请使用MAC ACL第2层在Catalyst 4500 Series Switches的控制帧

目录

简介

本文描述工作情况MAC访问控制表(MAC ACL)在Catalyst 4500 series switches的控制层面非IP数据流。MAC ACL可以用于为了过滤非IP数据流在VLAN和在一个物理层2 (L2)端口。

关于在Mac access-list被扩大的命令的支持的非IP协议的更多信息，请参考Catalyst 4500 Series Switch Cisco IOS命令参考资料。

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
!
```

> **Note**:此ACL不否决L2控制层面数据流类似与的CDP/UDLD/VTP/PAgP帧来入站在接口GigabitEthernet2/4的目的地MAC = 0100.0ccc.cccc。

在Catalyst 4500 switches，有踢L2控制层面数据流对CPU优先于用户定义的ACL，为了分类此数据流的系统生成的内藏的ACL。因此，用户定义的ACL不达到此目的。此工作情况是特定的对Catalyst 4500平台，其他平台也许有不同的工作情况。

解决方案

如果有需要如此，执行此方法可以用于降低数据流在进入端口或在CPU。

> **Caution**:这里步骤打算丢弃有目的地MAC = 0100.0ccc.cccc在一个特定接口进来的所有帧。UDLD/DTP/VTP/Pagp控制层面协议数据单元使用此MAC地址(PDUs)。

如果目标将修正此数据流和不下降所有，控制平面策略是一个首选的解决方案。参考配置在Catalyst 4500的控制平面策略

步骤1. Enable (event) cdp VTP的控制信息包服务质量(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
```

> **Note**:用户定义的已命名MAC ACL (如显示这里)可能也使用而不是系统被定义的ACL如生成前。请使用系统生成或用户定义的ACL为了节约三重内容可编址存储器资源。

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

步骤2.创建一class-map为了匹配击中此ACL的数据流：

```
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.创建一个策略映射并且修正匹配第2步组一致action=丢弃的数据流并且超出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.适用策略映射入站在此数据流需要降低的L2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下降，相似的系统生成的ACL可以用于其他L2控制帧。如镜像所显示，参考第2层控制数据包QoS关于详细资料和。

```
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