Blok ARP-pakketten met gebruik van MAC-toegangslijsten en VLAN-toegangskaarten op Catalyst 2970, 3550, 3560 en 3750 Series-switches

Inhoud

Inleiding

Dit document behandelt de configuratie voor een Cisco Catalyst 3550 Series-switch. U kunt in dit scenario elke Catalyst 2970, 3560 of 3750 Series switch gebruiken om dezelfde resultaten te bereiken. Het document demonstreert hoe u een MAC Access Control List (ACL) kunt configureren om communicatie tussen apparaten in een VLAN te blokkeren. U kunt één host of een reeks hosts blokkeren, gebaseerd op de fabrikant van de host-netwerkinterfacekaart (NIC)-adapter. U kunt een bereik van hosts blokkeren als u IP-pakketten (adresresolutie Protocol) van de hand wijst die van deze apparaten zijn gebaseerd op de IEEE Organisational Unitional Identifier (OUI) en company_id opdrachten.

In een netwerk kunt u ARP-verzoekpakketten blokkeren om de toegang van de gebruiker te beperken. In sommige netwerkscenario's, wilt u ARP-pakketten blokkeren die niet op het IP-adres zijn gebaseerd, maar op de Layer 2 MAC-adressen. U kunt dit type van beperking bereiken als u MAC-adres ACL's en VLAN-toegangskaarten maakt en deze op een VLAN-interface toepast.

Voorwaarden

Vereisten

Raadpleeg de IEEE OUI- en Company_id-opdrachten om de IEEE OUI- en Company_id-opdrachten te bepalen.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst 3550 switch.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Andere switches die de opdrachten in deze configuratie ondersteunen, omvatten Catalyst 2970, 3560 of 3750 Series-switches.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Om het MAC-adresfilter te configureren en het op de VLAN-interface toe te passen, moet u meerdere stappen voltooien. Eerst maakt u de VLAN-toegangskaarten voor elk type verkeer dat moet worden gefilterd. U selecteert een MAC-adres of een MAC-bereik voor het blokkeren. U moet ook het ARP-verkeer in de toegangslijst identificeren. In overeenstemming met RFC 826 , gebruikt een ARP frame het Ethernet protocol type van waarde 0x806. U kunt op dit protocol filteren als interessant verkeer voor de toegangslijst.

1. In de mondiale configuratiemodus moet u een genaamd MAC Extended Access List met de naam ARP_Packet maken.Voer de **uitgebreide** *ACL_name* **toegangslijst** in **en** voeg het adres of de adressen van host MAC toe die u wilt blokkeren.
```
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. Voer de **vlan access-map** *map_ name* opdracht in en de **action drop** opdracht, die de uit te voeren actie is.De **vlan access-map** *map_ name* **opdracht gebruikt de MAC access lijst die u maakte om ARP verkeer vanaf de hosts te blokkeren.**
```
Switch(config)#vlan access-map block_arp 10

Switch (config-access-map)#action drop
Switch (config-access-map)#match mac address ARP_Packet
```
3. Voeg een extra lijn aan de zelfde de toegangskaart van VLAN toe om de rest van het verkeer door te sturen.
```
Switch(config)#vlan access-map block_arp 20
Switch (config-access-map)#action forward
```
4. Kies een VLAN-toegangskaart en pas deze toe op een VLAN-interface.Voer de **VLAN filter** *vlan_access_map_name* **vlan-list** *vlan_number* **opdracht in.**
```
Switch(config)#vlan filter block_arp vlan-list 2
```

Monsterconfiguratie

Deze voorbeeldconfiguratie maakt drie MAC-toegangslijsten en drie VLAN-toegangskaarten. De configuratie past de derde toegangskaart van VLAN op interface 2 toe.

Catalyst 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 addre
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.
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

U kunt controleren of de schakelaar het adres van MAC of ARP heeft geleerd alvorens u de MAC ACL ACL toepast. Voer de opdracht show mac-adres-tabel in zoals dit voorbeeld toont.

De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show**-opdrachten. Gebruik de CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

```
switch#show mac-address-table dynamic vlan 2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address    Type        Ports
----    -----------    --------    -----
   2  0000.861f.3745 DYNAMIC     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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Productondersteuning voor switches
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems