Use MAC ACL para frames de controle da camada 2 em Catalyst 4500 Series Switch

Índice

Introdução

Este original descreve o comportamento do Access Control List MAC (MAC ACL) no tráfego não-IP do plano do controle em Catalyst 4500 Series Switch. O MAC ACL pode ser usado a fim filtrar o tráfego não-IP em um VLAN e em uma porta da camada física 2 (L2).

Para obter mais informações sobre dos protocolos não-IP apoiados no comando estendido lista de acesso MAC, consulte a referência de comandos do ® do Cisco IOS do Catalyst 4500 Series Switch.

Problema

Supõe esta configuração:

```
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**: Este ACL não nega o tráfego plano do controle L2 como quadros CDP/UDLD/VTP/PAgP com MAC de destino = 0100.0ccc.cccc que vem de entrada na relação GigabitEthernet2/4.

Em Catalyst 4500 Switch, há um sistema o ACL inerente gerado que tráfego plano do controle dos pontapés L2 ao CPU que toma a precedência sobre um ACL definido pelo utilizador, a fim classificar este tráfego. Daqui, um ACL definido pelo utilizador não consegue esta finalidade. Este comportamento é específico à plataforma do Catalyst 4500, outras Plataformas pôde ter comportamentos diferentes.

Solução

Este método pode ser usado para deixar cair o tráfego na porta de ingresso ou no CPU, se há uma necessidade de fazer assim.

> **Caution**: As etapas aqui são pretendidas deixar cair todos os quadros que têm o MAC de destino = o 0100.0ccc.cccc que vem dentro em uma relação específica. Este MAC address é usado pelas unidades de dados de protocolo do plano do controle UDLD/DTP/VTP/Pagp (PDU).

Se o objetivo é policiar este tráfego e não deixar cair todo o ele, o Policiamento do plano de controle é uma solução preferida. Consulte configurando o Policiamento do plano de controle no Catalyst 4500

Etapa 1. Permita o Qualidade de Serviço (QoS) do pacote de controle para o CDP-VTP:

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

Esta etapa gerencie um ACL gerado sistema:

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

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

> **Note**: Um MAC Nomeado definido pelo utilizador ACL (como mostrado aqui) pode igualmente ser usado em vez do ACL definido sistema como gerado mais cedo. Use o ACL gerado ou definido pelo utilizador do sistema a fim salvar recursos do Ternary Content Addressable Memory (TCAM).

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

Etapa 2. Crie um mapa de classe a fim combinar o tráfego que bate este ACL:

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

Etapa 3. Crie um mapa de política e um tráfego da polícia que classe de etapa 2 dos fósforos com conform action = gota e ação excedada = gota:

```
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#
```

Etapa 4. Aplique o mapa de política de entrada na porta L2 onde este tráfego precisa de ser deixado cair:

```
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
```

Sistema similar os ACL gerados podem ser usados para outros frames de controle L2 caso que precisam de ser policiados ou deixado cair. Consulte o pacote de controle QoS da camada 2 para detalhes e segundo as indicações da imagem.

```
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