Catalyst 2970, 3550, 3560 및 3750 Series 스위치에서 MAC 액세스 목록 및 VLAN 액세스 맵을 사용하여 ARP 패킷 차단

목차

소개

이 문서에서는 Cisco Catalyst 3550 Series 스위치의 구성에 대해 설명합니다.동일한 결과를 얻기 위해 이 시나리오에서 Catalyst 2970, 3560 또는 3750 Series 스위치를 사용할 수 있습니다.이 문서에서는 VLAN 내의 디바이스 간 통신을 차단하기 위해 MAC ACL(Access Control List)을 구성하는 방법을 보여 줍니다.호스트 NIC(Network Interface Card) 어댑터 제조업체에 따라 단일 호스트 또는 호스트 범위를 차단할 수 있습니다.IEEE OUI(Organizational Unique Identifier) 및 company_id 할당을 기반으로 이러한 디바이스에서 시작되는 ARP(Address Resolution Protocol) 패킷을 허용하지 않을 경우 호스트 범위를 차단할 수 있습니다.

네트워크에서 사용자 액세스를 제한하기 위해 ARP 요청 패킷을 차단할 수 있습니다.일부 네트워크 시나리오에서는 IP 주소가 아니라 레이어 2 MAC 주소를 기반으로 ARP 패킷을 차단하려고 합니다.MAC 주소 ACL 및 VLAN 액세스 맵을 만들고 VLAN 인터페이스에 적용하는 경우 이러한 제한 유형을 수행할 수 있습니다.

사전 요구 사항

요구 사항

IEEE OUI 및 company_id 할당을 확인하려면 IEEE OUI 및 Company_id 할당을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco Catalyst 3550 스위치를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션에서 명령을 지원하는 다른 스위치로는 Catalyst 2970, 3560 또는 3750 Series 스위치가 있습니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

MAC 주소 필터링을 구성하고 VLAN 인터페이스에 적용하려면 몇 단계를 완료해야 합니다.먼저 필터링해야 하는 각 트래픽 유형에 대한 VLAN 액세스 맵을 생성합니다.차단할 MAC 주소 또는 MAC 주소 범위를 선택합니다.또한 액세스 목록에서 ARP 트래픽을 식별해야 합니다.RFC 826 에 따라 ARP 프레임은 이더넷 프로토콜 유형 값 0x806을 사용합니다. 이 프로토콜 유형을 액세스 목록에 대한 흥미로운 트래픽으로 필터링할 수 있습니다.

1. 글로벌 컨피그레이션 모드에서 이름이 ARP_Packet인 명명된 MAC 확장 액세스 목록을 생성합니다.**mac access-list extended** *ACL_name* 명령을 입력하고 차단할 호스트 MAC 주소 또는 주소를 추가합니다.
   ```
   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. vlan **access-map** *map_name* 명령 및 **action drop** 명령을 입력합니다. 이는 수행할 작업입니다 .vlan **access-map** *map_name* **명령은** 호스트에서 ARP 트래픽을 차단하기 위해 생성한 MAC 액세스 목록을 사용합니다.
   ```
   Switch(config)#vlan access-map block_arp 10

   Switch (config-access-map)#action drop
   Switch (config-access-map)#match mac address ARP_Packet
   ```
3. 나머지 트래픽을 전달하려면 동일한 VLAN 액세스 맵에 추가 라인을 추가합니다.
   ```
   Switch(config)#vlan access-map block_arp 20
   Switch (config-access-map)#action forward
   ```
4. VLAN 액세스 맵을 선택하고 VLAN 인터페이스에 적용합니다.VLAN **filter** *vlan_access_map_name vlan*-**list** vlan_*number* 명령**을** 입력합니다.
   ```
   Switch(config)#vlan filter block_arp vlan-list 2
   ```

샘플 컨피그레이션

이 샘플 컨피그레이션에서는 MAC 액세스 목록 3개와 VLAN 액세스 맵 3개를 생성합니다.이 컨피그레이션은 세 번째 VLAN 액세스 맵을 VLAN 인터페이스 2에 적용합니다.

3550 스위치

```
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.
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

MAC ACL을 적용하기 전에 스위치가 MAC 주소 또는 ARP 항목을 학습했는지 확인할 수 있습니다 .이 예와 같이 show mac-address-table 명령을 입력합니다.

Cisco CLI Analyzer(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 CLI Analyzer를 사용합니다.

```
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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 스위치 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems