请使用MAC ACL在Catalyst 4500系列交换机的Layer2控制帧

目录

简介

MAC访问控制表(MAC ACL)可以用于过滤非IP数据流在VLAN和在物理层2端口。 本文描述MAC ACL行为在控制层面非IP数据流的在Catalyst 4500系列交换机。

关于在mac access-list扩展的命令的支持的非IP协议的更多信息，请参考Catalyst 4500系列交换机cisco ios命令参考资料。

问题

assume在配置后：

```
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不会拒绝Layer2控制层面流量类似CDP/UDLD/VTP/PAgP帧用目的地MAC = 0100.0ccc.cccc来入站在接口GigabitEthernet2/4。

在Catalyst 4500交换机上，有系统生成的内藏的ACL优先于用户定义的ACL分类此流量的该平底船Layer2控制层面流量对CPU。因此用户定义的ACL不达到此目的。此行为是特定对Catalyst 4500平台，其他平台可能有不同的行为。

如果有需要如此，执行以下方法可以用于降低此流量在入站端口或在CPU。

解决方案

下面的步骤打算丢弃有进来在一个特定接口的目的地MAC = 0100.0ccc.cccc的所有帧。UDLD/DTP/VTP/Pagp控制层面使用此MAC地址PDU。请注意。

如果目标将修正此流量和不下降所有，控制平面策略是首选的解决方案。请参考配置在Catalyst 4500的控制平面策略

步骤1) cdp VTP的Enable (event)控制数据包QoS。

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

此步骤生成跟随的系统生成的ACL

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

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

注意：MAC ACL ()ACLACLTCAM

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

步骤2)创建类映射匹配点击此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)创建策略映射并且修正匹配在类上的流量与一致action=丢弃并且超出action=丢弃

```
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)应用策略映射入站在此流量需要丢弃的Layer2端口。

```
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
```

万一他们需要被管辖或丢弃，相似的系统生成的ACL可以用于其他Layer2控制帧。请参考Layer2控制数据包QoS关于详细信息。

```
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