

# Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

## Introducción

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

Para más información sobre los protocolos soportados del no IP en el comando ampliado lista de acceso del mac, refiera la referencia del comando cisco ios del Catalyst 4500 Series Switch.

## Problema

Assume después de la configuración:

Observe que este ACL no negará el tráfico del plano del control de la capa 2 como las tramas CDP/UDLD/VTP/PAgP con el MAC de destino = venir 0100.0ccc.cccc entrante en la interfaz GigabitEthernet2/4.

En los Catalyst 4500 Switch, hay un ACL incorporado generado del sistema que las bateas acodan el tráfico del plano de 2 controles al CPU que toma la precedencia sobre un ACL definido por el usuario para clasificar este tráfico. Por lo tanto un ACL definido por el usuario no alcanza este propósito. Este comportamiento es específico a la plataforma del Catalyst 4500, otras Plataformas puede tener diversos comportamientos.

El método siguiente se puede utilizar para caer este tráfico en el puerto de ingreso o en el CPU si hay una necesidad de hacer tan.

## Solución

Los pasos abajo se piensan para caer todas las tramas que tengan el MAC de destino = 0100.0ccc.cccc que vienen adentro en una interfaz específica. Esta dirección MAC es utilizada por el avión PDU del control UDLD/DTP/VTP/Pagp. Ejercite por favor la precaución.

Si el objetivo es limpiar este tráfico y no caer todo ello, las Políticas del plano de control son una solución preferida. Refiérase por favor [configurando las Políticas del plano de control en el Catalyst 4500](#)

**Paso 1)** Paquete de control QoS del permiso para el CDP-VTP.

Este paso genera el ACL generado del sistema de siguiente

Nota: Un MAC Nombrado definido por el usuario ACL (como se muestra abajo) se puede también utilizar en vez del ACL definido sistema según lo generado arriba. Utilice por favor ACL generado del sistema o definido por el usuario para salvar a los Recursos TCAM.

**Paso 2)** Cree un clase-mapa para hacer juego el tráfico que golpea este ACL.

**Paso 3)** Cree un tráfico de la correspondencia de políticas y de la policía que corresponde con sobre la clase con la acción de conformidad = el descenso y la acción de excedente = el descenso

**Paso 4)** Aplique el directiva-mapa entrante en el puerto de la capa 2 en donde este tráfico necesita ser caído.

Los ACL generados del sistema similares se pueden utilizar para otras tramas de control de la capa 2 en caso de que necesiten ser limpiados o ser caídos. Refiera por favor el [paquete de control QoS de la capa 2](#) para los detalles.

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