

Prise en charge des protocoles existants avec Catalyst 4000 Supervisor III/IV

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Routage IPX](#)

[Fonctionnalités prises en charge](#)

[Limites](#)

[Routage AppleTalk](#)

[Fonctionnalités prises en charge](#)

[Limites](#)

[Routage via un routeur externe](#)

[Améliorations supplémentaires des performances](#)

[DLSw](#)

[Filtrage des paquets non IP avec des listes de contrôle d'accès MAC étendues et des mappages VLAN](#)

[Autres fonctionnalités non prises en charge](#)

[CPU élevé après activation du routage IPX ou AppleTalk](#)

[Informations connexes](#)

Introduction

Ce document décrit comment les protocoles hérités tels que IPX, AppleTalk et DLSw (Data-Link Switching) sont mieux pris en charge dans un commutateur Catalyst 4000/4500 équipé du nouveau Supervisor III/IV. Ce superviseur est conçu pour le commutateur matériel de paquets IP version 4 (IPv4).

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent savoir comment configurer IPX, AppleTalk et DLSw. Pour plus d'informations sur ces protocoles, reportez-vous aux pages de support suivantes :

- [Page d'assistance technique IPX](#)
- [Page d'assistance technologique AppleTalk](#)

- [Page d'assistance technologique DLSw](#)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 4507R avec Supervisor IV
- Logiciel Cisco IOS® Version 12.1(13)EW

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.

Conventions

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

Routage IPX

Le routage IPX est pris en charge dans le logiciel Cisco IOS Version 12.1(12c)EW et ultérieure. Dans la version initiale, les performances sont comprises entre 20 et 30 kpps ; depuis la version 12.1(13)EW du logiciel Cisco IOS, il a été porté à 80 à 90 kpps. Il est recommandé d'utiliser le logiciel Cisco IOS Version 12.1(19)EW ou ultérieure en raison de la disponibilité d'un correctif logiciel pour l'[ID de bogue Cisco CSCea85204](#) (clients [enregistrés](#) uniquement). Ce débit de transfert est partagé par tous les flux qui passent par le commutateur. Ce transfert augmente la charge du processeur en raison du traitement logiciel. En tant que tel, le débit de transfert obtenu dépend du processeur du commutateur ; par exemple, combien de stratégies BGP (Border Gateway Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) ou OSPF (Open Shortest Path First) et SVI (Switched Virtual Interfaces) le commutateur possède-t-il ?

Remarque : les paquets IPv4 continuent d'être routés dans le matériel, même si les paquets IPX sont routés par logiciel.

Fonctionnalités prises en charge

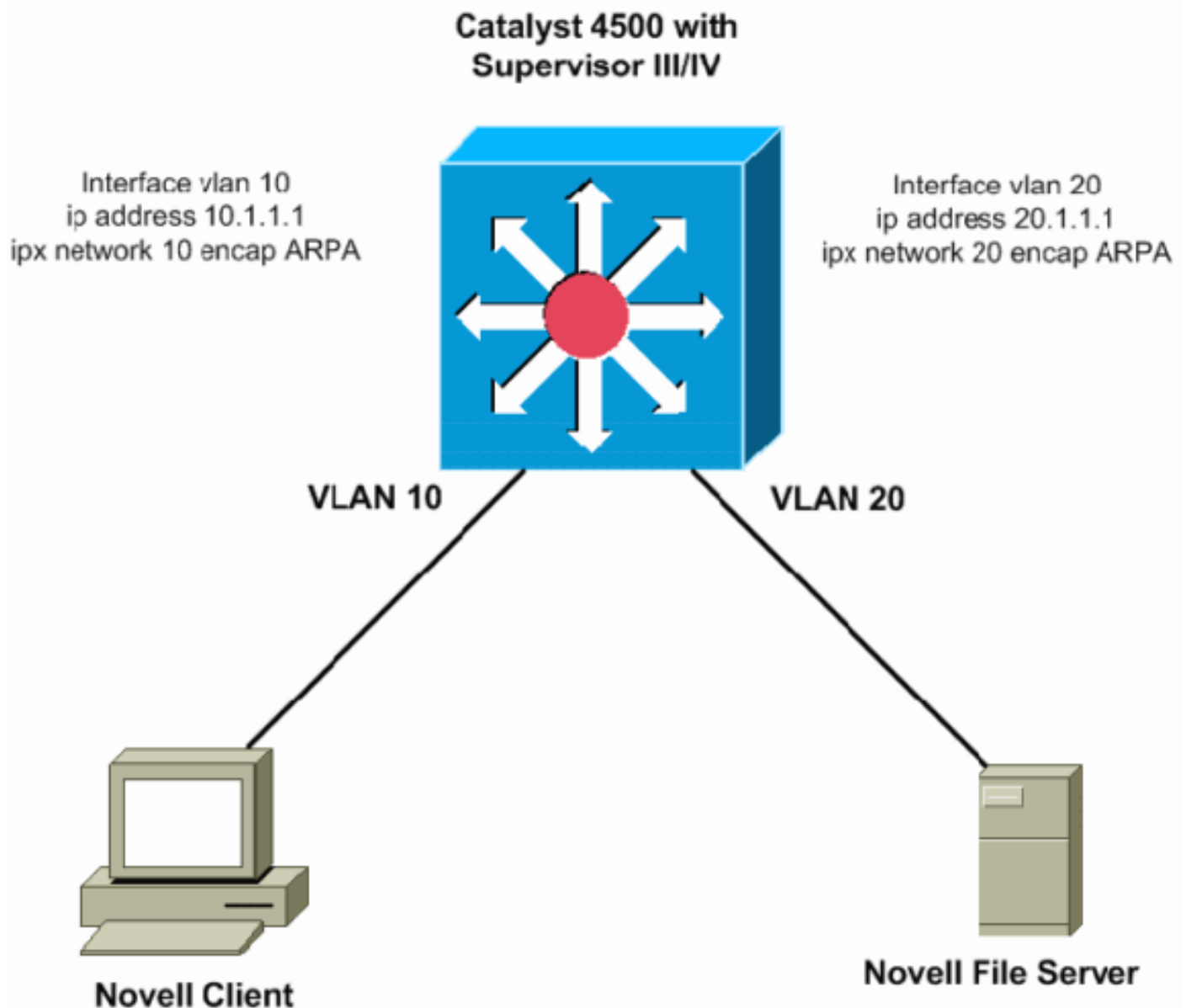
- La liste de contrôle d'accès MAC (ACL) pour IPX est prise en charge dans le logiciel Cisco IOS Version 12.1(12c)EW et ultérieure, qui peut être utilisé pour contrôler les paquets IPX.
- Protocole RIP (IPX Routing Information Protocol) (protocole SAP [Service Advertising Protocol])
- Protocole EIGRP (Enhanced Interior Gateway Routing Protocol) IPX
- compression d'en-tête

Remarque : IPX EIGRP est le protocole de routage préféré entre les routeurs pour de meilleures performances, car EIGRP effectue des mises à jour SAP incrémentielles. Le protocole EIGRP IPX peut être activé sur les segments sans serveur. Pour plus d'informations sur IPX EIGRP, référez-vous à [Comprendre IPX-EIGRP](#).

Limites

- Le routage IPX des paquets n'est pas pris en charge par le matériel. Cela se fait par le biais du traitement logiciel.
- Les listes d'accès IPX standard (800-899), IPX étendues (900-999), Get Nearest Server (GNS) ou SAP Filter (1000-1099) de Novell ne sont actuellement pas prises en charge.
- Pour le routage de logiciel IPX, ceux-ci ne sont pas pris en charge : Protocole NHRP (Next Hop Resolution Protocol) Protocole NLSP (Netware Link Service Protocol) trames jumbo

Cette figure illustre un scénario type avec le Catalyst 4000/4500 avec le routage IPX Supervisor III/IV. Dans ce scénario, les clients se trouvent dans le VLAN 10 et les serveurs dans le VLAN 20. IPX est configuré sur les interfaces VLAN 10 et 20, comme illustré dans ce schéma :



[Routage AppleTalk](#)

Le routage AppleTalk est pris en charge dans le logiciel Cisco IOS Version 12.1(12c)EW et ultérieure. Dans la version initiale, les performances sont comprises entre 20 et 30 kpps ; depuis la version 12.1(13)EW du logiciel Cisco IOS, il a été porté à 80 à 90 kpps. Il est recommandé d'utiliser le logiciel Cisco IOS Version 12.1(19)EW ou ultérieure en raison de la disponibilité d'un correctif logiciel pour l'[ID de bogue Cisco CSCea85204](#) (clients [enregistrés](#) uniquement). Ce débit de transfert est partagé par tous les flux qui passent par le commutateur. Ce transfert augmente la

charge du processeur en raison du traitement logiciel. En tant que tel, le débit de transfert obtenu dépend du processeur du commutateur : par exemple, combien de stratégies BGP, de routes EIGRP ou OSPF et d'interfaces SVI le commutateur possède-t-il ?

Remarque : les paquets IPv4 continuent d'être routés dans le matériel, même si les paquets AppleTalk sont routés par logiciel.

Fonctionnalités prises en charge

- La liste de contrôle d'accès MAC pour AppleTalk est prise en charge dans le logiciel Cisco IOS Version 12.1(12c)EW et ultérieure, qui peut être utilisé pour contrôler les paquets IPX.
- Routage DDP (Datagram Delivery Protocol)
- RTMP (Routing Table Maintenance Protocol)
- NBP (Name Binding Protocol)
- Protocole AppleTalk Echo (AEP)
- EIGRP AppleTalk

Remarque : le protocole EIGRP AppleTalk est le protocole de routage préféré entre les routeurs pour de meilleures performances, car le protocole EIGRP effectue des mises à jour incrémentielles. Pour plus d'informations sur le protocole EIGRP AppleTalk, référez-vous à la section [Configuration du protocole IGRP amélioré AppleTalk](#) de [Configuration d'AppleTalk](#).

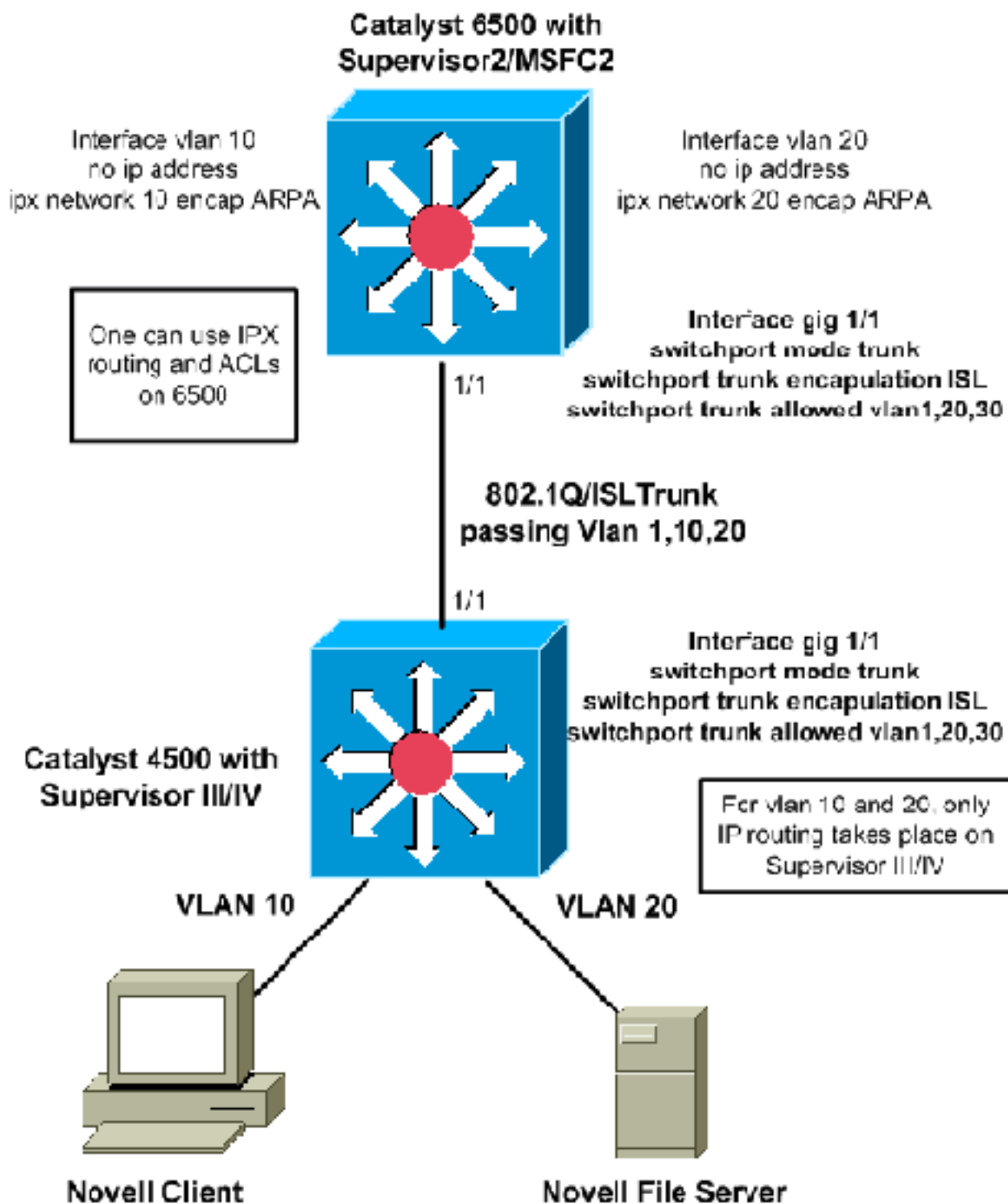
Limites

- Le routage AppleTalk des paquets n'est pas pris en charge par le matériel. Cela se fait par le biais du traitement logiciel.
- Les listes de contrôle d'accès AppleTalk ne sont pas prises en charge actuellement.
- Pour le routage du logiciel AppleTalk, ceux-ci ne sont pas pris en charge : Protocole AURP (Update-Based Routing Protocol) AppleTalk Protocole de contrôle AppleTalk pour PPP trames jumbo

Routage via un routeur externe

Si votre réseau nécessite de meilleures performances de routage des protocoles hérités précédemment mentionnés, vous pouvez utiliser un routeur externe (périphérique de couche 3 [L3]). Un tel périphérique de couche 3 peut être une carte MSFC (Multilayer Switch Feature Card) Catalyst 6000, un commutateur RSM Catalyst 5000, un commutateur de couche 3 (tel qu'un commutateur 2948G-L3) ou tout routeur. Ces périphériques effectuent le routage d'IPX avec l'assistance matérielle, et les performances sont bien supérieures à celles du Supervisor III/IV. Le Supervisor III/IV peut acheminer l'IP dans le chemin de commutation matériel, mais le périphérique externe achemine les protocoles hérités.

Le schéma suivant illustre un scénario dans lequel IPX est routé sur le commutateur principal/de distribution Catalyst 6500 sur la carte MSFC tandis que IP est routé entre VLAN 10 et VLAN 20 sur le commutateur Catalyst 4500 avec Supervisor III/IV. Les deux commutateurs sont agrégés, ce qui autorise les VLAN requis. L'avantage de ce type de conception est la possibilité d'utiliser des listes de contrôle d'accès IPX standard et l'augmentation des performances due au transfert assisté par matériel de ces paquets entre les deux VLAN. Vous pouvez également utiliser les protocoles de routage IPX sur le Catalyst 6500 ou sur le routeur externe pour communiquer avec les homologues pour l'échange de base de données de routage :



Améliorations supplémentaires des performances

Cette section présente des améliorations potentielles supplémentaires des performances qui peuvent être apportées à la commutation IPX ou AppleTalk sur le routeur externe.

- La liaison entre le routeur externe et le commutateur Catalyst peut être transformée en liaison port-channel, pour obtenir une bande passante plus élevée entre eux et pour avoir une redondance pour la liaison.
- Le trafic IP peut être filtré hors de la liaison de sorte que toute la bande passante soit utilisée pour le trafic non IP. Voici un exemple de configuration pour filtrer le trafic IP via la qualité de service (QoS) :

1. Émettez la commande de configuration globale QoS **qos**, pour activer QoS sur le superviseur.
2. Définissez la liste de contrôle d'accès pour qu'elle corresponde à tout le trafic IP.

```
access-list 101 permit ip any any
```
3. Définissez la carte de classe qui correspond à la liste de contrôle d'accès définie à l'étape 2.

```
class-map match-any ip-drops
match access-group 101
```
4. Définissez la stratégie : définir un régulateur qui abandonnera tout le trafic pour la classe définie à l'étape 3. Contrôlez tout le trafic en utilisant une granularité minimale de 32 kbits/s. Le superviseur abandonne tout le trafic IP avec ce régulateur au-delà de 32 kbits/s (les requêtes ping IP Cisco IOS risquent de ne pas pouvoir passer).

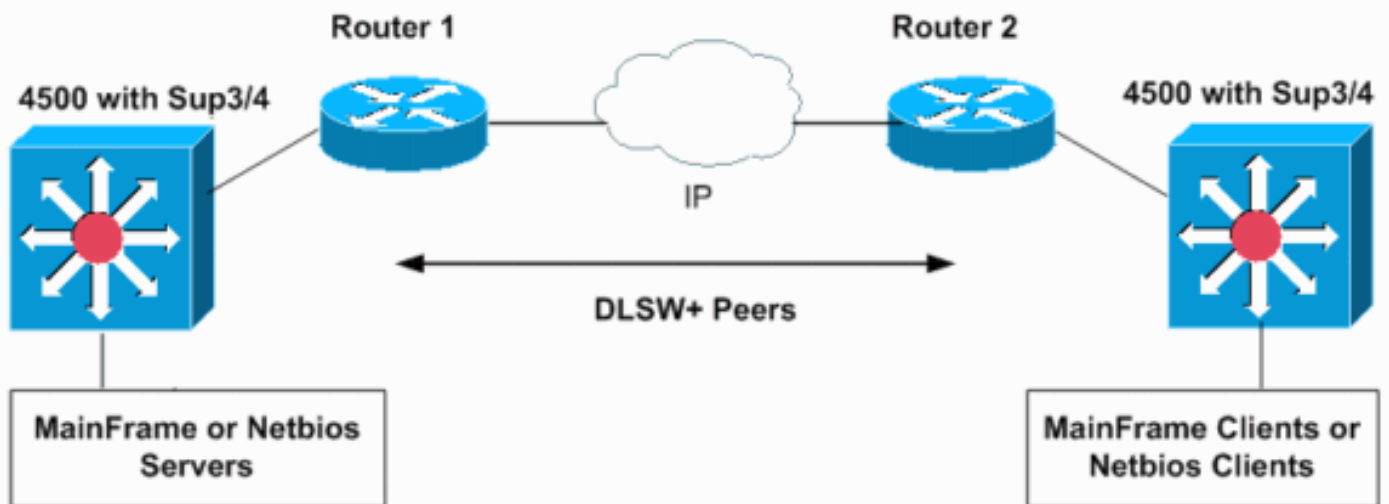
```
policy-map drop-ip
class ip-drops
police 32000 bps 1000 byte conform-action drop exceed-action drop
```
5. Appliquez la stratégie de service sortante sur l'interface qui se connecte au routeur externe.

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

Pour vérifier l'action de réglementation, exécutez la commande **show policy-map interface id-interface**.

DLSw

DLSw n'est pas pris en charge sur le Supervisor III/IV. Pour les réseaux avec SNA et protocoles IP, vous pouvez acheminer le trafic IP sur Catalyst 4000 Supervisor III/IV et relier le trafic SNA avec commutation DLSw sur le logiciel Cisco IOS sur un routeur externe :



Les configurations suivantes montrent comment relier le trafic SNA sur les VLAN 10 et 20 sur deux Catalyst 6500 MSFC2 dans deux domaines SNA distincts. Les agrégations 802.1Q du Supervisor III/IV peuvent être utilisées pour transporter (ponter) le trafic SNA ou NetBIOS vers un routeur Cisco ou vers des commutateurs Catalyst 6500.

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

255.255.255.0	255.255.255.0
bridge-group 1	bridge-group 2
!	!
bridge 1 protocol ieee	bridge 2 protocol ieee
dlsw local-peer peerid	dlsw local-peer peerid
1.1.1.1	2.2.2.2
dlsw remote-peer 0 tcp	dlsw remote-peer 0 tcp
2.2.2.2	1.1.1.1
dlsw bridge-group 1	dlsw bridge-group 2

Ceci montre les configurations réseau pour les commutateurs Catalyst 6500 dans différents domaines. Si les VLAN 10 et 20 sont sur le même commutateur ou MSFC, DLSw n'est pas requis. Les groupes de ponts IEEE simples sur une carte MSFC fonctionneront.

Filtrage des paquets non IP avec des listes de contrôle d'accès MAC étendues et des mappages VLAN

Supervisor III/IV ne prend pas en charge les listes de contrôle d'accès IPX, AppleTalk ou d'autres protocoles hérités. Pour les filtrer, vous pouvez utiliser une liste de contrôle d'accès étendue MAC associée à une carte d'accès VLAN. Les cartes VLAN peuvent contrôler l'accès de tout le trafic d'un VLAN. Vous pouvez appliquer des mappages VLAN sur le commutateur à tous les paquets qui sont routés vers ou depuis un VLAN ou qui sont pontés dans un VLAN. Contrairement aux listes de contrôle d'accès des routeurs, les cartes VLAN ne sont pas définies par la direction (entrée ou sortie).

Dans cet exemple de scénario, ces deux critères sont les objectifs de configuration :

- Empêchez tout le trafic IPX de l'hôte 000.0c00.0111 vers l'hôte 000.0c00.0211, mais autorisez tout autre trafic IPX et de protocole non IP via le VLAN 20.
- Refuser tout le trafic AppleTalk pour VLAN 10.

Remarque : les paquets IP ne peuvent pas être filtrés via une liste de contrôle d'accès MAC.

Remarque : Les listes de contrôle d'accès étendues MAC nommées ne peuvent pas être appliquées aux interfaces de couche 3.

1. Définissez des listes de contrôle d'accès MAC étendues pour définir le trafic intéressant pour les cartes 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. Exécutez la commande **show access-list *access-list-name* pour vérifier la liste de contrôle d'accès MAC étendue configurée**. Les listes de contrôle d'accès dans l'exemple précédent sont **denyIPXACL** et **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. Définissez l'action avec les cartes d'accès 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. Exécutez la commande **show vlan access-map *name* pour vérifier les cartes d'accès VLAN définies**.

```
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. Émettez la commande **vlan filter *name* vlan-list *vlan-list*** pour mapper la carte VLAN aux VLAN. Dans cet exemple, vous voulez filtrer IPX entre des hôtes spécifiques dans VLAN 20 et refuser AppleTalk sur VLAN 10.

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

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

6. Exécutez la commande **show vlan filter vlan *vlan-id*** pour vérifier que les filtres VLAN sont en place.


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

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

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

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

Autres fonctionnalités non prises en charge

Le Supervisor III/IV ne prend pas en charge ces fonctionnalités :

- Pontage de secours ou pontage inter-VLAN pour ponter les protocoles non routables
- Routage DECnet

Reportez-vous à [la section précédente](#), pour voir un exemple d'utilisation d'un routeur externe pour atteindre cette fonctionnalité.

CPU élevé après activation du routage IPX ou AppleTalk

Une fois que vous avez activé le routage IPX ou AppleTalk, l'utilisation du CPU augmente en fonction de la quantité de trafic IPX ou AppleTalk qui est acheminée dans le logiciel via le commutateur. Si vous émettez la commande **show processor cpu**, le résultat peut indiquer que le processus `Cat4k Mgmt LoPri` utilise le processeur. Cela indique que les paquets sont en cours de commutation de processus.

```
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

Remarque : Si le routage IPX ou AppleTalk n'est pas activé, mais que `Cat4k Mgmt LoPri` utilise un processeur élevé, vous devrez peut-être dépanner les paquets envoyés au processeur pour traitement. Contactez [le support technique de Cisco](#), si vous avez besoin d'une assistance supplémentaire.

Informations connexes

- [Configuration de la sécurité réseau avec les ACL](#)
- [Pages d'assistance Catalyst 4500](#)
- [Pages de support pour les produits LAN](#)
- [Page de support sur la commutation LAN](#)
- [Support et documentation techniques - Cisco Systems](#)