Uso di ACL MAC per i frame di controllo di layer 2 sugli switch Catalyst serie 4500

Sommario

Introduzione

In questo documento viene descritto il comportamento di MAC Access Control List (MAC ACL) sul piano di controllo e sul traffico non IP sugli switch Catalyst serie 4500. È possibile usare ACL MAC per filtrare il traffico non IP su una VLAN e su una porta fisica di layer 2 (L2).

Per ulteriori informazioni sui protocolli non IP supportati nel comando MAC access-list extended, consultare la guida di riferimento dei comandi degli switch Catalyst serie 4500 Cisco IOS®.

Problema

Si supponga che la configurazione

```
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
!
```

> **Nota:** Questo ACL non nega il traffico del control plane L2, come i frame CDP/UDLD/VTP/PAgP con MAC di destinazione = 0100.0ccc.ccc in entrata nell'interfaccia Gigabit Ethernet2/4.

Sugli switch Catalyst 4500, è presente un ACL integrato generato dal sistema che punta il traffico del control plane L2 alla CPU. Per classificare il traffico, tale ACL ha la precedenza su un ACL definito dall'utente. Pertanto, un ACL definito dall'utente non raggiunge questo scopo. Questo comportamento è specifico della piattaforma Catalyst 4500 e altre piattaforme potrebbero avere comportamenti diversi.

Soluzione

Questo metodo può essere utilizzato per rilasciare il traffico sulla porta di entrata o sulla CPU, se

necessario.

> **Attenzione:** Questa procedura ha lo scopo di eliminare tutti i frame con MAC di destinazione = 0100.0ccc.ccc in entrata su un'interfaccia specifica. Questo indirizzo MAC è utilizzato dalle unità dati del protocollo (PDU) UDLD/DTP/VTP/Pagp.

Se l'obiettivo è sorvegliare questo traffico e non farlo cadere tutto, control plane policing è una soluzione preferibile. Per ulteriori informazioni, fare riferimento al documento sulla [configurazione del Control Plane Policing su Catalyst 4500]

Passaggio 1. Abilitare Control-Packet Quality of Service (QoS) per cdp-vtp:

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

Questo passaggio genera un ACL generato dal sistema:

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

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

> **Nota:** È possibile usare anche un ACL MAC definito dall'utente (come mostrato qui) anziché un ACL definito dal sistema e generato in precedenza. Usare un ACL generato dal sistema o definito dall'utente per salvare le risorse TCAM (Ternary Content Addressable Memory).

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

Passaggio 2. Per creare una mappa delle classi in modo che corrisponda al traffico che raggiunge questo ACL, effettuare le operazioni riportate di seguito.

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

Passaggio 3. Creare una mappa dei criteri e il traffico della polizia che corrispondano alla classe del Passaggio 2 con l'azione di conformità = rilascio e superamento = rilascio:

```
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#
```

Passaggio 4. Applicare la mappa dei criteri in entrata sulla porta L2 da cui deve essere eliminato il traffico:

```
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
```

ACL simili generati dal sistema possono essere usati per altri frame di controllo L2 nel caso in cui abbiano bisogno di essere controllati o scartati. Per ulteriori informazioni, consultare il documento QoS sul controllo di livello 2 come mostrato nell'immagine.

```
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