

Obstrua pacotes ARP com uso de Listas de acesso MAC e de mapas do acesso de vlan no catalizador 2970, 3550, 3560, e 3750 Series Switch

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração de exemplo](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento discute a configuração para um Cisco Catalyst 3550 Series Switch. Você pode utilizar qualquer Catalyst 2970, 3560 ou 3750 Series Switch neste cenário para obter os mesmos resultados. O documento demonstra como configurar um Access Control List MAC (ACL) a fim obstruir uma comunicação entre dispositivos dentro de um VLAN. Você pode bloquear um host único ou um intervalo de hosts com base no fabricante do adaptador da placa de interface de rede (NIC) do host. Você pode obstruir uma escala dos anfitriões se você recusa os pacotes do Address Resolution Protocol (ARP) que originam destes dispositivos baseados nas atribuições do identificador exclusivo organizacional (OUI) e do company_id da IEEE.

Em uma rede, você pode obstruir pacotes de solicitação ARP a fim restringir o acesso de usuário. Em alguns cenários de rede, você deseja bloquear os pacotes ARP baseados não no endereço IP, mas nos endereços MAC da camada 2. Você pode realizar este tipo de limitação se você cria mapas do MAC address ACL e do acesso de vlan e os aplica a uma interface de VLAN.

Pré-requisitos

Requisitos

Consulte [OUI e Atribuições de Company id do IEEE](#) para determinar o OUI e atribuições de company_id do IEEE.

[Componentes Utilizados](#)

As informações neste documento baseiam-se no Cisco Catalyst 3550 Switch.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

O outro Switches que apoia os comandos nesta configuração inclui o catalizador 2970, 3560, ou 3750 Series Switch.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Para configurar a filtragem de endereços MAC e aplicá-la à interface de VLAN, você deve concluir vários passos. Primeiramente, você cria os mapas do acesso de vlan para cada tipo de tráfego que deve ser filtrado. Você seleciona um endereço MAC ou um intervalo de endereços MAC para bloqueio. Você também precisa identificar o tráfego ARP na lista de acessos. De acordo com o [RFC 826](#), um quadro ARP usa o tipo de protocolo de Ethernet do valor 0x806. [Você pode filtrar este tipo de protocolo como o tráfego de interesse para a lista de acessos.](#)

1. No modo de configuração global, crie uma lista de acesso estendida de MAC com o nome ARP_Packet. Inscreva o [comando mac access-list extended ACL_name](#) e adicionar o MAC address ou os endereços do host que você quer obstruir.

```
Switch(config)#mac access-list extended ARP_Packet Switch(config-ext-nacl)#permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0 Switch(config-ext-nacl)#end Switch(config)#
```
2. Inscreva o [comando vlan access-map map_name](#) e o comando action drop, que é a ação a executar. O comando vlan access-map map_name usa a lista de acesso de MAC que você criou para bloquear o tráfego ARP dos hosts.

```
Switch(config)#vlan access-map block_arp 10 Switch (config-access-map)#action drop Switch (config-access-map)#match mac address ARP_Packet
```
3. Adicione uma linha extra ao mesmo mapa do acesso de VLAN para encaminhar o resto do tráfego.

```
Switch(config)#vlan access-map block_arp 20 Switch (config-access-map)#action forward
```
4. Escolha um mapa de acesso de VLAN e aplique-o a uma interface de VLAN. Inscreva o comando VLAN filter vlan_access_map_name vlan-list vlan_number.

```
Switch(config)#vlan filter block_arp vlan-list 2
```

Configuração de exemplo

Esta configuração de exemplo cria três listas de acessos de MAC e três mapas de acesso de VLAN. A configuração aplica o terceiro mapa do acesso de VLAN à interface de VLAN 2.

3550 Switch

```
mac access-list extended ARP_Packet
permit host 0000.861f.3745 host 0006.5bd8.8c2f 0x806 0x0
!--- This blocks communication between hosts with this MAC. ! mac access-list extended ARP_ONE_OUI perm
0000.8600.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from this v
OUI. ! mac access-list extended ARP_TWO_OUI permit 0000.8600.0000 0000.00ff.ffff any 0x806 0x0 permit
0006.5b00.0000 0000.00ff.ffff any 0x806 0x0 !--- This blocks any ARP packet that originates from these
vendor OUIs. ! vlan access-map block_arp 10 action drop match mac address ARP_Packet vlan access-map
```

```
block_arp 20 action forward vlan access-map block_one_oui 10 action drop match mac address ARP_ONE_OUI
access-map block_one_oui 20 action forward vlan access-map block_two_oui 10 action drop match mac address
ARP_TWO_OUI vlan access-map block_two_oui 20 action forward ! vlan filter block_two_oui vlan-list 2 !
applies the MAC ACL name "block_two_oui" to VLAN 2.
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Você pode verificar se o switch aprendeu o endereço MAC ou a entrada de ARP antes de aplicar a ACL de MAC. Inscreva o [comando show mac-address-table](#), como este exemplo mostra.

[O analisador do CLI Cisco \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use o analisador CLI a fim ver uma análise do emissor de comando de execução.

```
switch#show mac-address-table dynamic vlan 2 Mac Address Table -----
----- Vlan Mac Address Type Ports -----
Fa0/21 2 0006.5bd8.8c2f DYNAMIC Fa0/22 Total Mac Addresses for this criterion: 2
switch#show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.2 26 0000.861f.3745 ARPA
Vlan2 Internet 10.1.1.3 21 0006.5bd8.8c2f ARPA
Vlan2 Internet 10.1.1.1 - 000d.65b6.9700 ARPA
Vlan2
```

Troubleshooting

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

Informações Relacionadas

- [Suporte ao Produto - Switches](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)