Supporto dei protocolli legacy con Catalyst 4000 Supervisor III/IV

Sommario

Introduzione

In questo documento viene descritto come supportare al meglio protocolli legacy come IPX, AppleTalk e DLSw (Data-Link Switching) in uno switch Catalyst 4000/4500 con il nuovo Supervisor III/IV. Questo Supervisor è progettato per i pacchetti IP versione 4 (IPv4) dello switch hardware.

Prerequisiti

Requisiti

I lettori di questo documento devono sapere come configurare IPX, AppleTalk e DLSw. Per informazioni su questi protocolli, consultare le seguenti pagine di supporto:

- Pagina di supporto per la tecnologia IPX
- Pagina di supporto per la tecnologia AppleTalk
- Pagina di supporto per la tecnologia DLSw

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Routing IPX

Il routing IPX è supportato nel software Cisco IOS versione 12.1(12c)EW e successive. Nella versione iniziale, le prestazioni sono comprese tra 20 e 30 kpps; a partire dal software Cisco IOS versione 12.1(13)EW, è stato aumentato a 80 kpps e 90 kpps. Si consiglia di utilizzare il software Cisco IOS versione 12.1(19)EW o successive perché è disponibile una correzione software per l'ID bug Cisco CSCea85204 (solo utenti registrati). Questa velocità di inoltro è condivisa da tutti i flussi che seguono lo switch. Questo inoltro aumenta il carico della CPU a causa dell'elaborazione del software. Di conseguenza, la velocità di inoltro ottenuta dipende dalla CPU dello switch; ad esempio, il numero di policy Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP) o Open Shortest Path First (OSPF) e di interfacce virtuali commutate (SVI) di cui dispone lo switch.

Nota: i pacchetti IPv4 continuano ad essere indirizzati nell'hardware, anche se i pacchetti IPX sono indirizzati al software.

Caratteristiche supportate

- MAC Access Control List (ACL) per IPX è supportato nel software Cisco IOS versione 12.1(12c)EW e successive, che può essere usato per controllare i pacchetti IPX.
- Protocollo RIP (Routing Information Protocol) IPX (Service Advertising Protocol [SAP])
- Protocollo EIGRP (IPX Enhanced Interior Gateway Routing Protocol)
- compressione intestazione

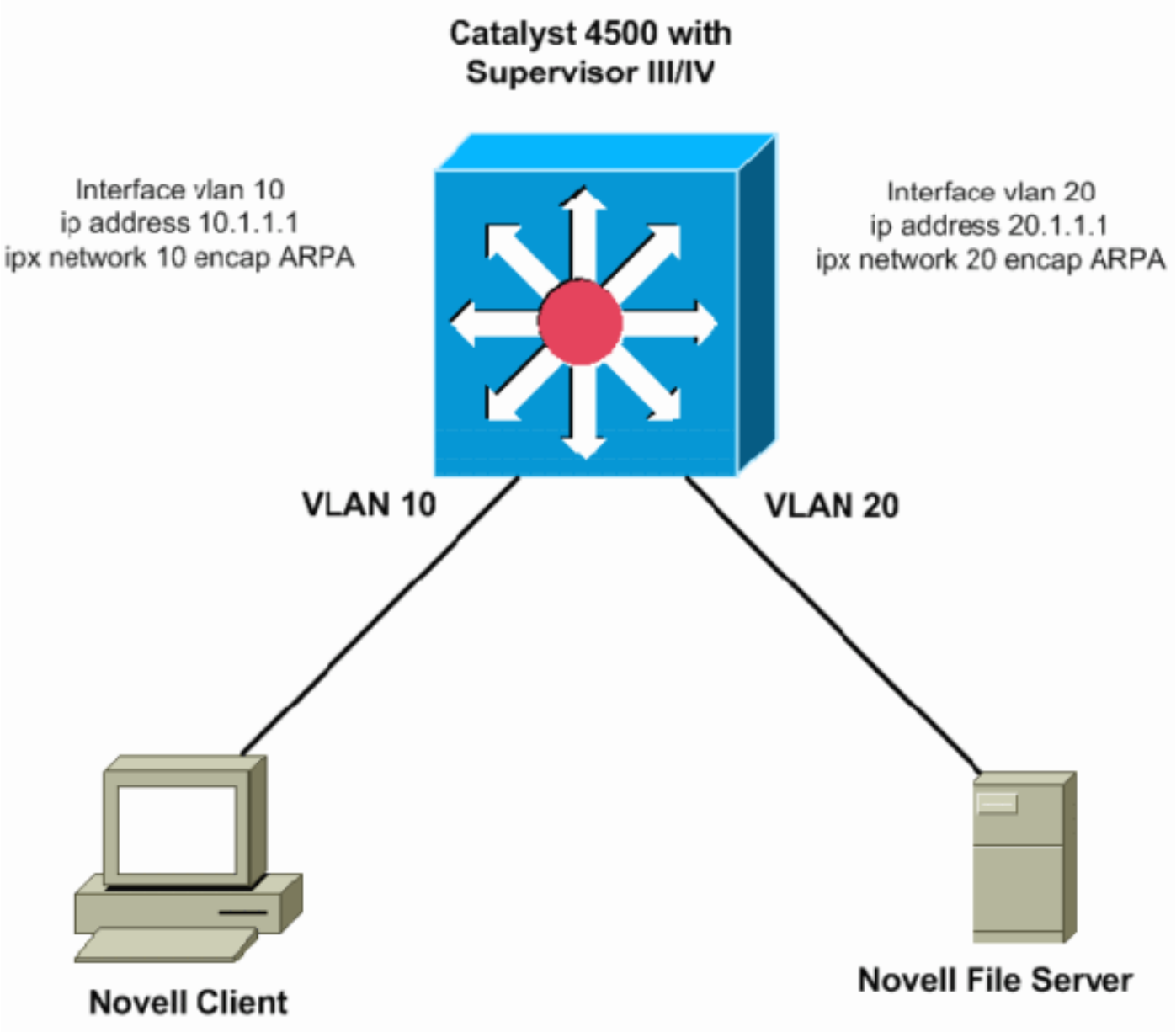
Nota: IPX EIGRP è il protocollo di routing preferito tra router per prestazioni migliori, in quanto EIGRP esegue aggiornamenti SAP incrementali. È possibile abilitare IPX EIGRP sui segmenti senza server. Per informazioni su IPX EIGRP, vedere Informazioni su IPX-EIGRP.

Limitazioni

- Il routing IPX dei pacchetti non è assistito da hardware. Viene eseguita tramite elaborazione software.
- Gli elenchi degli accessi IPX standard (800-899), IPX esteso (900-999), Get Nearest Server

(GNS) o i filtri SAP (1000-1099) non sono attualmente supportati.
- Per il routing del software IPX, non sono supportati:Protocollo NHRP (Next Hop Resolution Protocol)Protocollo NLSP (Netware Link Service Protocol)frame jumbo

Nella figura viene mostrato uno scenario tipico con Catalyst 4000/4500 con routing IPX Supervisor III/IV. In questo scenario, i client si trovano sulla VLAN 10 e i server sulla VLAN 20. Il protocollo IPX è configurato sulla VLAN 10 e sulle interfacce 20, come mostrato nel diagramma seguente:



Routing AppleTalk

Il routing di AppleTalk è supportato nel software Cisco IOS versione 12.1(12c)EW e successive. Nella versione iniziale, le prestazioni sono comprese tra 20 e 30 kpps; a partire dal software Cisco IOS versione 12.1(13)EW, è stato aumentato a 80 kpps e 90 kpps. Si consiglia di utilizzare il software Cisco IOS versione 12.1(19)EW o successive perché è disponibile una correzione software per l'ID bug Cisco CSCea85204 (solo utenti registrati). Questa velocità di inoltro è condivisa da tutti i flussi che seguono lo switch. Questo inoltro aumenta il carico della CPU a causa dell'elaborazione del software. Di conseguenza, la velocità di inoltro ottenuta dipende dalla CPU dello switch: ad esempio, il numero di policy BGP, route EIGRP o OSPF e SVI dello switch.

Nota: i pacchetti IPv4 continuano ad essere indirizzati nell'hardware, anche se i pacchetti

AppleTalk sono indirizzati al software.

Caratteristiche supportate

- Gli ACL MAC per AppleTalk sono supportati nel software Cisco IOS versione 12.1(12c)EW e successive, che può essere utilizzato per controllare i pacchetti IPX.
- Routing Datagram Delivery Protocol (DDP)
- Protocollo RTMP (Routing Table Maintenance Protocol)
- Protocollo NBP (Name Binding Protocol)
- Protocollo AEP (AppleTalk Echo Protocol)
- AppleTalk EIGRP

Nota: per prestazioni migliori, il protocollo EIGRP AppleTalk è il protocollo di routing preferito tra router, in quanto EIGRP esegue aggiornamenti incrementali. Per ulteriori informazioni su AppleTalk EIGRP, fare riferimento alla sezione Configurazione di AppleTalk Enhanced IGRP in Configurazione di AppleTalk.

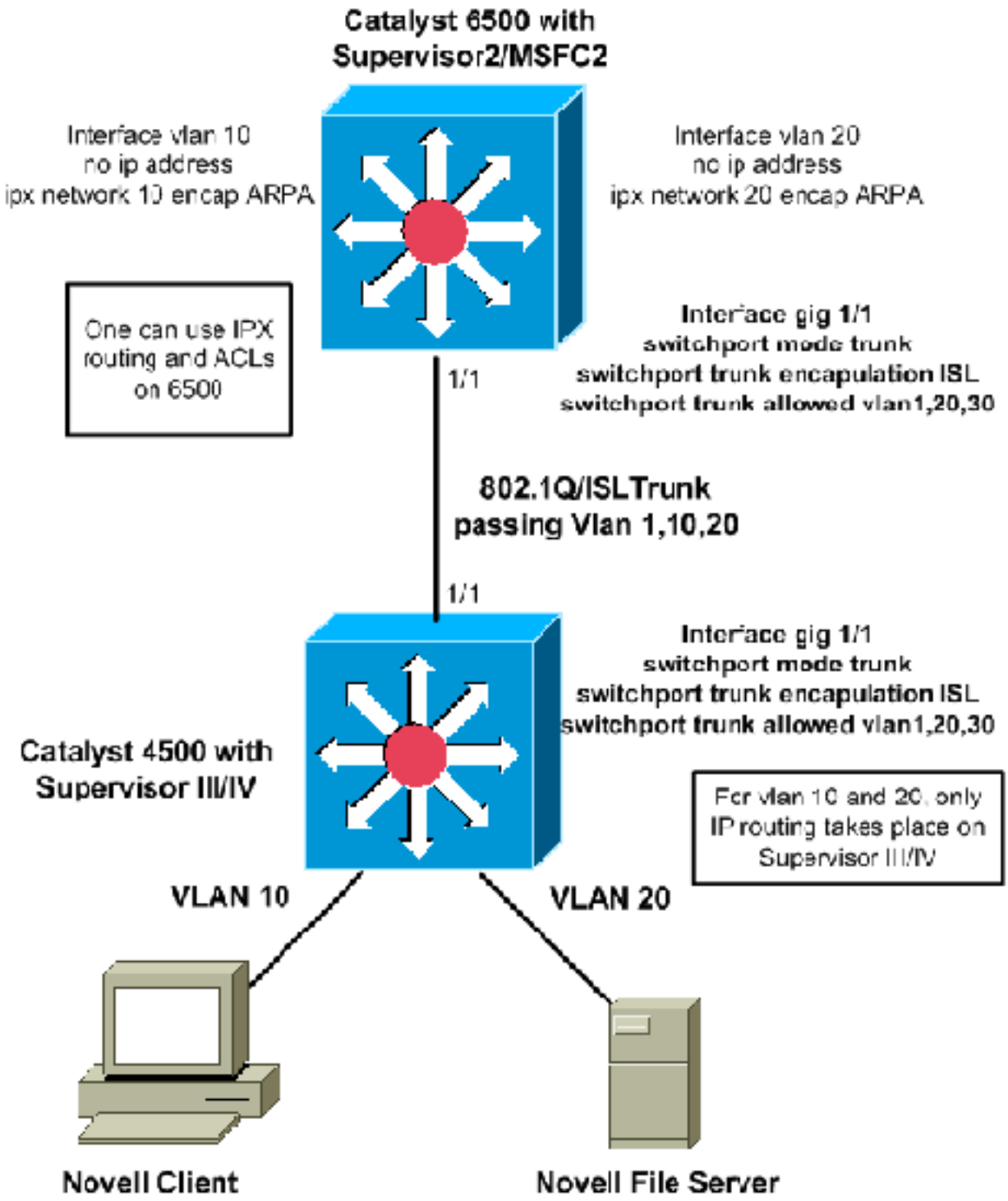
Limitazioni

- Il routing AppleTalk dei pacchetti non è assistito da hardware. Viene eseguita tramite elaborazione software.
- Gli ACL AppleTalk non sono attualmente supportati.
- Per il routing del software AppleTalk, questi non sono supportati:Protocollo AURP (AppleTalk Update-Based Routing Protocol)Protocollo di controllo AppleTalk per PPPframe jumbo

Routing attraverso un router esterno

Se la rete richiede prestazioni di routing migliori rispetto ai protocolli precedenti, è possibile utilizzare un router esterno (dispositivo di livello 3 [L3]). Un dispositivo L3 di questo tipo potrebbe essere un modulo Catalyst 6000 Multilayer Switch Feature Card (MSFC), Catalyst 5000 RSM, uno switch L3 (ad esempio 2948G-L3) o un router qualsiasi. Questi dispositivi eseguono il routing di IPX con assistenza hardware e le prestazioni sono molto superiori a quelle del Supervisor III/IV. Il Supervisor III/IV può instradare l'IP nel percorso di commutazione hardware, ma il dispositivo esterno instrada i protocolli legacy.

Nello schema successivo viene mostrato uno scenario in cui l'IPX viene instradato sul core/distribuzione Catalyst 6500 sull'MSFC mentre l'IP viene instradato tra la VLAN 10 e la VLAN 20 sul Catalyst 4500 con Supervisor III/IV. I due switch sono trunking, il che consente le VLAN richieste. Il vantaggio di questo tipo di progettazione è la capacità di usare ACL IPX standard e l'aumento delle prestazioni causato dall'inoltro basato su hardware di questi pacchetti tra le due VLAN. Per comunicare con i peer per lo scambio del database di routing, è possibile usare anche i protocolli di routing IPX sullo switch Catalyst 6500 o sul router esterno:



Ulteriori miglioramenti delle prestazioni

In questa sezione vengono illustrati ulteriori miglioramenti potenziali delle prestazioni che è possibile apportare alla commutazione IPX o AppleTalk sul router esterno.

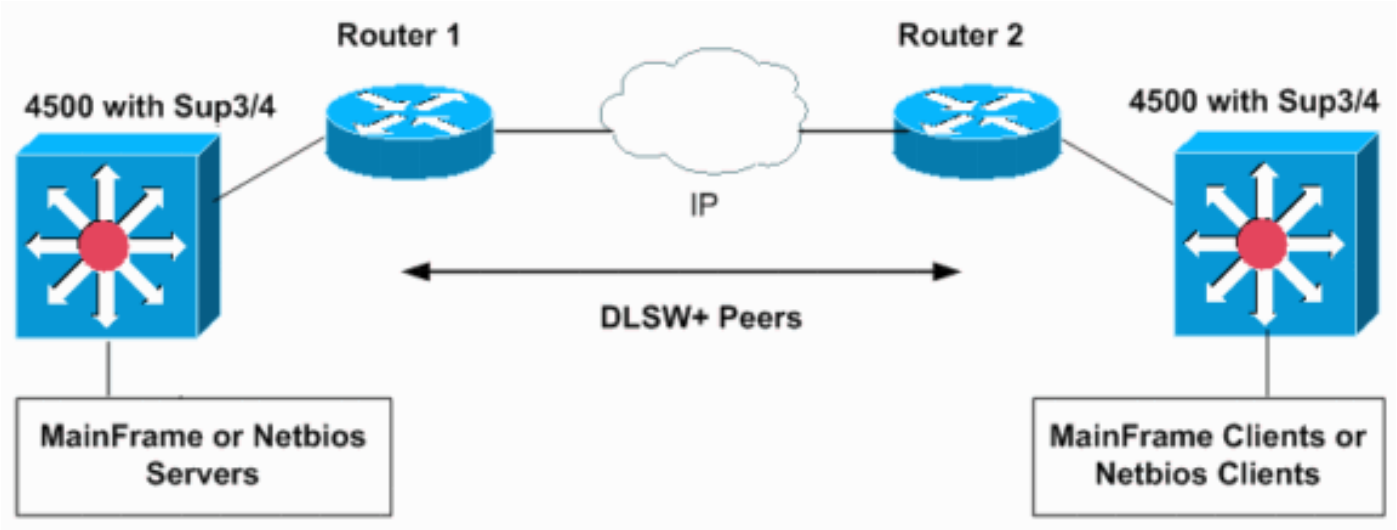
- Il collegamento tra il router esterno e lo switch Catalyst può essere trasformato in un collegamento porta-canale, per ottenere una larghezza di banda più elevata tra i due e per ottenere una ridondanza per il collegamento.
- Il traffico IP può essere filtrato fuori dal collegamento in modo che tutta la larghezza di banda venga usata per il traffico non IP. Di seguito è riportata una configurazione di esempio per filtrare il traffico IP tramite QoS (Quality of Service):

1. Utilizzare il comando di configurazione globale QoS **qos** per abilitare QoS sul Supervisor.
2. Definire l'ACL in modo che corrisponda a tutto il traffico IP.
   ```
   access-list 101 permit ip any any
   ```
3. Definire la class-map che corrisponde all'ACL definito nel passaggio 2.
   ```
   class-map match-any ip-drops
     match access-group 101
   ```
4. Definire il criterio: definire un policer che scarti tutto il traffico per la classe definita nel passaggio 3. Applicare il policer a tutto il traffico utilizzando una granularità minima di 32 kbps. Il Supervisor scarta tutto il traffico IP con questo policer oltre i 32 kbps (potrebbero non essere in grado di passare i ping IP di Cisco IOS).
   ```
   policy-map drop-ip
     class ip-drops
       police 32000 bps 1000 byte conform-action drop exceed-action drop
   ```
5. Applicare i criteri del servizio in uscita sull'interfaccia che si connette al router esterno.
   ```
   interface GigabitEthernet 1/1
       service-policy output drop-ip
   ```

Per verificare l'azione di controllo, eseguire il comando **show policy-map interface** *id-interfaccia*.

DLSw

DLSw non è supportato sul Supervisor III/IV. Per le reti con protocolli SNA e IP, è possibile indirizzare il traffico IP sul Catalyst 4000 Supervisor III/IV e collegare il traffico SNA con la commutazione DLSw sul software Cisco IOS su un router esterno:



Le configurazioni successive mostrano come eseguire il bridging del traffico SNA sulle VLAN 10 e 20 su due Catalyst 6500 MSFC2 in due domini SNA separati. I trunk 802.1Q sul Supervisor III/IV possono essere utilizzati per trasportare (collegare) il traffico SNA o NetBIOS a un router Cisco o a switch 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 bridge-group 1	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

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

Qui vengono mostrate le configurazioni di rete per gli switch Catalyst 6500 in domini diversi. Se le VLAN 10 e 20 si trovano sullo stesso switch o su MSFC, non è richiesto DLSw. Funzioneranno gruppi di bridge IEEE semplici su un MSFC.

Filtraggio di pacchetti non IP con ACL MAC estesi e mappe VLAN

Supervisor III/IV non supporta IPX, AppleTalk o altri ACL di protocollo legacy. Per filtrarli, è possibile usare un ACL esteso all'indirizzo MAC insieme a una mappa degli accessi alla VLAN. Le mappe VLAN possono controllare l'accesso di tutto il traffico di una VLAN. Sullo switch è possibile applicare le mappe VLAN a tutti i pacchetti in entrata o in uscita da una VLAN o che sono collegati tramite bridge all'interno di una VLAN. A differenza degli ACL del router, le mappe VLAN non sono definite in direzione (input o output).

In questo scenario di esempio, gli obiettivi di configurazione sono i due criteri seguenti:

- Impedire tutto il traffico IPX dall'host 000.0c00.0111 all'host 000.0c00.0211, ma autorizzare tutto il resto del traffico IPX e del protocollo non IP attraverso la VLAN 20.
- Negare tutto il traffico AppleTalk per la VLAN 10.

Nota: i pacchetti IP non possono essere filtrati tramite un ACL MAC.

Nota: gli ACL estesi con nome MAC non possono essere applicati alle interfacce L3.

1. Definire gli ACL MAC estesi per definire il traffico interessante per le mappe 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. Utilizzare il comando **show access-list** *access-list-name* per verificare l'ACL MAC esteso

configurato. Gli ACL dell'esempio precedente sono `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. Definire l'azione con le mappe di accesso 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. Utilizzare il comando **show vlan access-map *name*** per verificare le mappe di accesso VLAN definite.

```
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. Utilizzare il comando **vlan filter *name* vlan-list** vlan-list per mappare la mappa VLAN alle VLAN. Nell'esempio, si desidera filtrare il protocollo IPX tra host specifici della VLAN 20 e negare l'accesso AppleTalk sulla VLAN 10.

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

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

6. Per verificare che i filtri VLAN siano presenti, usare il comando **show vlan filter vlan *vlan-id***.

```
Switch# show vlan filter vlan 20

Vlan 20 has filter denyIPX.

Switch# show vlan filter vlan 10

Vlan 10 has filter denyapple.
```

Altre caratteristiche non supportate

Supervisor III/IV non supporta le seguenti funzionalità:

- Bridging di fallback o bridging tra VLAN per il bridging di protocolli non indirizzabili
- Routing DECnet

Per un esempio di come utilizzare un router esterno per ottenere questa funzionalità, consultare la sezione precedente.

CPU elevata dopo l'abilitazione del routing IPX o AppleTalk

Dopo aver abilitato il routing IPX o AppleTalk, l'utilizzo della CPU aumenterà in base alla quantità di traffico IPX o AppleTalk instradato nel software tramite lo switch. Se si usa il comando **show processor cpu**, l'output potrebbe indicare che il processo `Cat4k Mgmt LoPri` sta usando la CPU. Ciò indica che i pacchetti sono in fase di commutazione di contesto.

```
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: se il routing IPX o AppleTalk non è abilitato, ma si continua a vedere `Cat4k Mgmt LoPri` con CPU alta, potrebbe essere necessario risolvere i problemi relativi ai pacchetti inviati alla CPU per l'elaborazione. Per ulteriore assistenza, contattare il supporto tecnico Cisco.

Informazioni correlate

- Configurazione della sicurezza di rete con gli ACL
- Pagine di supporto per Catalyst 4500
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems