Utilice MAC ACL para los marcos del control de la capa 2 en los Catalyst 4500 Series Switch

Contenido

Introducción

Este documento describe el comportamiento de la lista de control de acceso MAC (MAC ACL) en el tráfico no IP del avión del control en los Catalyst 4500 Series Switch. El MAC ACL se puede utilizar para filtrar el tráfico no IP en un VLA N y en un puerto de la Capa física 2 (L2).

Para más información sobre los protocolos utilizados no-IP en el comando ampliado acceso-lista MAC, refiera la referencia del comando del ® del Cisco IOS del Catalyst 4500 Series Switch.

Problema

Asuma 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
!
```

> **Note**: Este ACL no niega el tráfico del plano del control L2 como los marcos CDP/UDLD/VTP/PAgP con el destino MAC = 0100.0ccc.cccc que venga entrante en el interfaz GigabitEthernet2/4.

En los Catalyst 4500 Switch, hay un ACL incorporado generado del sistema que lleva en batea el tráfico del plano del control L2 a la CPU que toma la precedencia sobre un ACL definido por el usario, para clasificar este tráfico. Por lo tanto, un ACL definido por el usario no alcanza este propósito. Este comportamiento es específico a la plataforma del catalizador 4500, otras Plataformas pudo tener diversos comportamientos.

Solución

Este método se puede utilizar para caer el tráfico en el puerto de ingreso o en la CPU, si hay una

necesidad de hacer tan.

> **Caution**: Los pasos aquí se piensan para caer todos los marcos que tienen destino MAC = 0100.0ccc.cccc que venga adentro en un interfaz específico. Esta dirección MAC es utilizada por las unidades de datos de protocolo del avión del control UDLD/DTP/VTP/Pagp (PDUs).

Si el objetivo es limpiar este tráfico y no caer todo ello, las Políticas del plano de control son una solución preferida. Refiérase configurando las Políticas del plano de control en el catalizador 4500

Paso 1. Calidad de Servicio (QoS) del control-paquete del permiso para el cdp-vtp:

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

Este paso genera un ACL generado del sistema:

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

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

> **Note**: Un MAC Nombrado definido por el usario ACL (como se muestra aquí) se puede también utilizar en vez del ACL definido sistema según lo generado anterior. Utilice ACL generado del sistema o definido por el usario para salvar los recursos ternarios del Content Addressable Memory (TCAM).

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

Paso 2. Cree una clase-correspondencia para hacer juego el tráfico que golpea 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#
```

Paso 3. Cree una correspondencia de la directiva y el tráfico de la policía con el cual hace juego la clase del paso 2 conforman acción = descenso y excede la acción = el descenso:

```
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 la directiva-correspondencia entrante en el puerto L2 donde este tráfico necesita ser caído:

```
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
```

Los ACL generados del sistema similares se pueden utilizar para otros marcos del control L2 en caso de que necesiten ser limpiados o ser caídos. Refiera el paquete de control de la capa 2 QoS para los detalles y tal y como se muestra en de 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