

Soportar los protocolos heredados con el Catalyst 4000 Supervisor III/IV

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Ruteo de IPX](#)

[Características admitidas](#)

[Limitaciones](#)

[Ruteo de AppleTalk](#)

[Características admitidas](#)

[Limitaciones](#)

[Ruteo a través de un Router Externo](#)

[Mejoras de rendimiento adicionales](#)

[DLSw](#)

[Paquetes de filtración del no IP con las correspondencias extendidas MAC ACL y del VLA N](#)

[Otras funciones no compatibles](#)

[Alto nivel de CPU después de habilitar el ruteo AppleTalk o IPX](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo los protocolos heredados tales como IPX, AppleTalk y Conmutación de link de datos (DLSw) son admitidos de mejor manera en un switch Catalyst 4000/4500 equipado con el Supervisor III/IV más reciente. Diseñan a este supervisor al switch de hardware versión IP 4 paquetes (del IPv4).

prerrequisitos

Requisitos

Los Quien lea este documento deben tener conocimiento de cómo configurar el IPX, el APPLETALK, y DLSw. Para la información sobre estos protocolos, refiera a estas páginas de soporte:

- [Página de soporte de la tecnología IPX](#)
- [Página de soporte de la tecnología del APPLETALK](#)

- [Página de soporte de la tecnología DLSw](#)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 4507R con el Supervisor IV
- Software Release 12.1(13)EW de Cisco IOS®

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Ruteo de IPX

Rutear el IPX se soporta en el Cisco IOS Software Release 12.1(12c)EW y Posterior. En la versión inicial, el funcionamiento está en el rango de 20 a 30 kpps; a partir del Cisco IOS Software Release 12.1(13)EW, se ha aumentado a 80 a 90 kpps. Se recomienda que usted utiliza el Cisco IOS Software Release 12.1(19)EW o Posterior debido a la Disponibilidad de una parche de software para el [Id. de bug Cisco CSCea85204 \(clientes registrados solamente\)](#). Esta velocidad de reenvío es compartida por todos los flujos que sigan a través del Switch. Esta expedición aumenta carga de la CPU el debido al proceso del software. Como tal, la velocidad de reenvío alcanzada es dependiente en el Switch CPU; por ejemplo, cuántas directivas del Border Gateway Protocol (BGP), rutas del Enhanced Interior Gateway Routing Protocol (EIGRP) o del Open Shortest Path First (OSPF), y interfaces virtuales conmutadas (SVI) que el Switch tiene.

Nota: Los paquetes del IPv4 continúan siendo ruteados en hardware, aunque los paquetes IPX son ruteado por software.

Características admitidas

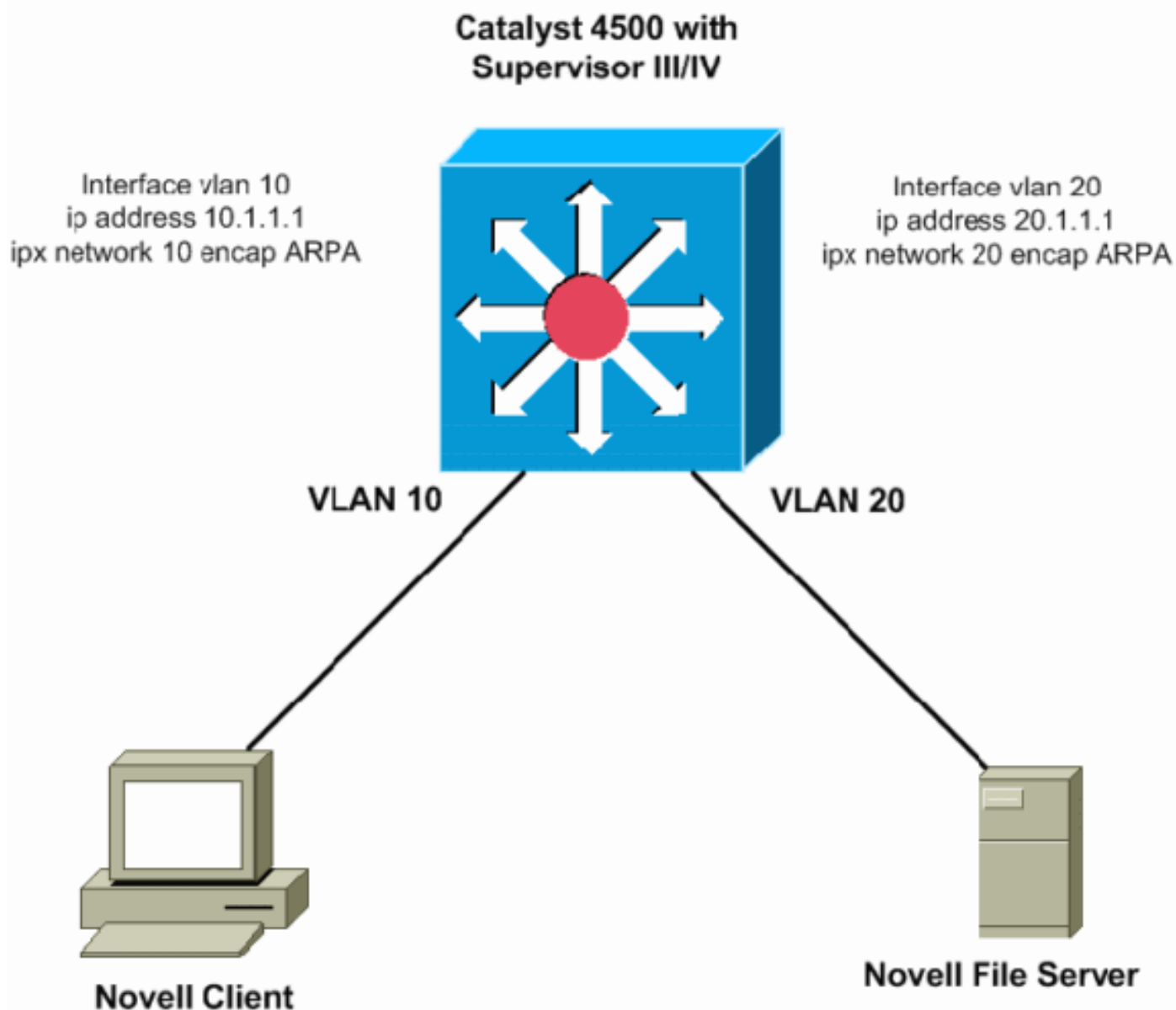
- La lista de control de acceso (ACL) MAC para el IPX se soporta en el Cisco IOS Software Release 12.1(12c)EW y Posterior, que se puede utilizar para controlar los paquetes IPX.
- Routing Information Protocol (RIP) IPX ([SAP] del protocolo service advertising)
- Enhanced Interior Gateway Routing Protocol (EIGRP) IPX
- compresión del encabezamiento

Nota: El EIGRP IPX es el protocolo del ruteo preferido entre el Routers para el mejor rendimiento, pues el EIGRP hace las actualizaciones graduales de SAP. El EIGRP IPX se puede habilitar en los segmentos del servidor-menos. Para la información sobre el EIGRP IPX, refiera [compresión del IPX-EIGRP](#).

Limitaciones

- El IPX Routing de los paquetes no es asistido por hardware. Se realiza a través del procesamiento de software.
- El estándar de Novell IPX (800-899), IPX ampliado (900-999), consigue el servidor más cercano (GNS), o las Listas de acceso de los filtros de SAP (1000-1099) no se soportan actualmente.
- Para la encaminamiento del software de IPX, éstos no se soportan: Protocolo de resolución de salto siguiente (NHRP) Protocolo de servicio de link Netware (NLSP) Tramas gigantes

Esta figura ilustra un escenario típico con Catalyst 4000 con supervisor III o IV el IPX que rutea. En este escenario, los clientes están en el VLAN10 y los servidores están en el VLAN20. El IPX se configura en el VLAN10 y 20 interfaces, tal y como se muestra en de este diagrama:



Ruteo de AppleTalk

Rutear el APPLE TALK se soporta en el Cisco IOS Software Release 12.1(12c)EW y Posterior. En la versión inicial, el funcionamiento está en el rango de 20 a 30 kpps; a partir del Cisco IOS Software Release 12.1(13)EW, se ha aumentado a 80 a 90 kpps. Se recomienda que usted utiliza el Cisco IOS Software Release 12.1(19)EW o Posterior debido a la Disponibilidad de una parche de software para el [Id. de bug Cisco CSCea85204](#) ([clientes registrados solamente](#)). Esta

velocidad de reenvío es compartida por todos los flujos que sigan a través del Switch. Esta expedición aumenta carga de la CPU el debido al proceso del software. Como tal, la velocidad de reenvío alcanzada es dependiente en el Switch CPU: por ejemplo, cuántas políticas de BGP, EIGRP o OSPF rutas, y SVI que el Switch tiene.

Nota: Los paquetes del IPv4 continúan siendo ruteados en hardware, aunque los paquetes del APPLETALK son ruteado por software.

Características admitidas

- El MAC ACL para el APPLETALK se soporta en el Cisco IOS Software Release 12.1(12c)EW y Posterior, que se puede utilizar para controlar los paquetes IPX.
- Ruteo del Protocolo de entrega de datagrama (DDP)
- Routing Table Maintenance Protocol (RTMP)
- Protocolo de asignación de nombres (NBP)
- Protocolo de archivado de AppleTalk (AFP)
- AppleTalk EIGRP

Nota: El Appletalk EIGRP es el protocolo del ruteo preferido entre el Routers para el mejor rendimiento, pues el EIGRP hace las actualizaciones graduales. Para más información sobre el Appletalk EIGRP, refiera a la sección del [IGRP mejorado del APPLETALK que configura de configurar el APPLETALK](#).

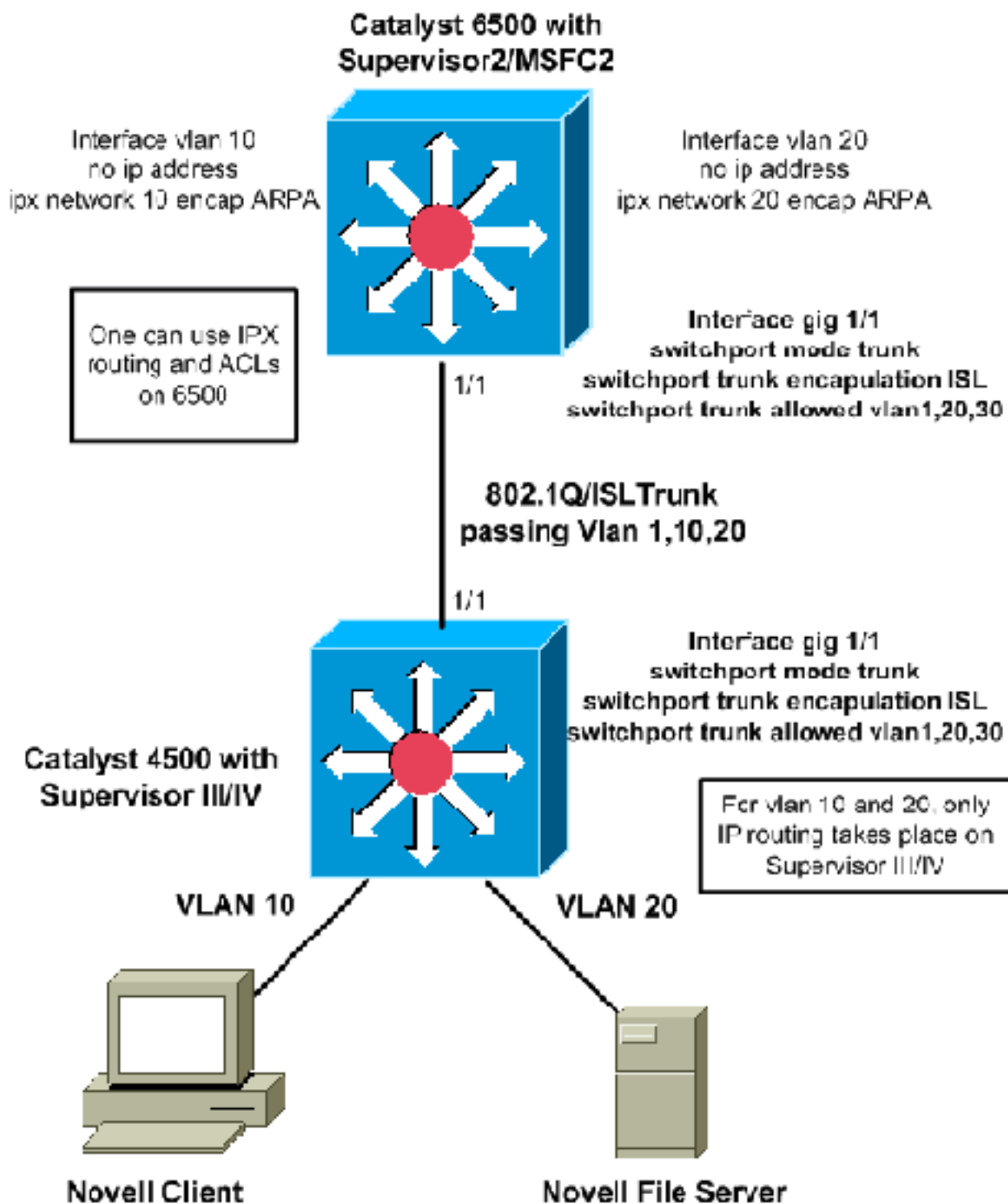
Limitaciones

- El AppleTalk Routing de paquetes no es asistido por hardware. Se realiza a través del procesamiento de software.
- El APPLETALK ACL no se soporta actualmente.
- Para la encaminamiento del software del APPLETALK, éstos no se soportan: Protocolo de ruteo basado en actualizaciones de AppleTalk (AURP) Protocolo de control AppleTalk para PPPTramas gigantes

Ruteo a través de un Router Externo

Si su red requiere un mejor funcionamiento de la encaminamiento de los protocolos heredados entonces mencionados previamente, usted puede querer utilizar a un router externo (dispositivo de la capa 3 [L3]). Tal dispositivo L3 podría ser un (MSFC) de la Multilayer Switch Feature Card del Catalyst 6000, el Catalyst 5000 RS, el Switch L3 (tal como un 2948G-L3), o cualquier router. Estos dispositivos realizan la encaminamiento del IPX con la asistencia de hardware, y el funcionamiento es mucho mayor que el Supervisor III/IV. El Supervisor III/IV puede rutear el IP en la trayectoria del Hardware Switching, pero el dispositivo externo rutea los protocolos heredados.

El diagrama siguiente ilustra un escenario en el cual el IPX se rutee en la base/el Catalyst 6500 de la distribución en el MSFC mientras que el IP se rutea entre el VLAN10 y el VLAN20 en el Catalyst 4500 con el Supervisor III/IV. El dos Switches es trunked, que permite los VLA N requeridos. La ventaja de este tipo de diseño es la capacidad de utilizar IPX estándar ACL y el incremento del rendimiento debido a la expedición asistida por hardware de estos paquetes entre los dos VLA N. Usted puede también utilizar los protocolos del IPX Routing en el Catalyst 6500 o en el router externo, para comunicar con los pares para el intercambio de la base de datos de ruteo:



Mejoras de rendimiento adicionales

Esta sección proporciona algunas mejoras adicionales del rendimiento potencial que se puedan llevar a cabo al IPX o a la transferencia del APPLE TALK en el router externo.

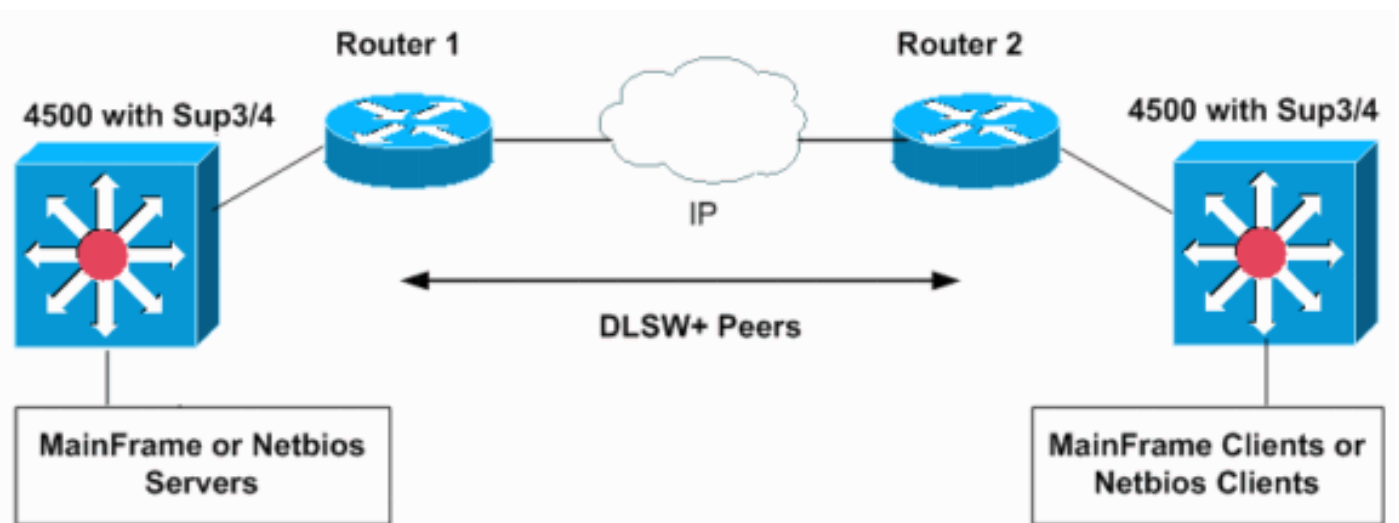
- El link entre el router externo y el switch de Catalyst se podía hacer en un link del canal del puerto, para conseguir el ancho de banda mayor entre ellos y para tener Redundancia para el link.
- El tráfico IP puede ser link filtrado de los para utilizar todo el ancho de banda para el tráfico no IP. Esto es una configuración de muestra para filtrar hacia fuera el tráfico IP con el Calidad de Servicio (QoS):

1. Publique los **qos del** comando global configuration de QoS, para habilitar QoS en el supervisor.
2. Defina el ACL para hacer juego todo el tráfico IP.`access-list 101 permit ip any any`
3. Defina el clase-mapa que hace juego el ACL definido en el paso 2.`class-map match-any ip-drops`
`match access-group 101`
4. Defina la directiva: defina un policer que caiga todo el tráfico para la clase definida en la policia del paso 3. todo el tráfico usando una granularidad mínima de 32 kbps. El supervisor caerá todo el tráfico IP con este regulador por encima de 32 kbps (los ping IP del Cisco IOS pueden no poder ir a través).`policy-map drop-ip`
`class ip-drops`
`police 32000 bps 1000 byte conform-action drop exceed-action drop`
5. Aplique la política de servicio el extranjero en la interfaz que conecta con el router externo.`interface GigabitEthernet 1/1`
`service-policy output drop-ip`

Para verificar la acción de regulación de tráfico, publique el comando **show policy-map interface interface-id**.

DLSw

DLSw no se soporta en el Supervisor III/IV. Para las redes con los protocolos SNA y IP, usted puede rutear el tráfico IP en el Catalyst 4000 Supervisor III/IV y interligar el tráfico SNA con la transferencia de DLSw en el Cisco IOS Software en un router externo:



Las configuraciones siguientes muestran cómo interligar el tráfico SNA en los VLA N 10 y 20 en dos Catalyst 6500 MSFC2 en dos dominios separados SNA. Los trunks del 802.1Q en el Supervisor III/IV se pueden utilizar para llevar (Bridge) el SNA o el tráfico de NETBIOS a un router Cisco o a los Catalyst 6500 Switch.

<pre>hostname MSFCRouter-1 interface loopback1 ip address 1.1.1.1 ! int vlan10 ip add 10.10.10.254 255.255.255.0 bridge-group 1</pre>	<pre>hostname MSFCRouter-2 interface loopback1 ip address 2.2.2.2 ! int vlan20 ip add 10.10.20.254 255.255.255.0 bridge-group 2</pre>
--	--

<pre>! bridge 1 protocol ieee dlsw local-peer peerid 1.1.1.1 dlsw remote-peer 0 tcp 2.2.2.2 dlsw bridge-group 1</pre>	<pre>! bridge 2 protocol ieee dlsw local-peer peerid 2.2.2.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 2</pre>
---	---

Esto muestra las configuraciones de red para los Catalyst 6500 Switch en diversos dominios. Si las VLAN 10 y 20 están en el mismo switch o MSFC, no se requiere DLSw. Los Grupos de Bridge simples de IEEE en un MSFC trabajarán.

[Paquetes de filtración del no IP con las correspondencias extendidas MAC ACL y del VLA N](#)

El Supervisor III/IV no soporta el IPX, el APPLE TALK, o el otro protocolo heredado ACL. Para filtrarlos, usted puede utilizar un ACL MAC-extendido combinado con una correspondencia del acceso de VLAN. Los mapas de VLAN pueden controlar el acceso de todo el tráfico en una VLAN. Puede aplicar mapas de VLAN en el switch a todos los paquetes que se enrutan hacia o desde una VLAN o que son conectados con puentes dentro de una VLAN. A diferencia del router ACLS, las correspondencias del VLA N no son definidas por la dirección (entrada o salida).

En este ejemplo de escenario, estos dos criterios son los objetivos de la configuración:

- Evitar todo el tráfico IPX desde el host 000.0c00.0111 al host 000.0c00.0211, pero permite todos los otros tráficos de protocolos IPX y sin IP a través de VLAN 20.
- Denegar todo el tráfico AppleTalk para VLAN 10.

Nota: Los paquetes del IP no se pueden filtrar con un MAC ACL.

Nota: Los ACL ampliados Nombrados MAC no se pueden aplicar a las interfaces L3.

1. Defina amplió MAC ACL para definir el tráfico interesante para las correspondencias del VLA N. Switch(config)# **mac access-list extended denyIPXACL** Switch(config-ext-macl)# **permit host 000.0c00.0111 host 000.0c00.0211 protocol-family ?** appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns Switch(config-ext-macl)# **\$00.0c00.0111 host 000.0c00.0211 protocol-family ipx** Switch(config-ext-macl)# **exit** Switch(config)# **mac access-list extended denyatalk** Switch(config-ext-macl)# **permit any any protocol-family appletalk** Switch(config)#
2. Publique el comando **show access-list access-list-name** de verificar configurado MAC ACL ampliada. Los ACL en el ejemplo anterior son denyIPXACL y denyatalk. Switch# **show access-lists denyIPXACL** Extended MAC access list denyIPXACL permit host 0000.0c00.0111 host 0000.0c00.0211 protocol-family ipx Switch# **show access-lists denyatalk** Extended MAC access list denyatalk permit any any protocol-family appletalk
3. Defina la acción con las correspondencias del acceso de VLAN. Switch(config)# **vlan access-map denyIPX** Switch(config-access-map)# **match mac address denyIPXACL** Switch(config-access-map)# **action drop** Switch(config-access-map)# **exit** Switch(config)# **vlan access-map denyapple** Switch(config-access-map)# **match mac address denyatalk** Switch(config-access-map)# **action drop** Switch(config-access-map)# **exit**
4. Publique el comando **show vlan access-map name** de verificar definido las correspondencias del acceso de VLAN. Switch# **show vlan access-map denyIPX** Vlan access-map "denyIPX" 10 Match clauses: mac address: denyIPXACL Action: drop Switch# **show vlan access-map denyapple** Vlan access-map "denyapple" 10 Match clauses: mac address: denyatalk Action: drop
5. Publique el comando **vlan filter name vlan-list vlan-list** de asociar la correspondencia del VLA N a los VLA N. En este ejemplo, usted quiere filtrar el IPX entre los host específicos en el

```
VLAN20 y negar el APPLE TALK en el VLAN10.Switch(config)# vlan filter denyIPX vlan-  
list 20 Switch(config)# vlan filter denyapple vlan-list 10
```

6. Publique el **comando show vlan filter vlan vlan-id** de verificar que los filtros del VLA N

```
existen.Switch# show vlan filter vlan 20 Vlan 20 has filter denyIPX. Switch# show vlan  
filter vlan 10 Vlan 10 has filter denyapple.
```

Otras funciones no compatibles

El Supervisor III/IV no soporta estas características:

- Bridging o Inter-VLAN Bridging del retraso para interligar los protocolos no enrutables
- ruteo DECnet

Refiera a la [sección anterior](#), para ver un ejemplo de cómo utilizar a un router externo para alcanzar estas funciones.

Alto nivel de CPU después de habilitar el ruteo AppleTalk o IPX

Después de que usted habilite la encaminamiento IPX o del APPLE TALK, el USO de la CPU aumentará basado en la cantidad tráfico IPX o AppleTalk de eso se está ruteando en el software a través del Switch. Si usted publica el **comando show processor cpu**, la salida puede mostrar que el proceso de LoPri del mgmt Cat4k está utilizando el CPU. Dicho resultado indica que los paquetes son conmutados por proceso.

```
Switch# show processes cpu CPU utilization for five seconds: 99%/0%; one minute: 86%; five  
minutes: 54% PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 1 8 607 13 0.00% 0.00%  
0.00% 0 Load Meter 2 496 4549 109 0.00% 0.01% 0.00% 0 Spanning Tree 3 0 1 0 0.00% 0.00% 0.00% 0  
Deferred Events 4 4756 480 9908 0.00% 0.08% 0.11% 0 Check heaps 5 0 1 0 0.00% 0.00% 0.00% 0  
Chunk Manager 6 0 1 0 0.00% 0.00% 0.00% 0 Pool Manager 7 0 2 0 0.00% 0.00% 0.00% 0 Timers 8 4 2  
2000 0.00% 0.00% 0.00% 0 Serial Backgroun 9 4 64 62 0.00% 0.00% 0.00% 0 ARP Input 10 24 3 8000  
0.00% 0.00% 0.00% 0 Entity MIB API 11 0 1 0 0.00% 0.00% 0.00% 0 SERIAL A'detect 12 0 1 0 0.00%  
0.00% 0.00% 0 Critical Bkgnd 13 25436 864 29439 0.00% 0.00% 0.00% 0 Net Background 14 0 58 0  
0.00% 0.00% 0.00% 0 Logger 15 52 2607 19 0.00% 0.00% 0.00% 0 TTY Background 16 440 2666 165  
0.00% 0.00% 0.00% 0 Per-Second Jobs 17 112328 410885 273 1.66% 2.37% 2.74% 0 Cat4k Mgmt HiPri 18  
1197172 21536 55589 98.56% 84.14% 49.15% 0 Cat4k Mgmt LoPri 19 0 1 0 0.00% 0.00% 0.00% 0  
Routekernel Proc
```

Nota: Si usted no hace la encaminamiento IPX o del APPLE TALK habilitar, sino todavía ve el mgmt LoPri Cat4k usando CPU elevada, después usted puede tener que resolver problemas que paquetes se envían al CPU para procesar. Entre en contacto el [Soporte técnico de Cisco](#), si usted necesita la asistencia adicional.

Información Relacionada

- [Configurar la seguridad de la red con los ACL](#)
- [Páginas de soporte del Catalyst 4500](#)
- [Páginas de Soporte de Productos de LAN](#)
- [Página de Soporte de LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)