Gebruik MAC ACL voor Layer 2 Control frames op Catalyst 4500 Series-switches

Inhoud

Inleiding

Dit document beschrijft het gedrag van MAC Access Control List (MAC ACL) op het besturingsplane voor niet-IP-verkeer op Catalyst 4500 Series-switches. MAC ACL kan worden gebruikt om niet-IP verkeer op een VLAN en op een fysieke Layer 2 (L2) poort te filteren.

Voor meer informatie over de ondersteunde niet-IP protocollen in de uitgebreide opdracht van MAC access-list, zie Catalyst 4500 Series switch Cisco IOS® Opdrachtreferentie.

Probleem

Stel deze configuratie in:

```
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
!
```

> Opmerking: Deze ACL ontkent geen L2-besturingsplaneverkeer zoals CDP/UDLD/VTP/PAgP-frames met bestemming MAC = 100.0cc.cc.cc die inkomende in interface Gigabit Ethernet2/4 komt.

Op Catalyst 4500-switches is er een systeem dat ingebouwde ACL gegenereerd heeft en L2-besturingsplane slaat op CPU en deze krijgt voorrang op een door gebruiker gedefinieerde ACL, om dit verkeer naar classificatie te classificeren. Daarom bereikt een door gebruiker gedefinieerde ACL niet dit doel. Dit gedrag is specifiek voor Catalyst 4500 platform, andere platforms zouden verschillende gedragingen kunnen hebben.

Oplossing

Deze methode kan worden gebruikt om het verkeer bij ingangspoorten of bij CPU's te laten vallen

wanneer dit nodig is.

> **Voorzichtig:** Stappen hier zijn bedoeld om alle frames te laten vallen die bestemmings-MAC = 0100.0cc.ccc hebben die op een specifieke interface worden ontvangen. Dit MAC-adres wordt gebruikt door UDLD/DTP/VTP/Pagp besturingsplane Data Units (PDU's).

Als het doel is om dit verkeer te controleren en niet alles te laten vallen, dan is controle op vliegtuigen een voorkeursoplossing. Raadpleeg Toezicht besturingsplane configureren op Catalyst 4500

Stap 1. Schakel QoS (Control-Packet Quality of Service) in voor cdp-vtp:

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

Deze stap genereert een systeem dat ACL gegenereerd heeft:

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

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

> Opmerking: Een door de gebruiker gedefinieerde MAC ACL (zoals hier weergegeven) kan ook worden gebruikt in plaats van systeem gedefinieerd ACL zoals eerder gegenereerd. Gebruik systeem dat gegenereerd is of door de gebruiker gedefinieerd ACL om Ternaire Content Adresseerbare Geheugenbronnen (TCAM) op te slaan.

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

Stap 2. Maak een class-map om het verkeer dat deze ACL raakt aan te passen:

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

Stap 3. Maak een beleidsplan en politieverkeer dat bij Stap 2 class met conforme actie = drop en groter dan actie = 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#
```

Stap 4. Pas de beleidskaart toe die op de L2 poort is ingestuurd, waar dit verkeer moet worden teruggebracht:

```
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
```

Een soortgelijk systeem heeft ACL's (ACL's) gegenereerd voor gebruik in andere L2-besturingsframes voor het geval dat deze moeten worden gecontroleerd of ingetrokken. Raadpleeg Layer 2 Control Packet QoS voor meer informatie en zoals in de afbeelding.

```
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