對Catalyst 4500系列交換器上的第2層控制訊框使用MAC ACL

目錄

簡介

本檔案將說明Catalyst 4500系列交換器上控制平面非IP流量的MAC存取控制清單(MAC ACL)的行為。MAC ACL可用於過濾VLAN和實體第2層(L2)連線埠上的非IP流量。

有關MAC access-list extended命令中支援的非IP協定的詳細資訊，請參閱Catalyst 4500系列交換機Cisco IOS®命令參考。

問題

假設以下設定：

```
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
!
```

> **附註**：此ACL不會拒絕目的MAC為0100.0ccc的CDP/UDLD/VTP/PAgP幀等傳入介面GigabitEthernet2/4的第2層控制平面流量。

在Catalyst 4500交換器上，有一個系統產生的內建ACL，會將L2控制平面流量強制推送至優先於使用者定義ACL的CPU，以便對此流量進行分類。因此，使用者定義ACL無法達成此目的。此行為特定於Catalyst 4500平台，其他平台可能有不同的行為。

解決方案

如果有必要，此方法可用於丟棄入口埠或CPU上的流量。

> **注意**：此處的步驟旨在刪除特定介面上傳入的目標MAC = 0100.0ccc.cccc的所有幀。UDLD/DTP/VTP/Pagp控制平面協定資料單元(PDU)使用此MAC地址。

如果目標是管制此流量而不是丟棄所有流量，則控制平面策略是首選解決方案。請參閱在Catalyst 4500上設定控制階段管制

步驟1.為cdp-vtp啟用控制資料包服務品質(QoS):

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

此步驟生成系統生成的ACL:

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

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

> **附註**：也可以使用使用者定義的命名MAC ACL（如此處所示），而不是先前生成的系統定義ACL。使用系統生成的或使用者定義的ACL來儲存三重內容可定址儲存器(TCAM)資源。

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

步驟2.建立類別對映以匹配到達此ACL的流量：

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

步驟3.建立策略對映並管制與步驟2類匹配且具有conform action = drop和exceed action = drop的流量：

```
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#
```

步驟4.在需要捨棄此流量的L2連線埠上套用原則圖傳入：

```
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
```

類似的系統生成的ACL可用於其他L2控制幀，以備在需要對其進行管制或丟棄時使用。有關詳細資訊，請參閱第2層控制資料包QoS，如下圖所示。

```
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