser usada para atenuar várias explorações de rede baseadas em ARP é o uso de rastreamento de DHCP juntamente com inspeção ARP dinâmica. Esses recursos do Catalyst validam os pacotes ARP em uma rede e permitem a interceptação, o registro e o descarte de pacotes ARP com endereços MAC inválidos para associações de endereços IP.O rastreamento de DHCP filtra mensagens DHCP confiáveis para fornecer segurança. Em seguida, essas mensagens são usadas para criar e manter uma tabela de vinculação de rastreamento de DHCP. O rastreamento de DHCP considera as mensagens DHCP que se originam de qualquer porta para o usuário que não seja uma porta do servidor DHCP como não confiável. De uma perspectiva de rastreamento de DHCP, essas portas não confiáveis voltadas para o usuário não devem enviar respostas de tipo de servidor DHCP, como DHCPOFFER, DHCPACK ou DHCPNAK. A tabela de vinculação de rastreamento de DHCP contém o endereço MAC, o endereço IP, o tempo de concessão, o tipo de vinculação, o número da VLAN e as informações de interface que correspondem às interfaces não confiáveis locais de um switch. A tabela de associação de rastreamento de DHCP não contém informações sobre

hosts interconectados com uma interface confiável. Uma interface não confiável é uma interface configurada para receber mensagens de fora da rede ou do firewall. Uma interface confiável é uma interface configurada para receber apenas mensagens de dentro da rede. A tabela de vinculação de rastreamento de DHCP pode conter endereços MAC dinâmicos e estáticos para associações de endereços IP.A inspeção ARP dinâmica determina a validade de um pacote ARP com base no endereço MAC válido para associações de endereços IP armazenadas em um banco de dados de rastreamento de DHCP. Além disso, a inspeção ARP dinâmica pode validar pacotes ARP com base nas listas de controle de acesso (ACLs) configuráveis pelo usuário. Isso permite a inspeção de pacotes ARP para hosts que usam endereços IP configurados estaticamente. A inspeção ARP dinâmica permite o uso de PACLs (Access Control Lists, listas de controle de acesso) por porta e VLAN para limitar os pacotes ARP para endereços IP específicos a endereços MAC específicos.

- **Privação do Dynamic Host Configuration Protocol (DHCP)**Um ataque de privação de DHCP funciona pelo broadcast de solicitações de DHCP com endereços MAC falsificados. Se forem enviadas solicitações suficientes, o invasor de rede pode esgotar o espaço de endereço disponível para os servidores DHCP por um período de tempo. O invasor de rede pode configurar um servidor DHCP invasor em seu sistema e responder a novas solicitações DHCP de clientes na rede. Com a colocação de um servidor DHCP invasor na rede, um invasor de rede pode fornecer aos clientes endereços e outras informações de rede. Como as respostas DHCP geralmente incluem informações de gateway padrão e de servidor DNS, o invasor de rede pode fornecer seu próprio sistema como o gateway padrão e o servidor DNS. Isso resulta em um ataque do tipo "homem no meio". No entanto, o escape de todos os endereços DHCP não é necessário para introduzir um servidor DHCP invasor.Recursos adicionais na família de switches Catalyst, como o rastreamento de DHCP, podem ser usados para ajudar a proteger contra um ataque de inanição de DHCP. O rastreamento de DHCP é um recurso de segurança que filtra mensagens DHCP não confiáveis e cria e mantém uma tabela de vinculação de rastreamento de DHCP. A tabela de vinculação contém informações como o endereço MAC, o endereço IP, o tempo de concessão, o tipo de vinculação, o número da VLAN e as informações de interface que correspondem às interfaces não confiáveis locais de um switch. As mensagens não confiáveis são aquelas recebidas de fora da rede ou firewall. As interfaces de switch não confiáveis são aquelas configuradas para receber essas mensagens de fora da rede ou do firewall.Outros recursos do switch Catalyst, como o IP source guard, podem fornecer defesa adicional contra ataques como privação de DHCP e falsificação de IP. Semelhante ao rastreamento de DHCP, o IP source guard está ativado em portas da Camada 2 não confiáveis. Todo o tráfego IP é inicialmente bloqueado, exceto os pacotes DHCP capturados pelo processo de rastreamento de DHCP. Quando um cliente recebe um endereço IP válido do servidor DHCP, um PACL é aplicado à porta. Isso restringe o tráfego IP do cliente aos endereços IP de origem configurados na associação. Qualquer outro tráfego IP com um endereço de origem diferente dos endereços na associação é filtrado.

Configurar

Nesta seção, você recebe as informações para configurar os recursos de segurança Port Security, DHCP Snooping, Dynamic ARP Inspection e IP Source Guard.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

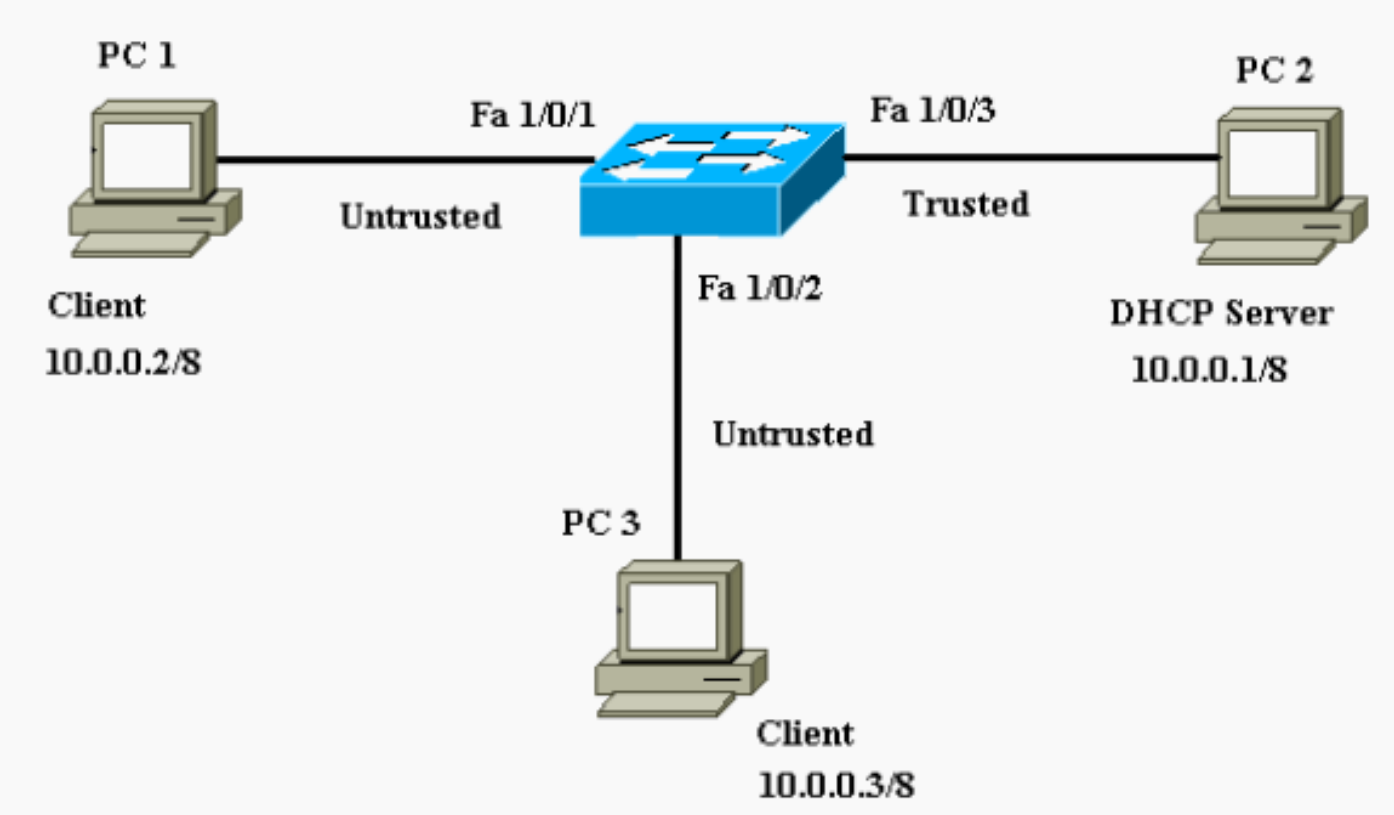
As configurações do Switch Catalyst 3750 contêm:

- Segurança da porta
- Rastreamento de DHCP
- Inspeção ARP dinâmica
- Proteção de origem de IP

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

- PC 1 e PC 3 são clientes conectados ao switch.
- PC 2 é um servidor DHCP conectado ao switch.
- Todas as portas do switch estão na mesma VLAN (VLAN 1).
- O servidor DHCP é configurado para atribuir endereços IP aos clientes com base em seus endereços MAC.



Segurança da porta

Você pode usar o recurso de segurança de porta para limitar e identificar os endereços MAC das estações com permissão para acessar a porta. Isso restringe a entrada a uma interface. Quando você atribui endereços MAC seguros a uma porta segura, a porta não encaminha pacotes com endereços de origem fora do grupo de endereços definidos. Se você limitar o número de endereços MAC seguros a um e atribuir um único endereço MAC seguro, a estação de trabalho conectada a essa porta terá a largura de banda total garantida da porta. Se uma porta é configurada como uma porta segura e o número máximo de endereços MAC seguros é alcançado, quando o endereço MAC de uma estação que tenta acessar a porta é diferente de qualquer um dos endereços MAC seguros identificados, ocorre uma violação de segurança. Além disso, se uma estação com um endereço MAC seguro configurado ou aprendido em uma porta segura tenta acessar outra porta segura, uma violação é sinalizada. Por padrão, a porta é

desligada quando o número máximo de endereços MAC seguros é excedido.

Nota:Quando um Catalyst 3750 Switch ingressa em uma stack, o novo switch recebe os endereços seguros configurados. Todos os endereços seguros dinâmicos são baixados pelo novo membro da pilha dos outros membros da pilha.

Consulte as Diretrizes de Configuração para obter as diretrizes de configuração da segurança de portas.

Aqui, o recurso de segurança de porta é mostrado configurado na interface FastEthernet 1/0/2. Por padrão, o número máximo de endereços MAC seguros para a interface é um. Você pode executar o comando **show port-security interface** para verificar o status de segurança de porta de uma interface.

Segurança da porta

```
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
```

Observação: os mesmos endereços MAC não devem ser configurados como endereços MAC seguros e estáticos em portas diferentes de um switch.

Quando um telefone IP é conectado a um switch através da porta de switch configurada para VLAN de voz, o telefone envia pacotes CDP não marcados e pacotes CDP de voz marcados. Assim, o endereço MAC do telefone IP é aprendido tanto no PVID quanto no VVID. Se o número apropriado de endereços seguros não estiver configurado, você poderá receber uma mensagem de erro semelhante a esta mensagem:

```
%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:
```

Você deve definir o máximo de endereços seguros permitidos na porta como dois (para telefone IP) mais o número máximo de endereços seguros permitidos na VLAN de acesso para resolver esse problema.

Consulte Configuração da Segurança de Portas para obter mais informações.

Rastreamento de DHCP

O rastreamento de DHCP atua como um firewall entre hosts não confiáveis e servidores DHCP. Você usa o rastreamento de DHCP para diferenciar entre interfaces não confiáveis conectadas ao usuário final e interfaces confiáveis conectadas ao servidor DHCP ou a outro switch. Quando um switch recebe um pacote em uma interface não confiável e a interface pertence a uma VLAN com snooping de DHCP habilitado, o switch compara o endereço MAC de origem e o endereço de hardware do cliente DHCP. Se os endereços coincidirem (o padrão), o switch encaminhará o pacote. Se os endereços não corresponderem, o switch descarta o pacote. O switch descarta um pacote DHCP quando ocorre uma destas situações:

- Um pacote de um servidor DHCP, como um pacote DHCPOFFER, DHCPACK, DHCPNAK ou DHCPLEASEQUERY, é recebido de fora da rede ou do firewall.
- Um pacote é recebido em uma interface não confiável e o endereço MAC origem e o endereço de hardware do cliente DHCP não correspondem.
- O switch recebe uma mensagem de broadcast DHCPRELEASE ou DHCPDECLINE que tem um endereço MAC no banco de dados de associação de rastreamento de DHCP, mas as informações de interface no banco de dados de associação não correspondem à interface na qual a mensagem foi recebida.
- Um agente de retransmissão de DHCP encaminha um pacote DHCP, que inclui um endereço IP de agente de retransmissão que não seja 0.0.0.0, ou o agente de retransmissão encaminha um pacote que inclui informações da opção 82 para uma porta não confiável.

Consulte as Diretrizes de Configuração do Snooping de DCHP para obter as diretrizes de configuração do snooping de DHCP.

Nota:Para que o snooping de DHCP funcione corretamente, todos os servidores DHCP deverão se conectar ao switch por meio de interfaces confiáveis.

Nota:Em uma switch stack com Catalyst 3750 Switches, o snooping de DHCP é gerenciado no master da stack. Quando um novo switch entra na pilha, o switch recebe a configuração de rastreamento de DHCP do mestre da pilha. Quando um membro sai da pilha, todos os vínculos de rastreamento de DHCP associados ao tempo de saída do switch.

Nota:Para garantir a exatidão do tempo de concessão no banco de dados, a Cisco recomenda habilitar e configurar o NTP. Quando o NTP está configurado, o switch insere as alterações de ligação no arquivo de ligação somente quando o relógio do sistema do switch está sincronizado com o NTP.

Os servidores DHCP invasores podem ser atenuados por recursos de rastreamento de DHCP. O comando **ip dhcp snooping** é executado para habilitar o DHCP globalmente no switch. Quando configurado com rastreamento de DHCP, todas as portas na VLAN não são confiáveis para respostas de DHCP. Aqui, somente a interface FastEthernet 1/0/3 conectada ao servidor DHCP é configurada como confiável.

Rastreamento 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.
```

Consulte Configuração de Recursos de DHCP para obter mais informações.

Inspeção ARP dinâmica

A inspeção ARP dinâmica é um recurso de segurança que valida pacotes ARP em uma rede. Ele intercepta, registra e descarta pacotes ARP com associações inválidas de endereço IP para MAC. Esse recurso protege a rede de determinados ataques de intermediários.

A inspeção ARP dinâmica garante que somente as solicitações ARP válidas e as respostas sejam retransmitidas. O switch executa estas atividades:

- Intercepta todas as solicitações e respostas ARP em portas não confiáveis
- Verifica se cada um desses pacotes interceptados tem uma associação de endereço IP para MAC válida antes de atualizar o cache ARP local ou antes de encaminhar o pacote para o destino apropriado
- Descarta pacotes ARP inválidos

A inspeção ARP dinâmica determina a validade de um pacote ARP com base em vínculos válidos de endereço IP para MAC armazenados em um banco de dados confiável, o banco de dados de vínculo de rastreamento de DHCP. Esse banco de dados é criado pelo rastreamento de DHCP se o rastreamento de DHCP estiver ativado nas VLANs e no switch. Se o pacote ARP for recebido em uma interface confiável, o switch encaminhará o pacote sem nenhuma verificação. Em interfaces não confiáveis, o switch encaminha o pacote somente se for válido.

Em ambientes não DHCP, a inspeção ARP dinâmica pode validar os pacotes ARP em relação às ACLs ARP configuradas pelo usuário para hosts com endereços IP configurados estaticamente. Você pode executar o comando de configuração global **arp access-list** para definir uma ACL de ARP. As ACLs ARP têm precedência sobre as entradas no banco de dados de associação de rastreamento de DHCP. O switch usa ACLs somente se você emitir o comando de configuração global **ip arp inspection filter vlan** para configurar as ACLs. O switch compara primeiro pacotes ARP a ACLs ARP configuradas pelo usuário. Se a ACL ARP negar o pacote ARP, o switch também negará o pacote mesmo que exista uma associação válida no banco de dados

preenchido pelo rastreamento DHCP.

Consulte as Diretrizes de Configuração da Inspeção de ARP Dinâmica para obter as diretrizes de configuração da inspeção de ARP dinâmica.

O comando de configuração global **ip arp inspection vlan** é emitido para ativar a inspeção ARP dinâmica por VLAN. Aqui, somente a interface FastEthernet 1/0/3 conectada ao servidor DHCP é configurada como confiável com o comando **ip arp inspection trust**. O snooping de DHCP deve ser habilitado para permitir os pacotes de ARP com endereços IP atribuídos dinamicamente. Consulte a seção Snooping de DHCP deste documento para obter informações de configuração do snooping de DHCP.

Inspeção ARP dinâmica

```
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 Configurando a Inspeção de ARP Dinâmica para obter mais informações.

Proteção de origem de IP

O IP source guard é um recurso de segurança que filtra o tráfego com base no banco de dados de vinculação de rastreamento de DHCP e em associações de origem de IP configuradas manualmente para restringir o tráfego IP em interfaces de Camada 2 não roteadas. Você pode usar o protetor de origem de IP para evitar ataques de tráfego causados quando um host tenta usar o endereço IP de seu vizinho. O protetor de origem de IP evita falsificação de IP/MAC.

Você pode habilitar o IP source guard quando o rastreamento de DHCP estiver habilitado em uma interface não confiável. Depois que o protetor de origem de IP é ativado em uma interface, o switch bloqueia todo o tráfego IP recebido na interface, exceto os pacotes DHCP permitidos pelo rastreamento de DHCP. Uma ACL de porta é aplicada à interface. A ACL de porta permite somente o tráfego IP com um endereço IP de origem na tabela de vinculação de origem IP e nega todo o tráfego restante.

A tabela de vinculação de origem de IP tem vínculos aprendidos pelo rastreamento de DHCP ou configurados manualmente (vínculos de origem de IP estático). Uma entrada nesta tabela tem um endereço IP, seu endereço MAC associado e seu número de VLAN associado. O switch usa a tabela de vinculação de origem de IP somente quando o protetor de origem de IP está ativado.

Você pode configurar a proteção de origem de IP com a filtragem de endereços IP de origem ou com a filtragem de endereços IP e MAC de origem. Quando a proteção de origem de IP está habilitada com essa opção, o tráfego IP é filtrado com base no endereço IP de origem. O switch encaminha o tráfego IP quando o endereço IP de origem corresponde a uma entrada no banco de dados de associação de rastreamento de DHCP ou a uma associação na tabela de vinculação de origem de IP. Quando o protetor de origem de IP está ativado com essa opção, o tráfego IP é filtrado com base nos endereços IP e MAC de origem. O switch encaminha o tráfego somente quando os endereços IP e MAC de origem correspondem a uma entrada na tabela de vinculação de origem IP.

Nota:A proteção de origem de IP pode ser habilitada somente em portas da Camada 2, o que inclui portas de acesso e tronco.

Consulte as Diretrizes de Configuração da Proteção de Origem de IP para obter as diretrizes de configuração da proteção de origem de IP.

Aqui, a proteção de origem de IP com filtragem de IP de origem é configurada na interface FastEthernet 1/0/1 com o comando **ip verify source**. Quando a proteção de origem de IP com filtragem de IP de origem é habilitada em uma VLAN, o snooping de DHCP deve ser habilitado na VLAN de acesso à qual a interface pertence. Execute o comando **show ip verify source** para verificar a configuração da proteção de origem de IP no switch.

Proteção de origem de IP

```
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#
```

Consulte Entendendo a Proteção de Origem de IP para obter mais informações.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Protegendo redes com VLANs privados e listas de controle de acesso de VLAN
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems