

Protocolos legado de apoio com Catalyst 4000 Supervisor III/IV

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Routing IPX](#)

[Recursos suportados](#)

[Limitações](#)

[Routing AppleTalk](#)

[Recursos suportados](#)

[Limitações](#)

[Roteando por meio de um roteador externo](#)

[Melhorias de desempenho adicionais](#)

[DLSW](#)

[Pacotes não-IP de filtração com os mapas prolongados MAC ACL e VLAN](#)

[Outros recursos não suportados](#)

[CPU de Alto Desempenho após Habilitação do IPX Routing ou AppleTalk](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como os protocolos legados, como IPX, AppleTalk e Data-Link Switching (DLSw), têm melhor suporte em um Catalyst 4000/4500 Switch equipado com o mais novo Supervisor III/IV. Este supervisor é projetado aos pacotes da versão IP 4 do switch de hardware (IPv4).

[Pré-requisitos](#)

[Requisitos](#)

Os leitores deste documento devem ter o conhecimento de como configurar o IPX, o APPLETALK, e o DLSw. Para obter informações sobre destes protocolos, refira estas páginas de suporte:

- [Página da Suporte da Tecnologia IPX](#)
- [Página de suporte de tecnologia do APPLETALK](#)

- [Página de suporte à tecnologia DLSw](#)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Routing IPX

Distribuir o IPX é apoiada no Cisco IOS Software Release 12.1(12c)EW e Mais Recente. Na versão inicial, o desempenho está na escala de 20 a 30 kpps; até à data do Cisco IOS Software Release 12.1(13)EW, foi aumentado a 80 a 90 kpps. Recomenda-se que você use o Cisco IOS Software Release 12.1(19)EW ou Mais Recente devido à Disponibilidade de um reparo de software para a [identificação de bug Cisco CSCea85204 \(clientes registrados somente\)](#). Esta taxa de encaminhamento é compartilhada por todos os fluxos que seguem através do interruptor. Esta transmissão aumenta a carga de CPU devido ao processamento do software. Como tal, a taxa de encaminhamento conseguida é dependente do interruptor CPU; por exemplo, quantas políticas, Enhanced Interior Gateway Routing Protocol (EIGRP) ou Open Shortest Path First (OSPF) do Border Gateway Protocol (BGP) distribui, e interfaces virtuais comutadas (SVI) que o interruptor tem.

Nota: Os pacotes IPv4 continuam a ser distribuídos no hardware, mesmo que os pacotes IPX sejam roteado por software.

Recursos suportados

- O Access Control List MAC (ACL) para o IPX é apoiado no Cisco IOS Software Release 12.1(12c)EW e Mais Recente, que pode ser usado para controlar os pacotes IPX.
- Routing Information Protocol (RIP) IPX ([SAP] do protocolo service advertising)
- Enhanced Interior Gateway Routing Protocol (EIGRP) IPX
- compressão de cabeçalhos

Nota: O IPX EIGRP é o protocolo do roteamento preferido entre o Roteadores para o melhor desempenho, porque o EIGRP faz atualizações de SAP de acréscimo. O IPX EIGRP pode ser permitido em segmentos do server-menos. Para obter informações sobre de IPX EIGRP, refira a [compreensão do IPX-EIGRP](#).

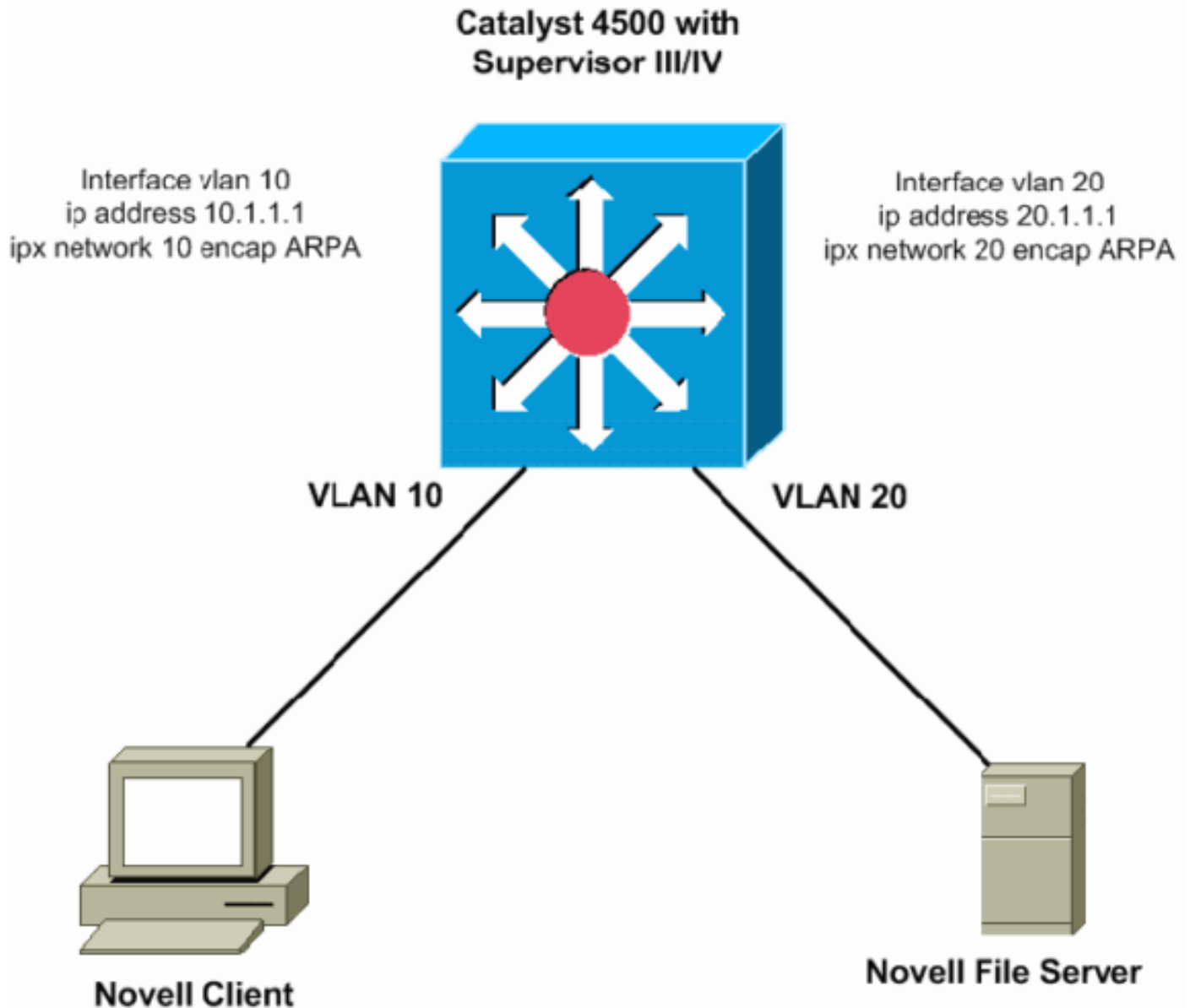
Limitações

- O roteamento IPX dos pacotes hardware-não é ajudado. Ele é realizado pelo processamento

de software.

- O padrão Novell IPX (800-899), IPX estendido (900-999), obtém o server o mais próximo (GNS), ou as Listas de acesso dos filtros de SAP (1000-1099) não são apoiadas atualmente.
- Para o roteamento do software IPX, estes não são apoiados: Protocolo de Resolução do Próximo Salto (NHRP) Netware Link Service Protocol (NLSP) jumbo frames

Esta figura ilustra um cenário típico com o Catalyst 4000/4500 com supervisor III/IV que distribui o IPX. Nesta encenação, os clientes estão no VLAN10 e nos server estão no VLAN20. O IPX é configurado no VLAN10 e nas 20 relações, segundo as indicações deste diagrama:



[Routing AppleTalk](#)

Distribuir o APPLE TALK é apoiada no Cisco IOS Software Release 12.1(12c)EW e Mais Recente. Na versão inicial, o desempenho está na escala de 20 a 30 kpps; até à data do Cisco IOS Software Release 12.1(13)EW, foi aumentado a 80 a 90 kpps. Recomenda-se que você usa o Cisco IOS Software Release 12.1(19)EW ou Mais Recente devido à Disponibilidade de um reparo de software para a [identificação de bug Cisco CSCea85204 \(clientes registrados somente\)](#). Esta taxa de encaminhamento é compartilhada por todos os fluxos que seguem através do interruptor. Esta transmissão aumenta a carga de CPU devido ao processamento do software. Como tal, a

taxa de encaminhamento conseguida é dependente do interruptor CPU: por exemplo, quantas políticas do BGP, EIGRP ou rotas de OSPF, e SVI que o interruptor tem.

Nota: Os pacotes IPv4 continuam a ser distribuídos no hardware, mesmo que os pacotes appletalk sejam roteado por software.

Recursos suportados

- O MAC ACL para o APPLETALK é apoiado no Cisco IOS Software Release 12.1(12c)EW e Mais Recente, que pode ser usado para controlar os pacotes IPX.
- Roteamento do DDP
- Protocolo de manutenção de tabela de roteamento (RTMP)
- Protocolo de associação de nomes (NBP)
- Protocolo de Eco AppleTalk (AEP)
- AppleTalk EIGRP

Nota: O Appletalk EIGRP é o protocolo de roteamento preferido entre os roteadores para o melhor desempenho, porque o EIGRP faz atualizações de acréscimo. Para obter mais informações sobre o Appletalk EIGRP, refira a seção [configurando do IGRP aprimorado do APPLETALK de configurar o APPLETALK](#).

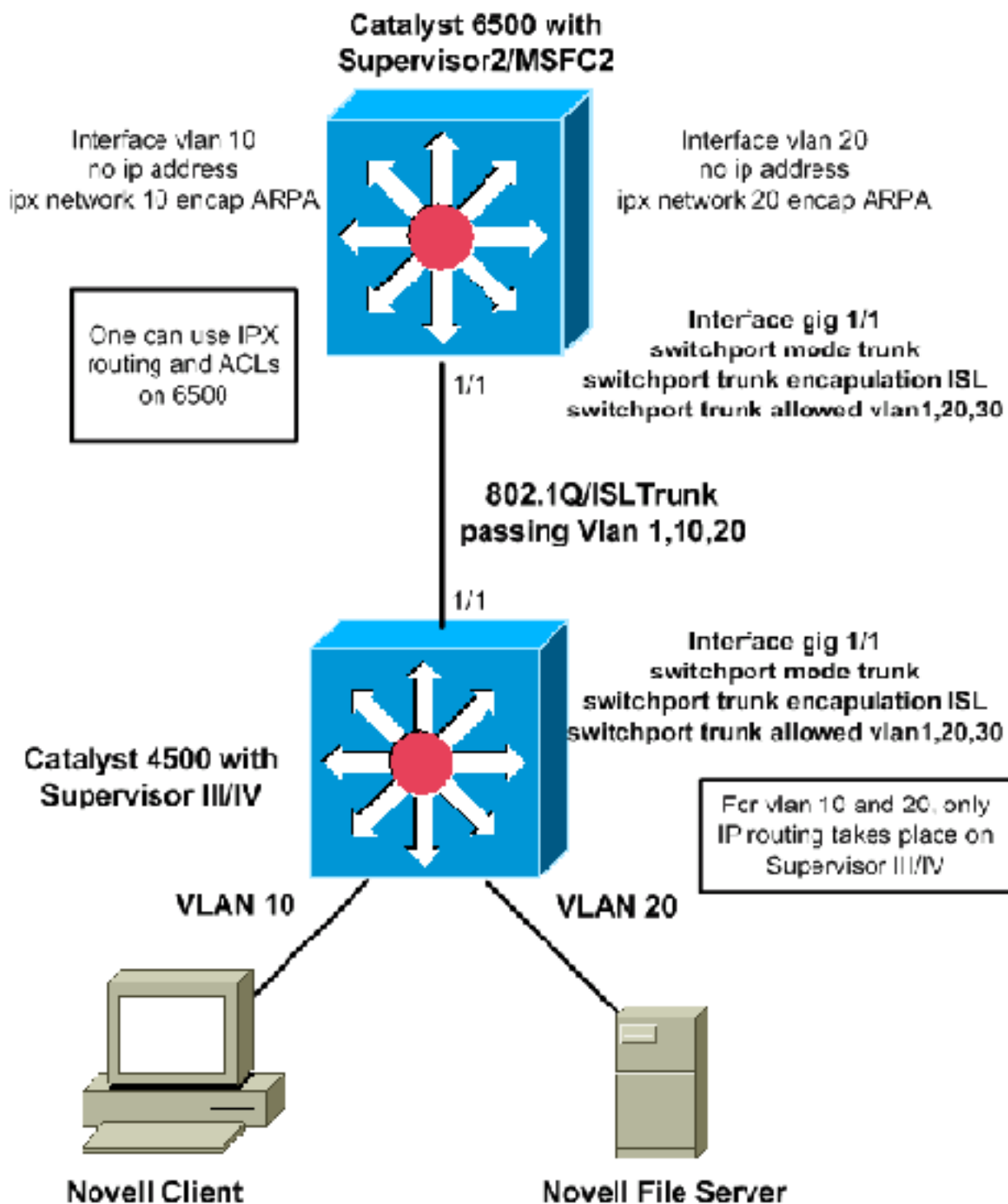
Limitações

- O roteamento APPLETALK de pacotes hardware-não é ajudado. Ele é realizado pelo processamento de software.
- O APPLETALK ACL não é apoiado atualmente.
- Para o roteamento do software do APPLETALK, estes não são apoiados: Protocolo AURP (AppleTalk Update-Based Routing Protocol) Protocolo de controle AppleTalk para PPPjumbo frames

Roteando por meio de um roteador externo

Se sua rede exige o melhor desempenho do roteamento dos protocolos legado então mencionados previamente, você pode querer usar um roteador externo (dispositivo da camada 3 [L3]). Tal dispositivo L3 poderia ser um Multilayer Switch Feature Card (MSFC) do catalizador 6000, o catalizador 5000 RS, o interruptor L3 (tal como um 2948G-L3), ou o todo o roteador. Estes dispositivos executam o roteamento do IPX com a assistência de hardware, e o desempenho é muito maior do que o Supervisor III/IV. O Supervisor III/IV pode distribuir o IP no trajeto de switching de hardware, mas o dispositivo externo distribui os protocolos legado.

O diagrama seguinte ilustra uma encenação em que o IPX está distribuído no núcleo/Catalyst 6500 da distribuição no MSFC quando o IP for distribuído entre o VLAN10 e o VLAN20 no Catalyst 4500 com Supervisor III/IV. Os dois Switches são o em tronco, que permite os VLAN exigidos. O benefício deste tipo de projeto é a capacidade para usar o padrão IPX ACL e o aumento de desempenho devido à transmissão hardware-ajudada destes pacotes entre os dois VLAN. Você pode igualmente usar protocolos do roteamento IPX no Catalyst 6500 ou no roteador externo, para comunicar-se com os pares para a troca da base de dados de roteamento:



Melhorias de desempenho adicionais

Isto secciona fornece algumas melhorias adicionais do desempenho potencial que podem ser feitas ao IPX ou ao interruptor do APPLE TALK no roteador externo.

- O link entre o roteador externo e o Catalyst Switch podia ser feito em um link do canal de porta, para obter a largura de banda mais alta entre eles e para ter a Redundância para o link.
- O tráfego IP pode ser filtrado fora do link de modo que toda a largura de banda seja usada para o tráfego não-IP. Esta é uma configuração de exemplo para filtrar para fora o tráfego IP com o Qualidade de Serviço (QoS):

1. Emita os **qos do** comando global configuration de QoS, para permitir QoS no supervisor.
2. Defina o ACL para combinar todo o tráfego IP.

```
access-list 101 permit ip any any
```
3. Defina o mapa de classe que combina o ACL definido em etapa 2.

```
class-map match-any ip-drops
  match access-group 101
```
4. Defina a política: defina um vigilante que deixe cair todo o tráfego para a classe definida na polícia de etapa 3. todo o tráfego usando uma granularidade mínima de 32 kbps. O supervisor deixará cair todo o tráfego IP com esta vigilância além 32 kbps (os ping IP do Cisco IOS não podem ir completamente).

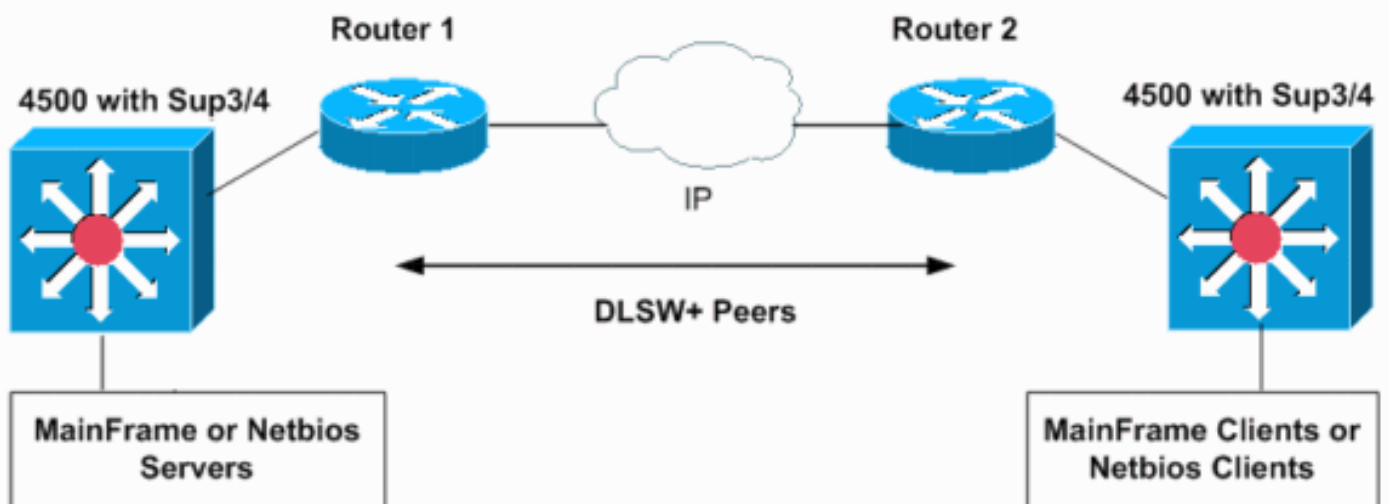
```
policy-map drop-ip
  class ip-drops
    police 32000 bps 1000 byte conform-action drop exceed-action drop
```
5. Aplique a política de serviços de partida na relação que conecta ao roteador externo.

```
interface GigabitEthernet 1/1
  service-policy output drop-ip
```

Para verificar a ação de vigilância, emita o comando **show policy-map interface interface-id**.

DLSW

DLSw não é apoiado no Supervisor III/IV. Para redes com SNA e protocolos IP, você pode distribuir o tráfego IP no Catalyst 4000 Supervisor III/IV e construir uma ponte sobre o tráfego SNA com interruptor de DLSw no Cisco IOS Software em um roteador externo:



As configurações seguintes mostram como construir uma ponte sobre o tráfego SNA em VLAN 10 e 20 em dois Catalyst 6500 MSFC2 em dois domínios separados SNA. Os troncos 802.1Q no Supervisor III/IV podem ser usados para levar (ponte) o SNA ou o tráfego de netbios a um roteador Cisco ou aos 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>
---	---

Isto mostra configurações de rede para Catalyst 6500 Switch em domínios diferentes. Se os VLAN 10 e 20 estão no mesmo interruptor ou MSFC, DLSw não está exigido. Os grupos de bridge simples da IEEE em um MSFC trabalharão.

Pacotes não-IP de filtração com os mapas prolongados MAC ACL e VLAN

O Supervisor III/IV não apoia o IPX, o APPLETALK, ou o outro protocolo legado ACL. Para filtrá-los, você pode usar um ACL MAC-prolongado combinado com um mapa do acesso de vlan. Os mapas de VLAN podem controlar o acesso de todo o tráfego em uma VLAN. Você pode aplicar mapas VLAN no interruptor a todos os pacotes em que são distribuídos ou fora de um VLAN ou construídos uma ponte sobre dentro de um VLAN. Ao contrário dos ACLs de roteador, os mapas VLAN não são definidos pelo sentido (entrada ou saída).

Neste exemplo de cenário, estes dois critérios são os objetivos de configuração:

- Impede todo o tráfego de IPX do host 000.0c00.0111 ao host 000.0c00.0211, mas permite todos os outros tráfegos de IPX e de protocolos sem IP através do VLAN 20.
- Negar todo o tráfego AppleTalk para VLAN 10.

Nota: Os pacotes IP não podem ser filtrados com um MAC ACL.

Nota: Os ACL estendido Nomeados MAC não podem ser aplicados às relações L3.

1. Defina estendeu MAC ACL para definir o tráfego interessante para os mapas 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. Emita o comando **show access-list access-list-name** verificar o ACL MAC estendido

configurado. Os ACL no exemplo anterior são denyIPXACL e 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 a ação com os mapas do acesso 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. Emita o comando show vlan access-map name verificar definido os mapas do acesso 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. Emita o comando vlan filter name vlan-list vlan-list traçar o mapa VLAN aos VLAN. Neste exemplo, você quer filtrar o IPX entre anfitriões específicos no VLAN20 e negar o APPLETALK no VLAN10.

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

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

6. Emita o comando show vlan filter vlan-id verificar que os filtros VLAN são no lugar.

```
Switch# show vlan filter vlan 20
```

```
Vlan 20 has filter denyIPX.
```

```
Switch# show vlan filter vlan 10
```

```
Vlan 10 has filter denyapple.
```


Outros recursos não suportados

O Supervisor III/IV não apoia estas características:

- Construção de uma ponte sobre ou Inter-VLAN Bridging da reserva para construir uma ponte sobre protocolos não roteável
- DECnet Routing

Refira a [seção anterior](#), para ver um exemplo de como usar um roteador externo para conseguir esta funcionalidade.

CPU de Alto Desempenho após Habilitação do IPX Routing ou AppleTalk

Depois que você permite o roteamento IPX ou de APPLETALK, o USO de CPU aumentará baseado na quantidade de tráfego de IPX ou AppleTalk que está sendo distribuído no software através do interruptor. Se você emite o comando `show processor cpu`, a saída pode mostrar que o processo `Cat4k Mgmt LoPri` está usando o CPU. Isto indica que os pacotes estão sendo comutados por processo.

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 Background
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: Se você não tem o roteamento IPX ou de APPLETALK permitido, mas ainda vê `Cat4k Mgmt LoPri` usando a alta utilização da CPU, a seguir você pode ter que pesquisar defeitos que pacotes são enviados ao CPU para processar. Contacte o [Suporte técnico de Cisco](#), se você precisa a assistência adicional.

Informações Relacionadas

- [Configurando a segurança de rede com ACL](#)
- [Páginas de suporte do Catalyst 4500](#)
- [Páginas de Suporte de Produtos de LAN](#)

- [Página de suporte da switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)