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

Contenu

Introduction

Ce document décrit comment des protocoles existants tels que l'IPX, l'AppleTalk, et le Data-Link Switching (DLSw) mieux sont pris en charge dans un commutateur du Catalyst 4000/4500 équipé du superviseur plus nouveau III/IV. Ce superviseur est conçu à la version d'IP de commutateur de matériel 4 paquets (d'ipv4).

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la connaissance de la façon configurer l'IPX, l'AppleTalk, et le DLSw. Pour des informations sur ces protocoles, référez-vous à ces pages de support :

- Page de support technologique IPX
- Page de support technologique d'AppleTalk

- Page de support technologique de DLSw

Composants utilisés

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

- Catalyst 4507R avec le superviseur IV
- Version de logiciel 12.1(13)EW de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Acheminement de l'IPX

L'acheminement de l'IPX est pris en charge dans la version du logiciel Cisco IOS 12.1(12c)EW et plus tard. Dans la version initiale, la représentation est de l'ordre de 20 à 30 kpps ; en date du Logiciel Cisco IOS version 12.1(13)EW, il a été grimpé jusqu'à 80 à 90 kpps. Il est recommandé que vous utilisez le Logiciel Cisco IOS version 12.1(19)EW ou plus tard en raison de la Disponibilité d'une correction logicielle pour l'ID de bogue Cisco CSCea85204 (clients enregistrés seulement). Ce taux à terme est partagé par tous les écoulements qui suivent par le commutateur. Cet expédition augmente le chargement CPU dû au traitement de logiciel. En soi, le taux à terme réalisé dépend de la CPU de commutateur ; par exemple, combien de stratégies, Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) ou Protocole OSPF (Open Shortest Path First) de Protocole BGP (Border Gateway Protocol) conduit, et interfaces virtuelles commutées (SVI) que le commutateur a.

Remarque: Des paquets d'ipv4 continuent à être conduits dans le matériel, quoique des paquets IPX logiciel-soient conduits.

Caractéristiques prises en charge

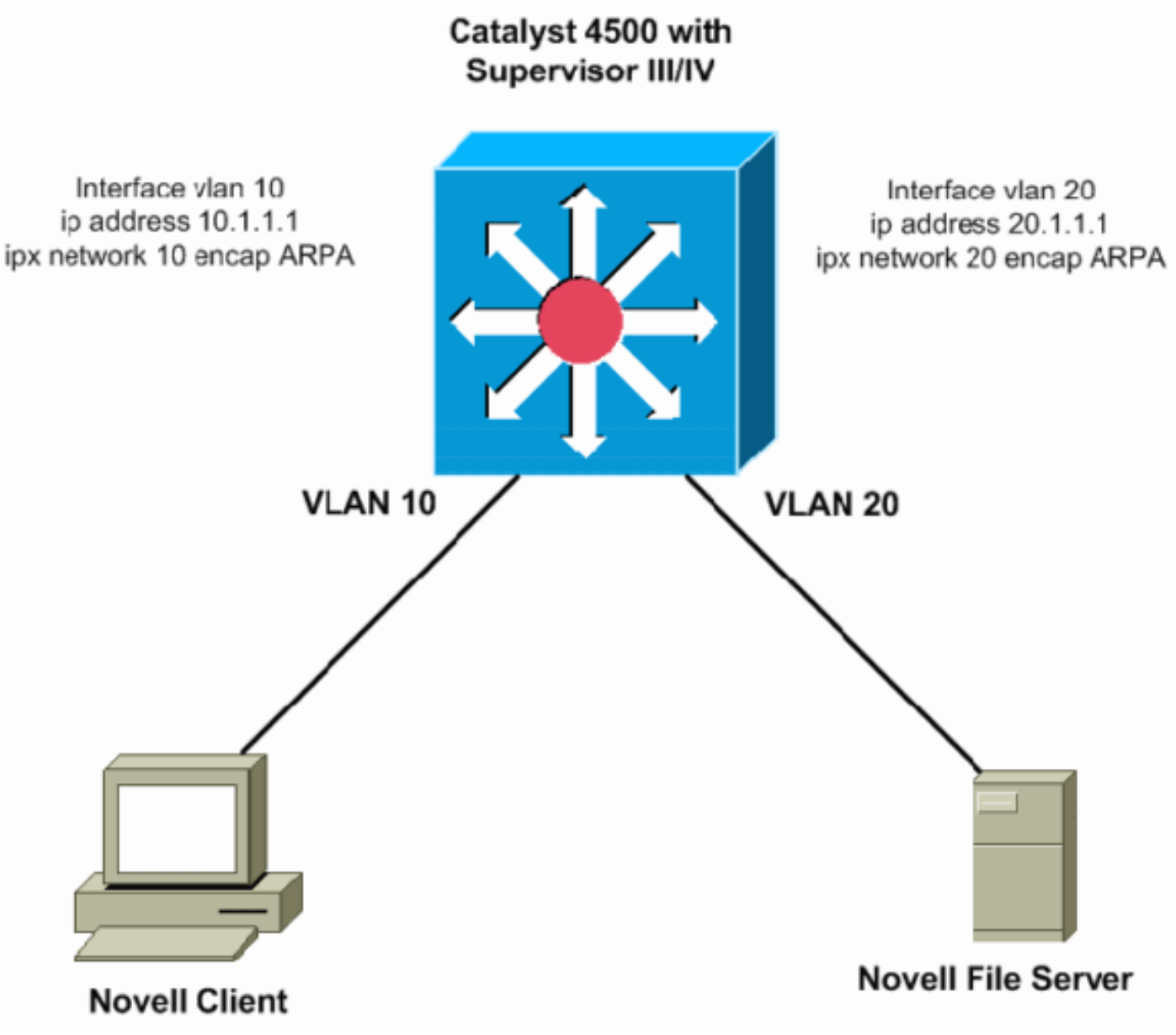
- La liste de contrôle d'accès de MAC (ACL) pour l'IPX est prise en charge dans la version du logiciel Cisco IOS 12.1(12c)EW et plus tard, qui peut être utilisée pour contrôler les paquets IPX.
- Protocole RIP (Routing Information Protocol) IPX (service annonçant Protocol [SAP])
- Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) IPX
- compression d'en-tête

Remarque: L'IPX EIGRP est le protocole de routage préféré entre les Routeurs pour une meilleure représentation, car l'EIGRP fait des mise à jour incrémentielle des points d'accès au service. L'IPX EIGRP peut être activé sur des segments sans serveur. Pour des informations sur l'IPX EIGRP, référez-vous compréhension derrière l'IPX EIGRP.

Limites

- Le routage ipx des paquets n'est pas assisté par le matériel. Il est fait par le traitement de logiciel.
- La norme IPX de Novell (800-899), IPX étendu (900-999), obtiennent le serveur le plus proche (GNS), ou des Listes d'accès des filtres de SAP (1000-1099) ne sont pas actuellement prises en charge.
- Pour le routage de logiciel IPX, ceux-ci ne sont pas pris en charge :Protocole NHRP (Next Hop Resolution Protocol)Service de lien de NetWare Protocol (NLSP)Trames étendues

Cette figure montre un scénario typique avec du Catalyst 4000/4500 avec le superviseur III/IV conduisant l'IPX. Dans ce scénario, les clients sont dans le VLAN 10 et des serveurs sont dans le VLAN 20. L'IPX est configuré sur le VLAN 10 et 20 interfaces, suivant les indications de ce diagramme :



Acheminement de l'AppleTalk

L'acheminement de l'AppleTalk est pris en charge dans la version du logiciel Cisco IOS 12.1(12c)EW et plus tard. Dans la version initiale, la représentation est de l'ordre de 20 à 30 kpps ; en date du Logiciel Cisco IOS version 12.1(13)EW, il a été grimpé jusqu'à 80 à 90 kpps. Il est recommandé que vous utilisez le Logiciel Cisco IOS version 12.1(19)EW ou plus tard en raison de

la Disponibilité d'une correction logicielle pour l'ID de bogue Cisco CSCea85204 (clients enregistrés seulement). Ce taux à terme est partagé par tous les écoulements qui suivent par le commutateur. Cet expédition augmente le chargement CPU dû au traitement de logiciel. En soi, le taux à terme réalisé dépend de la CPU de commutateur : par exemple, combien de stratégies BGP, artères EIGRP ou OSPF, et SVI que le commutateur a.

Remarque: Des paquets d'ipv4 continuent à être conduits dans le matériel, quoique des paquets d'AppleTalk logiciel-soient conduits.

Caractéristiques prises en charge

- L'ACL de MAC pour l'AppleTalk est pris en charge dans la version du logiciel Cisco IOS 12.1(12c)EW et plus tard, qui peut être utilisée pour contrôler les paquets IPX.
- Routage du protocole de transmission de datagramme (DDP)
- Conduisant le protocole de maintenance des tables (RTMP)
- Protocole de résolution de nom (NBP)
- Protocole d'écho APPLETALK (AEP)
- AppleTalk EIGRP

Remarque: L'AppleTalk EIGRP est le protocole de routage préféré entre les Routeurs pour une meilleure représentation, car l'EIGRP fait des mises à jour incrémentielles. Pour plus d'informations sur l'AppleTalk EIGRP, référez-vous à la section configurante d'Enhanced IGRP d'AppleTalk de configurer l'AppleTalk.

Limites

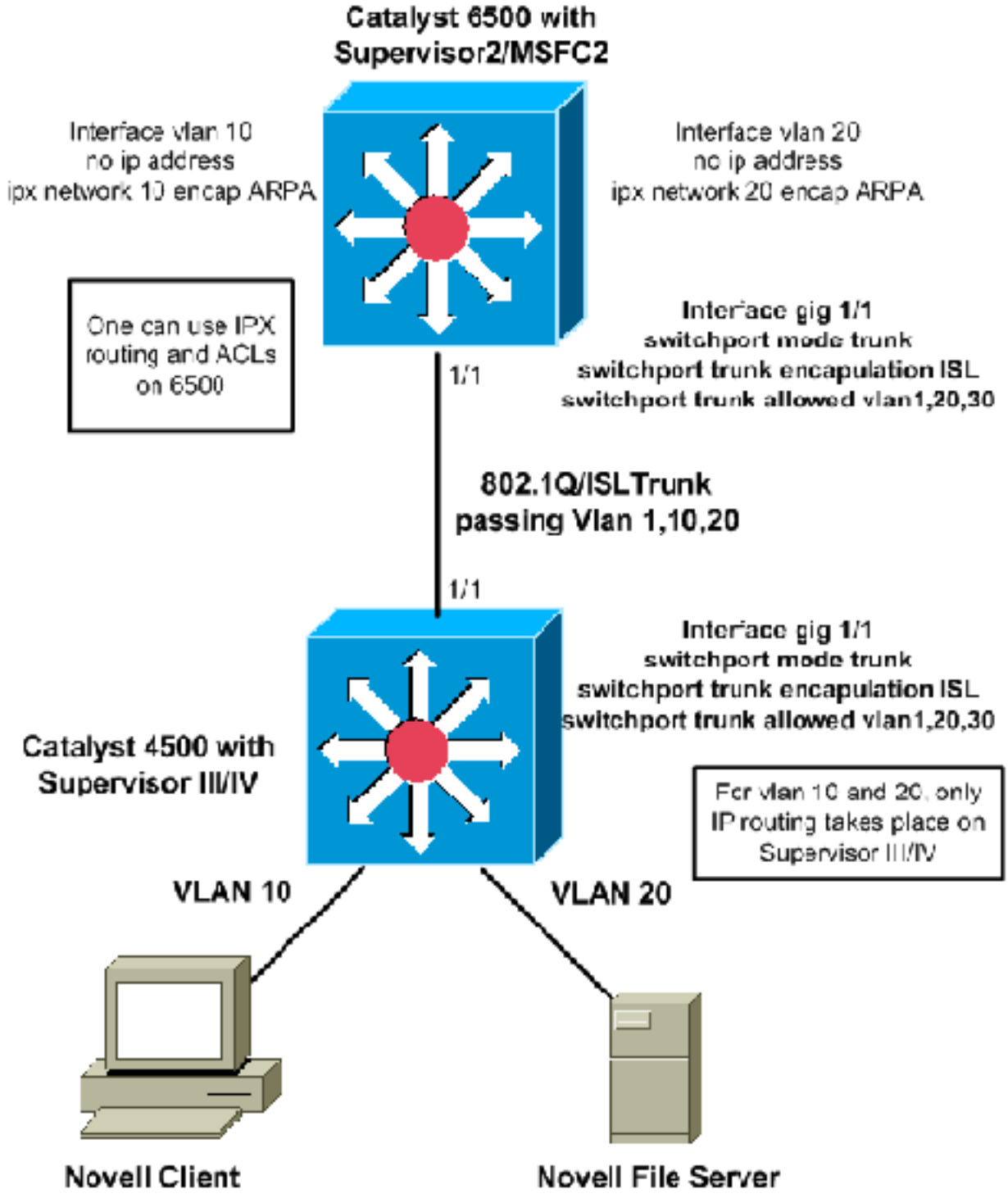
- L'appletalk routing des paquets n'est pas assisté par le matériel. Il est fait par le traitement de logiciel.
- L'AppleTalk ACLs ne sont pas actuellement pris en charge.
- Pour le routage de logiciel d'AppleTalk, ceux-ci ne sont pas pris en charge :Protocole AURP (AppleTalk Update-Based Routing Protocol)Protocole de contrôle Appletalk pour le PPPTrames étendues

Routage par un routeur externe

Si votre réseau exige une meilleure représentation de routage des protocoles existants alors précédemment mentionnés, vous pouvez vouloir utiliser un routeur externe (périphérique de couche 3 [L3]). Un tel périphérique L3 pourrait être une carte de commutation multicouche du Catalyst 6000 (MSFC), le Catalyst 5000 RSM, le commutateur L3 (tel qu'un 2948G-L3), ou n'importe quel routeur. Ces périphériques exécute le routage de l'IPX avec l'assistance de matériel, et la représentation est beaucoup plus grande que le superviseur III/IV. Le superviseur III/IV peut conduire l'IP dans le chemin de commutation de matériel, mais le périphérique externe conduit les protocoles existants.

Le prochain diagramme montre un scénario dans lequel l'IPX est conduit sur Catalyst 6500 le principal/distribution sur le MSFC tandis que l'IP est conduit entre le VLAN 10 et le VLAN 20 au Catalyst 4500 avec le superviseur III/IV. Les deux Commutateurs sont trunked, qui permet les VLAN exigés. L'avantage de ce type de conception est la capacité d'utiliser IPX standard ACLs et l'augmentation des performances due à l'expédition assisté par le matériel de ces paquets entre les deux VLAN. Vous pouvez également employer des protocoles de routage ipx relatif au

Catalyst 6500 ou relatif au routeur externe, pour communiquer avec les pairs pour conduire l'échange de base de données :



Améliorations de performance supplémentaire

Ceci sectionne apporte quelques améliorations des performances potentielles supplémentaires qui peuvent être apportées à l'IPX ou à la commutation d'AppleTalk sur le routeur externe.

- Le lien entre le routeur externe et le commutateur de Catalyst a pu être transformé en lien de Port canalisé, pour obtenir la bande passante élevée entre eux et pour avoir la Redondance pour le lien.
- Le trafic IP peut être filtré hors du lien de sorte que toute les bande passante soit utilisée pour le trafic non-IP. C'est une configuration d'échantillon pour filtrer le trafic IP à l'aide du Qualité

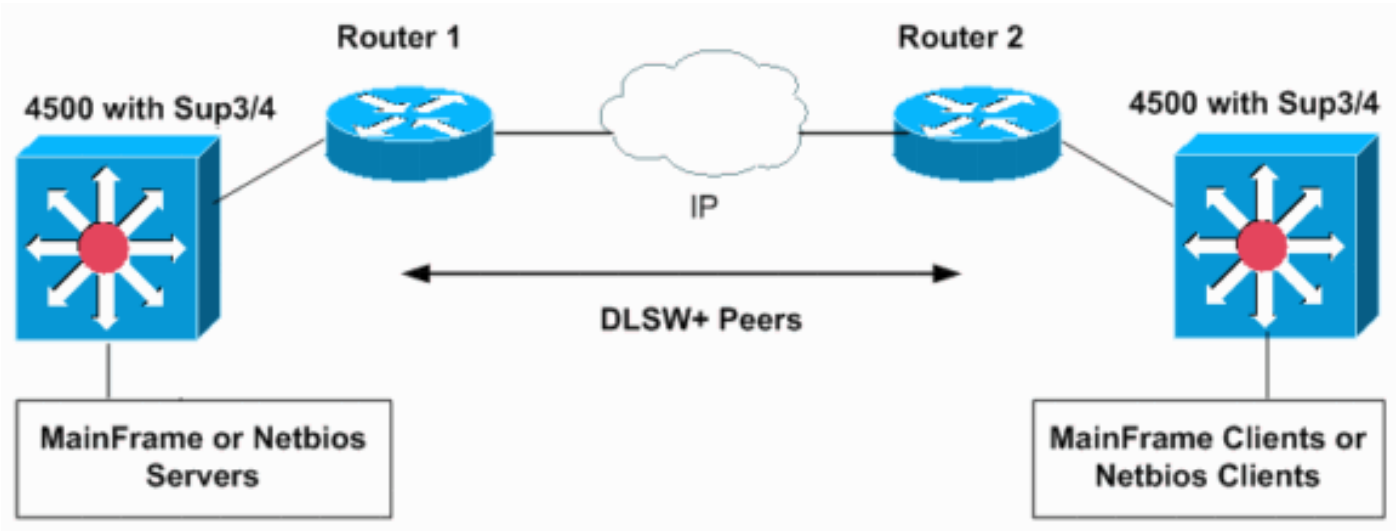
de service (QoS) :

1. Émettez les **qos de** commande de configuration globale de QoS, pour activer QoS sur le superviseur.
2. Définissez l'ACL pour apparier tout le trafic IP.
   ```
   access-list 101 permit ip any any
   ```
3. Définissez le class-map qui apparie l'ACL défini dans l'étape 2.
   ```
   class-map match-any ip-drops
     match access-group 101
   ```
4. Définissez la stratégie : définissez un régulateur qui relâchera tout le trafic pour la classe définie dans la police d'étape 3. tout le trafic utilisant une finesse minimum de 32 Kbps. Le superviseur relâchera tout le trafic IP avec ce régulateur au delà de 32 Kbps (les pings IP de Cisco IOS peuvent ne pas pouvoir intervenir).
   ```
   policy-map drop-ip
     class ip-drops
       police 32000 bps 1000 byte conform-action drop exceed-action drop
   ```
5. Appliquez la stratégie de service en partance sur l'interface qui se connecte au routeur externe.
   ```
   interface GigabitEthernet 1/1
       service-policy output drop-ip
   ```

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

DLSw

DLSw n'est pas pris en charge sur le superviseur III/IV. Pour des réseaux avec des protocoles SNA et IP, vous pouvez conduire le trafic IP sur le superviseur III/IV de Catalyst 4000 et jeter un pont sur le trafic SNA avec la commutation de DLSw sur le logiciel de Cisco IOS sur un routeur externe :



Les prochaines configurations affichent comment jeter un pont sur le trafic SNA sur VLAN 10 et 20 sur deux le Catalyst 6500 MSFC2 dans deux domaines distincts SNA. Les joncteurs réseau de 802.1Q sur le superviseur III/IV peuvent être utilisés pour porter (passerelle) la SNA ou le trafic de Netbios à un routeur de Cisco ou aux Commutateurs de Catalyst 6500.

`hostname MSFCRouter-1`	`hostname MSFCRouter-2`

interface loopback1 ip address 1.1.1.1 ! int vlan10 ip add 10.10.10.254 255.255.255.0 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	interface loopback1 ip address 2.2.2.2 ! int vlan20 ip add 10.10.20.254 255.255.255.0 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

Ceci affiche des configurations réseau pour des Commutateurs de Catalyst 6500 dans différents domaines. Si VLAN 10 et 20 sont sur le même commutateur ou MSFC, DLSw n'est pas exigé. Les groupes simples de passerelle d'IEEE sur un MSFC fonctionneront.

Paquets Non-IP de filtrage avec les cartes étendues de MAC ACLs et VLAN

Le superviseur III/IV ne prend en charge pas l'IPX, l'AppleTalk, ou tout autre protocole existant ACLs. Pour les filtrer, vous pouvez utiliser un ACL MAC-étendu combiné avec une carte d'accès VLAN. Les cartes VLAN peuvent contrôler l'accès de tout le trafic dans un VLAN. Vous pouvez appliquer des cartes VLAN sur le commutateur à tous les paquets dans lesquels sont conduits ou hors d'un VLAN ou pont dans un VLAN. À la différence du routeur ACLs, des cartes VLAN ne sont pas définies par la direction (entrée ou sortie).

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

- Empêchez tout le trafic IPX de l'hôte 000.0c00.0111 pour héberger 000.0c00.0211, mais permettez tout autre trafic de protocole IPX et non-IP par le VLAN 20.
- Refusez tout le trafic d'AppleTalk pour le VLAN 10.

Remarque: Des paquets IP ne peuvent pas être filtrés à l'aide d'un ACL de MAC.

Remarque: ACLs étendu MAC Désigné ne peut pas être appliqué aux interfaces L3.

1. Define a étendu le MAC ACLs 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. Émettez la commande d'Access-liste-*nom de **liste d'accès d'exposition*** de vérifier l'ACL de MAC étendu configuré. L'ACLs 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. Émettez la commande de *nom de **show vlan access-map*** de vérifier défini les cartes d'accès 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. Émettez la commande de VLAN-*liste de VLAN-**liste de** nom de **vlan filter*** de tracer la carte VLAN aux VLAN. Dans cet exemple, vous voulez filtrer l'IPX entre les hôtes spécifiques dans le VLAN 20 et refuser l'AppleTalk sur le VLAN 10.

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

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

6. Émettez la commande de VLAN-*id de **VLAN de show vlan filter*** de vérifier que les vlans filters 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.
```

D'autres fonctions non prises en charge

Le superviseur III/IV ne prend en charge pas ces caractéristiques :

- Transition ou inter-VLAN de retour jetant un pont sur pour jeter un pont sur des protocoles non routable
- Decnet routing

Référez-vous à la section précédente, pour voir un exemple de la façon utiliser un routeur externe pour réaliser cette fonctionnalité.

CPU de haute après l'activation de l'IPX ou de l'appletalk routing

Après que vous activiez l'IPX ou l'appletalk routing, l'utilisation du CPU augmentera basé sur la quantité du trafic IPX ou d'AppleTalk qui est conduit en logiciel par le commutateur. Si vous émettez la commande **CPU de processeur d'exposition**, la sortie peut prouver que le processus `Cat4k gestion LoPri` utilise la CPU. Ceci indique que les paquets sont commutés par 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 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
```

Remarque: Si vous ne faites pas activer l'IPX ou l'appletalk routing, mais voyez toujours `Cat4k gestion LoPri` utilisant la CPU de haute, alors vous pouvez devoir dépanner quels paquets sont envoyés à la CPU pour le traitement. Entrez en contact avec le support technique de Cisco, si vous avez besoin davantage de d'assistance.

Informations connexes

- Configuration de la sécurité réseau avec les ACL
- Pages de support du Catalyst 4500
- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems