在Catalyst 4500系列交换机上为第2层控制帧使用MAC ACL

目录

简介

本文档介绍Catalyst 4500系列交换机上控制平面非IP流量上MAC访问控制列表(MAC ACL)的行为。MAC ACL可用于过滤VLAN和物理第2层(L2)端口上的非IP流量。

有关MAC access-list extended命令中支持的非IP协议的详细信息，请参阅Catalyst 4500系列交换机Cisco IOS®命令参考。

问题

假设采用以下配置：

```
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
!
```

> **注意**：此ACL不拒绝L2控制平面流量，例如目的MAC = 0100.0ccc.cccc的CDP/UDLD/VTP/PAgP帧，该帧传入接口GigabitEthernet2/4。

在Catalyst 4500交换机上，有一个系统生成的内置ACL，它将L2控制平面流量传送到CPU，该CPU优先于用户定义的ACL，以便对此流量进行分类。因此，用户定义的ACL无法实现此目的。此行为特定于Catalyst 4500平台，其他平台可能具有不同的行为。

解决方案

如果需要，此方法可用于丢弃入口端口或CPU上的流量。

> **警告**：此处的步骤旨在丢弃特定接口上进入的目的MAC = 0100.0ccc.cccc的所有帧。此MAC地址由UDLD/DTP/VTP/Pagp控制平面协议数据单元(PDU)使用。

如果目标是管制此流量而不是丢弃所有流量，则控制平面策略是首选解决方案。请参阅在Catalyst 4500上配置控制平面策略

步骤1.为cdp-vtp启用控制数据包服务质量(QoS):

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

此步骤生成系统生成的ACL:

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

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

注意：用户定义的命名MAC ACL（如图所示）也可以用于代替先前生成的系统定义ACL。使用系统生成的ACL或用户定义的ACL来保存三态内容可寻址存储器(TCAM)资源。

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

步骤2.创建类映射以匹配到达此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#
```

步骤3.创建策略映射并管制与步骤2类匹配的流量，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#
```

步骤4.在需要丢弃此流量的L2端口上应用入站策略映射：

```
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
```

类似的系统生成的ACL可用于其他L2控制帧，以防其需要被管制或丢弃。如图所示，请参阅第2层控制数据包QoS了解详细信息。

```
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