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

Índice

Introdução

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

Para obter mais informações sobre dos protocolos não-IP apoiados no comando estendido lista de acesso do Mac, consulte a referência do comando cisco ios do Catalyst 4500 Series Switch.

Problema

Assume depois da 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 que este ACL não negará o tráfego plano do controle da camada 2 como quadros CDP/UDLD/VTP/PAgP com o MAC de destino = a vinda 0100.0ccc.cccc de entrada na relação GigabitEthernet2/4.

Em Catalyst 4500 Switch, há um sistema o ACL inerente gerado que os pontapés mergulham o tráfego plano de 2 controles ao CPU que toma a precedência sobre um ACL definido pelo utilizador para classificar este tráfego. Daqui um ACL definido pelo utilizador não consegue esta finalidade. Este comportamento é específico à plataforma do Catalyst 4500, outras Plataformas pode ter comportamentos diferentes.

O seguinte método pode ser usado para deixar cair este tráfego na porta de ingresso ou no CPU se há uma necessidade de fazer assim.

Solução

As etapas abaixo são pretendidas deixar cair todos os quadros que têm o MAC de destino = o

0100.0ccc.cccc que vêm dentro em uma relação específica. Este MAC address é usado pelo plano PDU do controle UDLD/DTP/VTP/Pagp. Exercite por favor o cuidado.

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 por favor configurando o Policiamento do plano de controle no Catalyst 4500

Etapa 1) Permita o pacote de controle QoS para o CDP-VTP.

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

Esta etapa gerencie o ACL gerado sistema de seguimento

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

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

> Nota: Um MAC Nomeado definido pelo utilizador ACL (como mostrado abaixo) pode igualmente ser usado em vez do ACL definido sistema como gerado acima. Use por favor o ACL gerado ou definido pelo utilizador do sistema para salvar recursos TCAM.

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

Etapa 2) Crie um mapa de classe para 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 combinam acima da classe com a conform action = a gota e a ação excedada = a 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 da camada 2 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 da camada 2 caso que precisam de ser policiados ou deixado cair. Consulte por favor o pacote de controle QoS da camada 2 para detalhes.

```
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