Utilice MAC ACL para tramas de control de capa 2 en switches Catalyst serie 4500

Contenido

Introducción

Este documento describe el comportamiento de la lista de control de acceso MAC (MAC ACL) en el plano de control que no es tráfico IP en los switches Catalyst de la serie 4500. MAC ACL se puede utilizar para filtrar el tráfico que no es de IP en una VLAN y en un puerto físico de capa 2 (L2).

Para obtener más información sobre los protocolos no IP soportados en el comando MAC access-list extended, refiérase a la Referencia de Comandos de Cisco IOS® del Switch de la Serie Catalyst 4500.

Problema

Suponga esta configuración:

```
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
!
```

> **Nota:** Esta ACL no niega el tráfico del plano de control L2 como las tramas CDP/UDLD/VTP/PAgP con MAC de destino = 0100.0ccc.cccc que ingresan en la interfaz GigabitEthernet2/4.

En los switches Catalyst 4500, hay una ACL integrada generada por el sistema que impulsa el tráfico del plano de control L2 a la CPU que tiene prioridad sobre una ACL definida por el usuario, para clasificar este tráfico. Por lo tanto, una ACL definida por el usuario no logra este propósito. Este comportamiento es específico de la plataforma Catalyst 4500; otras plataformas pueden tener diferentes comportamientos.

Solución

Este método se puede utilizar para descartar el tráfico en el puerto de ingreso o en la CPU, si es necesario hacerlo.

> **Precaución:** Los pasos aquí están destinados a descartar todas las tramas que tienen MAC de destino = 0100.0ccc.cccc que ingresan en una interfaz específica. Las unidades de datos del protocolo (PDU) del plano de control UDLD/DTP/VTP/Pagp utilizan esta dirección MAC.

Si el objetivo es controlar este tráfico y no descartarlo todo, la regulación del plano de control es una solución preferida. Consulte Configuración de Control Plane Policing en Catalyst 4500

Paso 1. Habilitar calidad de servicio (QoS) de paquete de control para cdp-vtp:

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

Este paso genera una ACL generada por el sistema:

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

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

> **Nota:** También se puede utilizar una ACL MAC definida por el usuario (como se muestra aquí) en lugar de la ACL definida por el sistema como se generó anteriormente. Utilice la ACL generada por el sistema o definida por el usuario para guardar los recursos de la Memoria direccionable de contenido ternario (TCAM).

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

Paso 2. Cree un mapa de clase para que coincida con el tráfico que llega a 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#
```

Paso 3. Cree un mapa de políticas y controle el tráfico que coincida con la clase del paso 2 con acción conforme = acción de descartar y exceder = descartar:

```
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#
```

Paso 4. Aplique el policy-map inbound en el puerto L2 donde este tráfico debe 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
```

Las ACL generadas por el sistema similares se pueden utilizar para otras tramas de control L2 en caso de que deban controlarse o eliminarse. Consulte QoS del paquete de control de capa 2 para obtener más detalles y como se muestra en la imagen.

```
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