Используйте ACL MAC для управляющих фрейм уровня 2 на коммутаторах серии Catalyst 4500

Содержание

Введение

Список контроля доступа MAC (ACL MAC) может использоваться для фильтрации не-IP трафик на VLAN и на порту физического уровня 2. Этот документ описывает поведение ACL MAC на не-IP трафик уровня управления на Коммутаторах серии Catalyst 4500.

Для получения дополнительной информации о поддерживаемых протоколах не-IP в команде mac access-list extended, обратитесь Ссылку Команды Cisco IOS Коммутатора серии Catalyst 4500.

Проблема

Примите следующую конфигурацию:

```
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
!
```

Обратите внимание на то, что этот ACL не запретит трафик уровня управления Уровня 2 как CDP/UDLD/VTP/кадры PAgP с получателем MAC = 0100.0ccc.cccc прибытие входящего в интерфейсном GigabitEthernet2/4.

На коммутаторах Catalyst 4500 существует генерируемый встроенный ACL системы, который плывет на плоскодонке трафик уровня управления Уровня 2 к ЦП, который имеет приоритет по определяемому пользователем ACL для классификации этого трафика. Следовательно определяемый пользователем ACL не достигает этой цели. Это поведение является определенным для платформы Catalyst 4500, другие платформы могут иметь другие способы поведения.

Если существует потребность сделать так, следующий метод может использоваться для отбрасывания этого трафика во входном порту или в ЦП.

Решение

Шаги ниже предназначены для отбрасывания всех кадров, которые имеют получателя MAC = 0100.0ccc.cccc входящий на определенном интерфейсе. Этот MAC-адрес используется PDU уровня управления UDLD/DTP/VTP/Pagp. Проявите осторожность.

Если цель состоит в том, чтобы определить политику этого трафика и не отбросить все это, контроль уровня управления является предпочтительным решением. Обратитесь Контроль уровня управления Настройки на Catalyst 4500

Шаг 1), Включают QoS управляющего пакета для vtp cdp.

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

Этот шаг генерирует генерируемый ACL следующей системы

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

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

> **Примечание:** Определяемый пользователем именованный ACL MAC (как показано ниже) может также использоваться вместо определенного ACL системы, как генерируется выше. Используйте или систему генерируемый или определяемый пользователем ACL для сохранения ресурсов TCAM.

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

Шаг 2), Создают class-map для соответствия с трафиком, который поражает этот ACL.

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

Шаг 3), Создают карту политик и определяют политику трафика, совпадающего выше класса с действием согласования = отбрасывание и действие в случае превышения = отбрасывание

```
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#
```

Шаг 4), Применяют policy-map, входящий на порт Уровня 2, где должен быть отброшен этот трафик.

```
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
```

Генерируемые ACL аналогичной системы могут использоваться для других управляющих

фрейм Уровня 2 в случае, если они должны охраняться или отбрасываться. Обратитесь QoS Управляющего пакета Уровня 2 для подробных данных.

```
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