Compatibilidad con protocolos heredados con Catalyst 4000 Supervisor III/IV

Contenido

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. Este supervisor está diseñado para los paquetes de la versión 4 (IPv4) del switch de hardware.

Prerequisites

Requirements

Los lectores de este documento deben tener conocimientos sobre cómo configurar IPX, AppleTalk y DLSw. Para obtener información sobre estos protocolos, consulte estas páginas de soporte:

- Página de soporte de la tecnología IPX
- Página de soporte de la tecnología 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 Supervisor IV
- Versión 12.1(13)EW del software del IOS® de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Ruteo de IPX

El IPX de ruteo es compatible con Cisco IOS Software Release 12.1(12c)EW y posteriores. En la versión inicial, el rendimiento está en el rango de 20 a 30 kpps; a partir de la versión 12.1(13)EW del software del IOS de Cisco, se ha aumentado a 80 a 90 kpps. Se recomienda que utilice Cisco IOS Software Release 12.1(19)EW o posterior debido a la disponibilidad de una corrección de software para Cisco bug ID CSCea85204 (sólo clientes registrados) . Todos los flujos que siguen a través del switch comparten esta velocidad de reenvío. Este reenvío aumenta la carga de la CPU debido al procesamiento del software. Como tal, la velocidad de reenvío alcanzada depende de la CPU del switch; por ejemplo, cuántas políticas de protocolo de gateway fronterizo (BGP), rutas de protocolo de routing de gateway interior mejorado (EIGRP) o de ruta de acceso más corta primero (OSPF) y interfaces virtuales conmutadas (SVI) que tiene el switch.

Nota: Los paquetes IPv4 siguen enrutándose en el hardware, aunque los paquetes IPX estén enrutados por software.

Características admitidas

- La lista de control de acceso (ACL) MAC para IPX se admite en la versión 12.1(12c)EW y posteriores del software del IOS de Cisco, que se puede utilizar para controlar los paquetes IPX.
- Protocolo de información de routing (RIP) IPX (protocolo de publicidad de servicios [SAP])
- Protocolo de routing de gateway interior mejorado IPX (EIGRP)
- Compresión de encabezados

Nota: IPX EIGRP es el protocolo de ruteo preferido entre routers para lograr un mejor rendimiento, ya que EIGRP realiza actualizaciones incrementales de SAP. IPX EIGRP se puede habilitar en segmentos sin servidor. Para obtener información sobre IPX EIGRP, consulte Introducción a IPX-EIGRP.

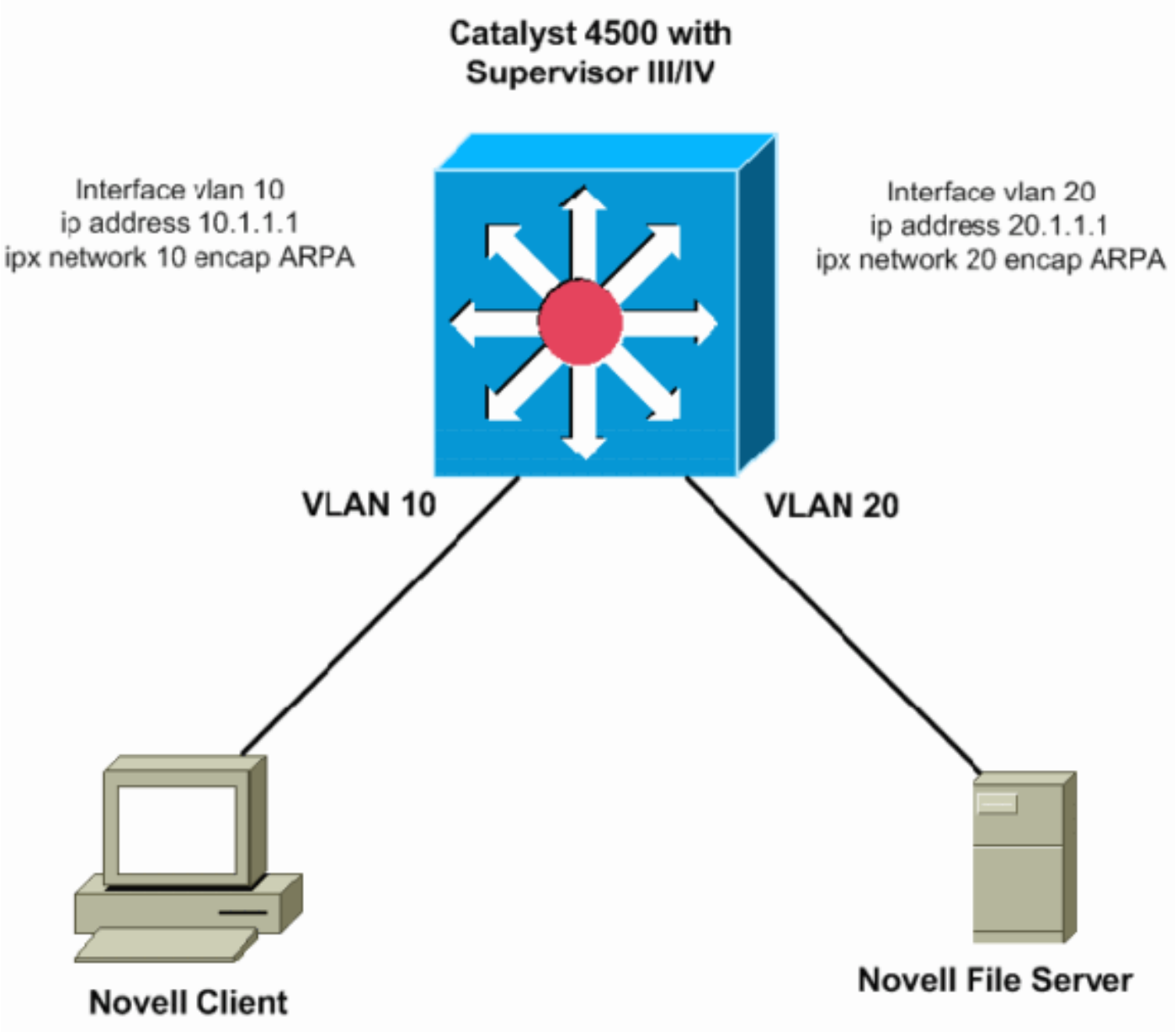
Limitaciones

- El ruteo IPX de paquetes no está asistido por hardware. Se realiza a través del procesamiento de software.
- Actualmente no se admiten las listas de acceso estándar Novell IPX (800-899), IPX ampliado

(900-999), Get Nearest Server (GNS) o filtros SAP (1000-1099).

- Para el ruteo de software IPX, estos no son compatibles:Protocolo de resolución de salto siguiente (NHRP)Protocolo de servicio de link Netware (NLSP)Tramas gigantes

Esta figura ilustra un escenario típico con Catalyst 4000/4500 con Supervisor III/IV Routing IPX. En este escenario, los clientes están en la VLAN 10 y los servidores están en la VLAN 20. IPX se configura en las interfaces VLAN 10 y 20, como se muestra en este diagrama:



Ruteo de AppleTalk

El ruteo AppleTalk se soporta en Cisco IOS Software Release 12.1(12c)EW y posterior. En la versión inicial, el rendimiento está en el rango de 20 a 30 kpps; a partir de la versión 12.1(13)EW del software del IOS de Cisco, se ha aumentado a 80 a 90 kpps. Se recomienda que utilice Cisco IOS Software Release 12.1(19)EW o posterior debido a la disponibilidad de una corrección de software para Cisco bug ID CSCea85204 (sólo clientes registrados) . Todos los flujos que siguen a través del switch comparten esta velocidad de reenvío. Este reenvío aumenta la carga de la CPU debido al procesamiento del software. Como tal, la velocidad de reenvío alcanzada depende de la CPU del switch: por ejemplo, cuántas políticas BGP, rutas EIGRP o OSPF y SVI tienen el switch.

Nota: Los paquetes IPv4 siguen enrutándose en hardware, aunque los paquetes AppleTalk estén enrutados por software.

Características admitidas

- MAC ACL para AppleTalk se soporta en 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)
- Protocolo de mantenimiento de tabla de routing (RTMP)
- Protocolo de asignación de nombres (NBP)
- Protocolo de archivado de AppleTalk (AFP)
- AppleTalk EIGRP

Nota: AppleTalk EIGRP es el protocolo de ruteo preferido entre routers para un mejor rendimiento, ya que EIGRP realiza actualizaciones incrementales. Para obtener más información sobre AppleTalk EIGRP, refiérase a la sección Configuración de AppleTalk Enhanced IGRP de Configuración de AppleTalk.

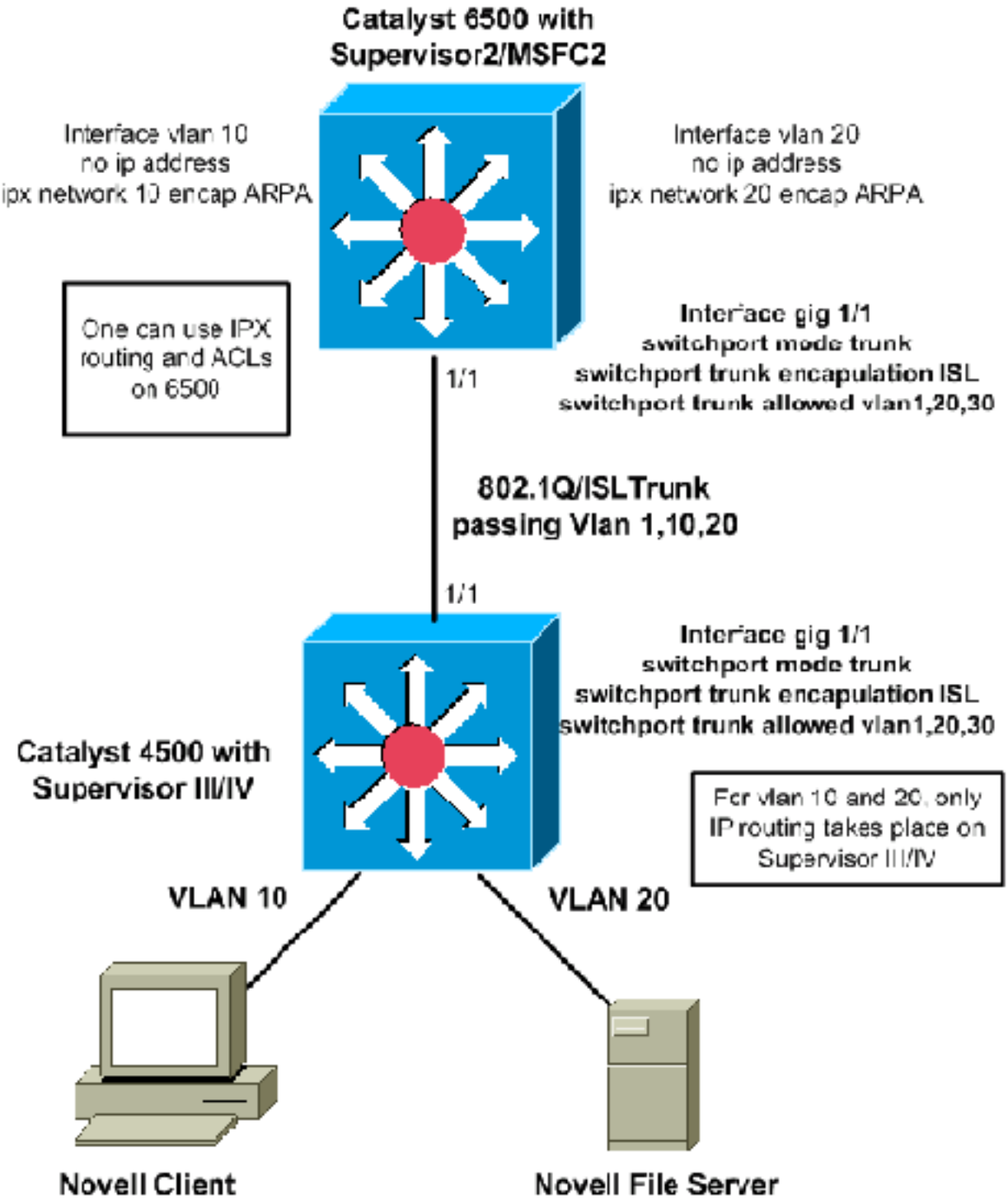
Limitaciones

- El ruteo de paquetes de AppleTalk no está asistido por hardware. Se realiza a través del procesamiento de software.
- Las ACL de AppleTalk no se soportan actualmente.
- Para el ruteo de software AppleTalk, estos no son compatibles: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 rendimiento de routing de los protocolos heredados mencionados anteriormente, es posible que desee utilizar un router externo (dispositivo de capa 3 [L3]). Este dispositivo L3 podría ser una tarjeta de función de switch multicapa (MSFC) de Catalyst 6000, Catalyst 5000 RSM, switch L3 (como 2948G-L3) o cualquier router. Estos dispositivos realizan el ruteo de IPX con asistencia de hardware y el rendimiento es mucho mayor que el Supervisor III/IV. El Supervisor III/IV puede rutear IP en la trayectoria de conmutación de hardware, pero el dispositivo externo rutea los protocolos heredados.

El siguiente diagrama ilustra un escenario en el que IPX se rutea en el Catalyst 6500 de núcleo/distribución en la MSFC mientras que la IP se rutea entre la VLAN 10 y la VLAN 20 en el Catalyst 4500 con el Supervisor III/IV. Los dos switches están troncales, lo que permite las VLAN necesarias. La ventaja de este tipo de diseño es la capacidad de utilizar ACL IPX estándar y el aumento del rendimiento debido al reenvío asistido por hardware de estos paquetes entre las dos VLAN. También puede utilizar los protocolos de ruteo IPX en el Catalyst 6500 o en el router externo para comunicarse con los pares para el intercambio de bases de datos de ruteo:



Mejoras de rendimiento adicionales

Esta sección proporciona algunas mejoras potenciales de rendimiento adicionales que se pueden realizar en IPX o en la conmutación AppleTalk en el router externo.

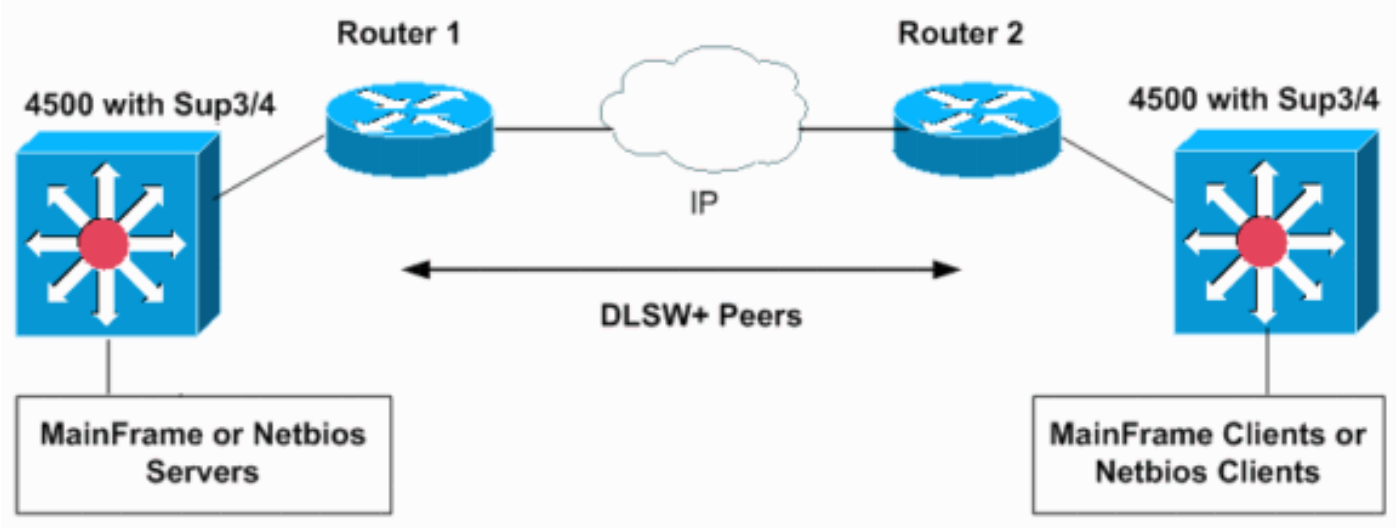
- El link entre el router externo y el switch Catalyst se puede convertir en un link de canal de puerto, para obtener un mayor ancho de banda entre ellos y para tener redundancia para el link.
- El tráfico IP se puede filtrar fuera del link para que todo el ancho de banda se utilice para el tráfico que no es de IP. Esta es una configuración de ejemplo para filtrar el tráfico IP a través de la calidad de servicio (QoS):

1. Ejecute el comando de configuración global de QoS **qos**, para habilitar QoS en el Supervisor.
2. Defina la ACL para que coincida con todo el tráfico IP.
   ```
   access-list 101 permit ip any any
   ```
3. Defina el class-map que coincide con la ACL definida en el Paso 2.
   ```
   class-map match-any ip-drops
     match access-group 101
   ```
4. Defina la política: defina un regulador que descartará todo el tráfico para la clase definida en el Paso 3. Controle todo el tráfico usando una granularidad mínima de 32 kbps. El Supervisor descartará todo el tráfico IP con este regulador de tráfico más allá de los 32 kbps (es posible que los pings IP de Cisco IOS no puedan atravesar).
   ```
   policy-map drop-ip
     class ip-drops
       police 32000 bps 1000 byte conform-action drop exceed-action drop
   ```
5. Aplique la política de servicio saliente en la interfaz que se conecta al router externo.
   ```
   interface GigabitEthernet 1/1
       service-policy output drop-ip
   ```

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

DLSw

El Supervisor III/IV no admite DLSw. Para redes con protocolos SNA e IP, puede rutear el tráfico IP en Catalyst 4000 Supervisor III/IV y puentear el tráfico SNA con conmutación DLSw en el software Cisco IOS en un router externo:



Las siguientes configuraciones muestran cómo conectar el tráfico SNA en las VLAN 10 y 20 en dos MSFC2 Catalyst 6500 en dos dominios SNA separados. Los troncales 802.1Q en el Supervisor III/IV se pueden utilizar para transportar tráfico SNA o NetBIOS (puente) a un router Cisco o a los switches Catalyst 6500.

hostname MSFCRouter-1 interface loopback1 ip address 1.1.1.1 ! int vlan10 ip add 10.10.10.254 255.255.255.0	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 1 ! 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	bridge-group 2 ! 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

Esto muestra las configuraciones de red para los switches Catalyst 6500 en diferentes dominios. Si las VLAN 10 y 20 están en el mismo switch o MSFC, no se requiere DLSw. Los grupos de puentes IEEE simples en un MSFC funcionarán.

Filtrado de Paquetes no IP con ACL MAC Extendidas y Mapas VLAN

El Supervisor III/IV no soporta IPX, AppleTalk u otras ACL de protocolo heredadas. Para filtrarlos, puede utilizar una ACL extendida por MAC combinada con un mapa de acceso 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 de las ACL del router, los mapas de VLAN no se definen por dirección (entrada o salida).

En este escenario de ejemplo, estos dos criterios son los objetivos de 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 IP no se pueden filtrar a través de una ACL MAC.

Nota: Las ACL ampliadas MAC con nombre no se pueden aplicar a las interfaces L3.

1. Defina las ACL MAC extendidas para definir el tráfico interesante para los mapas de VLAN.

```
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. Ejecute el comando **show access-list** *access-list-name* para verificar la ACL MAC extendida

configurada. Las ACL del 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 los mapas de 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. Ejecute el comando **show vlan access-map** *name* para verificar los mapas de acceso de VLAN definidos.

```
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. Ejecute el comando **vlan filter** *name* **vlan-list** *vlan-list* para asignar el mapa de VLAN a las VLAN. En este ejemplo, desea filtrar IPX entre hosts específicos en VLAN 20 y denegar AppleTalk en VLAN 10.

```
Switch(config)# vlan filter denyIPX vlan-list 20

Switch(config)# vlan filter denyapple vlan-list 10
```

6. Ejecute el comando **show vlan filter vlan** *vlan-id* para verificar que los filtros VLAN estén en su lugar.

```
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 admite estas características:

- Puente de reserva o conexión en puente entre VLAN para puentes de protocolos no enrutables
- ruteo DECnet

Consulte la sección anterior para ver un ejemplo de cómo utilizar un router externo para lograr esta funcionalidad.

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

Después de habilitar el ruteo IPX o AppleTalk, el uso de la CPU aumentará en función de la cantidad de tráfico IPX o AppleTalk que se rutea en software a través del switch. Si ejecuta el comando **show processor cpu**, el resultado puede mostrar que el proceso `Cat4k Mgmt LoPri` está usando la 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 no tiene habilitado el ruteo IPX o AppleTalk, pero sigue viendo `Cat4k Mgmt LoPri` usando CPU alta, es posible que tenga que resolver los problemas de los paquetes enviados a la CPU para su procesamiento. Póngase en contacto con el Soporte Técnico de Cisco, si necesita más ayuda.

Información Relacionada

- Configuración de la Seguridad de la Red con ACL
- Páginas de soporte de Catalyst 4500
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems