Catalyst 4500 Series 스위치의 레이어 2 컨트롤 프레임에 MAC ACL 사용

목차

소개

이 문서에서는 Catalyst 4500 시리즈 스위치의 컨트롤 플레인 비 IP 트래픽에서 MAC ACL(Access Control List)의 동작을 설명합니다.MAC ACL을 사용하여 VLAN과 물리적 레이어 2(L2) 포트에서 비 IP 트래픽을 필터링할 수 있습니다.

MAC access-list extended 명령에서 지원되는 비 IP 프로토콜에 대한 자세한 내용은 Catalyst 4500 Series Switch Cisco IOS® Command Reference를 참조하십시오.

문제

다음 컨피그레이션을 가정합니다.

```
mac access-list extended udld
 deny any host 0100.0ccc.cccc
 permit any any
!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 mac access-group udld in
!
```

> **참고:**이 ACL은 GigabitEthernet2/4 인터페이스에서 인바운드로 오는 CDP/UDLD/VTP/PAgP 프레임(대상 MAC = 0100.0ccc.cccc)과 같은 L2 제어 평면 트래픽을 거부하지 않습니다.

Catalyst 4500 스위치에는 L2 컨트롤 플레인 트래픽을 CPU로 푸시하는 시스템 생성 내장 ACL이 있으며, 이는 사용자 정의 ACL보다 우선하며, 이 트래픽을 분류하기 위한 것입니다.따라서 사용자 정의 ACL은 이러한 목적을 달성하지 못합니다.이러한 동작은 Catalyst 4500 플랫폼에만 해당되며 다른 플랫폼에는 다른 동작이 있을 수 있습니다.

솔루션

이 방법을 사용하여 인그레스 포트 또는 CPU에서 트래픽을 삭제할 수 있습니다(필요한 경우).

주의:이 단계는 특정 인터페이스에 들어오는 대상 MAC = 0100.0ccc.cccc가 있는 모든 프레임을 삭제하기 위한 것입니다.이 MAC 주소는 UDLD/DTP/VTP/Pagp 컨트롤 플레인 PDU(Protocol Data Units)에서 사용됩니다.

이 트래픽을 모두 삭제하지 않고 감시하는 것이 목표인 경우 컨트롤 플레인 폴리싱이 기본 솔루션입니다.Catalyst 4500에서 컨트롤 플레인 폴리싱 구성 참조

1단계. cdp-vtp에 대한 제어 패킷 QoS(Quality of Service)를 활성화합니다.

```
Catalyst4500(config)#qos control-packets cdp-vtp
```

이 단계에서는 시스템에서 생성된 ACL을 생성합니다.

```
Catalyst4500#show run | begin system-control

mac access-list extended system-control-packet-cdp-vtp
 permit any host 0100.0ccc.cccc
```

참고:앞서 생성한 시스템 정의 ACL 대신 MAC ACL이라는 사용자 정의 ACL을 사용할 수도 있습니다.TCAM(Ternary Content Addressable Memory) 리소스를 저장하려면 시스템 생성 또는 사용자 정의 ACL을 사용합니다.

```
mac access-list extended udld
 permit any host 0100.0ccc.cccc
```

2단계. 이 ACL에 도달하는 트래픽을 매칭하기 위해 클래스 맵을 만듭니다.

```
Catalyst4500(config)#class-map cdp-vtp
Catalyst4500(config-cmap)#match access-group name system-control-packet-cdp-vtp
Catalyst4500(config-cmap)#end
Catalyst4500#
```

3단계. conform action = drop and exceed action = drop:

```
Catalyst4500(config)#policy-map cdp-vtp-policy
Catalyst4500(config-pmap)#class cdp-vtp
Catalyst4500(config-pmap-c)#police 32000 conform-action drop exceed-action drop
Catalyst4500(config-pmap-c-police)#end
Catalyst4500#
```

4단계. 이 트래픽을 삭제해야 하는 L2 포트에 정책 맵 인바운드를 적용합니다.

```
Catalyst4500(config)#int gigabitEthernet 2/4
Catalyst4500(config-if)#service-policy input cdp-vtp-policy
Catalyst4500(config-if)#end

!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 service-policy input cdp-vtp-policy
end
```

다른 L2 제어 프레임에서 폴리싱하거나 삭제해야 하는 경우 유사한 시스템 생성 ACL을 사용할 수 있습니다.이미지에 표시된 대로 자세한 내용은 레이어 2 제어 패킷 QoS를 참조하십시오.

```
Catalyst4500(config)#qos control-packets ?
 bpdu-range       Enable QoS on BPDU-range packets
 cdp-vtp          Enable QoS on CDP and VTP packets
 eapol            Enable QoS on EAPOL packets
 lldp             Enable QoS on LLDP packets
 protocol-tunnel  Enable QoS on protocol tunneled packets
 sstp             Enable QoS on SSTP packets
 <cr>
```

Type of Packet that the Feature is Enabled On	Range of Address the Feature Acts On
BPDU-range	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 EAPOL
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD
LLDP	0180.C200.000E