Usar a ACL MAC para quadros de controle da camada 2 nos switches Catalyst 4500 Series

Contents

Introduction

Este documento descreve o comportamento da Lista de Controle de Acesso MAC (MAC ACL - MAC Access Control List) no plano de controle do tráfego não-IP nos switches da série Catalyst 4500. A ACL MAC pode ser usada para filtrar o tráfego não-IP em uma VLAN e em uma porta física de Camada 2 (L2).

Para obter mais informações sobre os protocolos não-IP suportados no comando MAC access-list extended, consulte a Referência de Comandos do Cisco IOS® do Catalyst 4500 Series Switch.

Problema

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

Nos switches Catalyst 4500, há uma ACL interna gerada pelo sistema que direciona o tráfego do plano de controle L2 para a CPU, que tem precedência sobre uma ACL definida pelo usuário, para classificar esse tráfego. Portanto, uma ACL definida pelo usuário não atinge essa finalidade. Esse comportamento é específico da plataforma Catalyst 4500, outras plataformas podem ter comportamentos diferentes.

Solução

Esse método pode ser usado para descartar o tráfego na porta de entrada ou na CPU, se houver necessidade de fazê-lo.

> **Caution**: As etapas aqui são destinadas a descartar todos os quadros que têm MAC de destino = 0100.0ccc.ccc que entra em uma interface específica. Esse endereço MAC é usado por UDLD/DTP/VTP/Pagp control plane Protocol Data Units (PDUs).

Se o objetivo é policiar esse tráfego e não descartá-lo totalmente, a vigilância do plano de controle é uma solução preferida. Consulte Configurando o policiamento de plano de controle no Catalyst 4500

Etapa 1. Habilitar QoS (Qualidade de Serviço) do pacote de controle para cdp-vtp:

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

Esta etapa gera uma ACL gerada pelo sistema:

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

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

> **Note**: Uma ACL MAC nomeada definida pelo usuário (como mostrado aqui) também pode ser usada em vez da ACL definida pelo sistema como gerada anteriormente. Use a ACL gerada pelo sistema ou definida pelo usuário para salvar os recursos da TCAM (Ternary Content Addressable Memory).

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

Etapa 2. Crie um mapa de classe para corresponder ao tráfego que atinge esta 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 políticas e policie o tráfego que corresponda à classe da Etapa 2 com a ação de conformidade = queda e ação excedida = queda:

```
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 a entrada do mapa de política na porta L2 onde esse tráfego precisa ser descartado:

```
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
```

ACLs geradas pelo sistema semelhantes podem ser usadas para outros quadros de controle L2 caso precisem ser policiados ou descartados. Consulte QoS do pacote de controle da camada 2 para obter detalhes e como mostrado na 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