Unterstützung älterer Protokolle mit Catalyst 4000 Supervisor III/IV

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ältere Protokolle wie IPX, AppleTalk und Data-Link Switching (DLSw) am besten von einem Catalyst 4000/4500-Switch unterstützt werden, der mit dem neueren Supervisor III/IV ausgestattet ist. Dieser Supervisor ist für Hardware-Switch-IP-Pakete der Version 4 (IPv4) konzipiert.

Voraussetzungen

Anforderungen

Leser dieses Dokuments sollten wissen, wie IPX, AppleTalk und DLSw konfiguriert werden. Informationen zu diesen Protokollen finden Sie auf den folgenden Support-Seiten:

- Support-Seite für IPX-Technologie
- Support-Seite für AppleTalk-Technologie
- Support-Seite für DLSw-Technologie

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst 4507R mit Supervisor IV
- Cisco IOS® Softwareversion 12.1(13)EW

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

IPX-Routing

Routing IPX wird von der Cisco IOS Software Version 12.1(12c)EW und höher unterstützt. In der ersten Version liegt die Leistung im Bereich von 20 bis 30 Kpps. Ab der Cisco IOS Software-Version 12.1(13)EW wurde sie auf 80 bis 90 Kpps erhöht. Es wird empfohlen, die Cisco IOS Softwareversion 12.1(19)EW oder höher zu verwenden, da eine Software-Fehlerbehebung für die Cisco Bug-ID CSCea85204 verfügbar ist (nur registrierte Kunden). Diese Weiterleitungsrate wird von allen Datenflüssen gemeinsam genutzt, die den Switch durchlaufen. Diese Weiterleitung erhöht die CPU-Last aufgrund der Softwareverarbeitung. Die erzielte Weiterleitungsrate hängt daher von der Switch-CPU ab. Beispiel: Anzahl der Border Gateway Protocol (BGP)-Richtlinien, EIGRP-Routen (Enhanced Interior Gateway Routing Protocol) oder OSPF-Routen (Open Shortest Path First) und SVIs (Switched Virtual Interfaces), über die der Switch verfügt.

Hinweis: IPv4-Pakete werden weiterhin in der Hardware geroutet, obwohl IPX-Pakete per Software weitergeleitet werden.

Unterstützte Funktionen

- MAC Access Control List (ACL) für IPX wird von der Cisco IOS Software Version 12.1(12c)EW und höher unterstützt, die zur Steuerung der IPX-Pakete verwendet werden kann.
- IPX Routing Information Protocol (RIP) (Service Advertising Protocol [SAP])
- IPX Enhanced Interior Gateway Routing Protocol (EIGRP)
- Header-Komprimierung

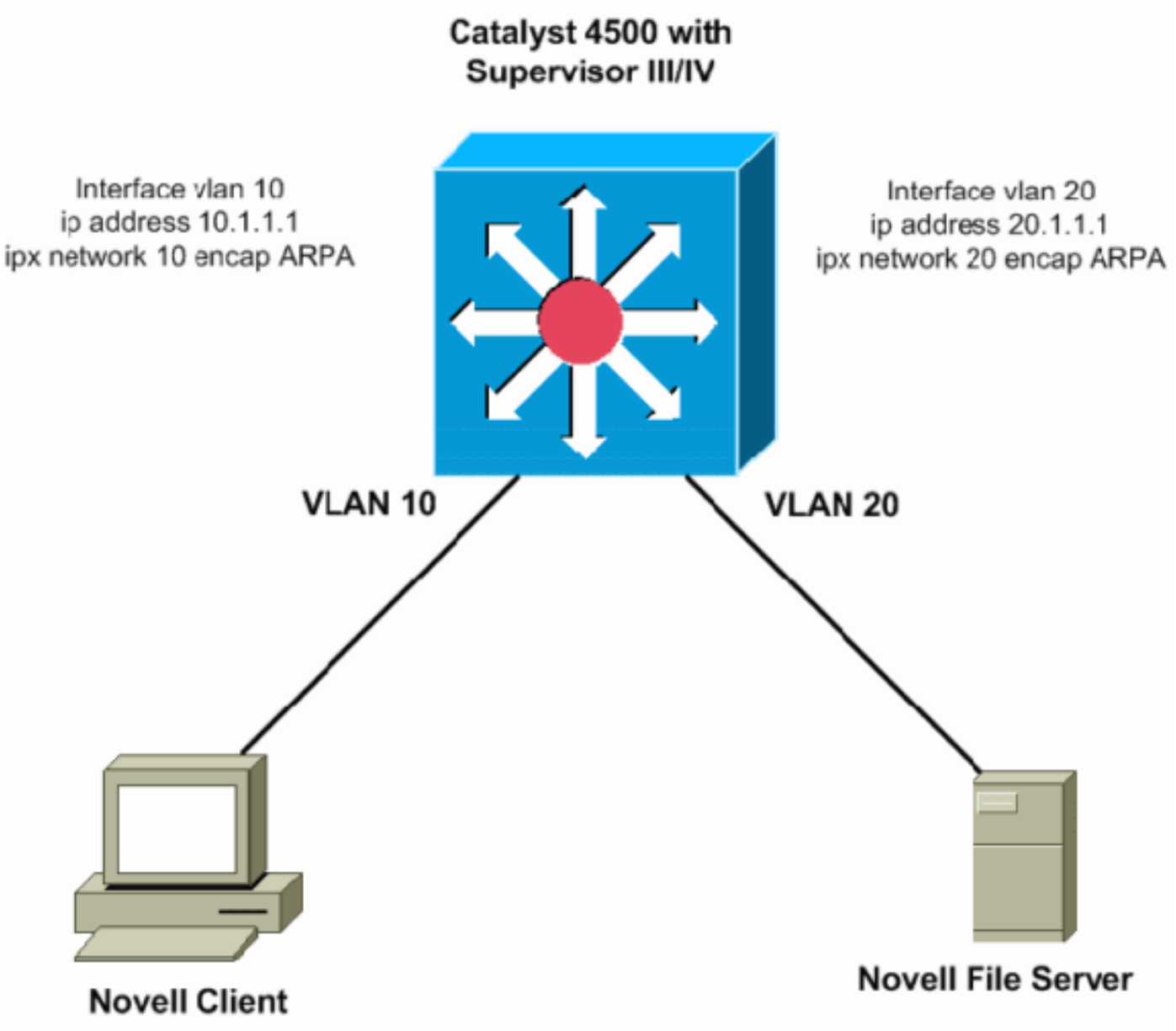
Hinweis: Für eine bessere Leistung ist IPX EIGRP das bevorzugte Routing-Protokoll zwischen Routern, da EIGRP inkrementelle SAP-Updates ausführt. IPX EIGRP kann in serverlosen Segmenten aktiviert werden. Weitere Informationen zu IPX EIGRP finden Sie unter IPX-EIGRP.

Einschränkungen

- Das IPX-Routing von Paketen wird nicht hardwareunterstützt. Dies erfolgt über die Softwareverarbeitung.

- Die Zugriffslisten für Novell IPX-Standard (800-899), IPX Extended (900-999), Get Nearest Server (GNS) oder SAP-Filter (1000-1099) werden derzeit nicht unterstützt.
- Für IPX-Software-Routing werden diese nicht unterstützt:Next Hop Resolution Protocol (NHRP)Netware Link Service Protocol (NLSP)Jumbo-Frames

Diese Abbildung zeigt ein typisches Szenario für Catalyst 4000/4500 mit Supervisor III/IV-Routing IPX. In diesem Szenario befinden sich die Clients im VLAN 10 und die Server im VLAN 20. IPX wird auf VLAN 10- und 20-Schnittstellen konfiguriert, wie in diesem Diagramm gezeigt:



Weiterleiten von AppleTalk

Routing AppleTalk wird von der Cisco IOS Software Version 12.1(12c)EW und höher unterstützt. In der ersten Version liegt die Leistung im Bereich von 20 bis 30 Kpps. Ab der Cisco IOS Software-Version 12.1(13)EW wurde sie auf 80 bis 90 Kpps erhöht. Es wird empfohlen, die Cisco IOS Softwareversion 12.1(19)EW oder höher zu verwenden, da eine Software-Fehlerbehebung für die Cisco Bug-ID CSCea85204 verfügbar ist (nur registrierte Kunden). Diese Weiterleitungsrate wird von allen Datenflüssen gemeinsam genutzt, die den Switch durchlaufen. Diese Weiterleitung erhöht die CPU-Last aufgrund der Softwareverarbeitung. Daher hängt die erzielte Weiterleitungsrate von der Switch-CPU ab: z. B. die Anzahl der BGP-Richtlinien, EIGRP- oder OSPF-Routen und SVIs, über die der Switch verfügt.

Hinweis: IPv4-Pakete werden weiterhin in der Hardware weitergeleitet, obwohl AppleTalk-Pakete per Software weitergeleitet werden.

Unterstützte Funktionen

- MAC ACL für AppleTalk wird in der Cisco IOS Software Version 12.1(12c)EW und höher unterstützt, die zur Steuerung der IPX-Pakete verwendet werden kann.
- DDP-Routing (Datagram Delivery Protocol)
- Routing Table Maintenance Protocol (RTMP)
- Name Binding Protocol (NBP)
- AppleTalk Echo Protocol (AEP)
- AppleTalk EIGRP

Hinweis: AppleTalk EIGRP ist das bevorzugte Routing-Protokoll zwischen Routern für eine bessere Leistung, da EIGRP inkrementelle Updates ausführt. Weitere Informationen zu AppleTalk EIGRP finden Sie im Abschnitt Konfigurieren von AppleTalk Enhanced IGRP unter Konfigurieren von AppleTalk.

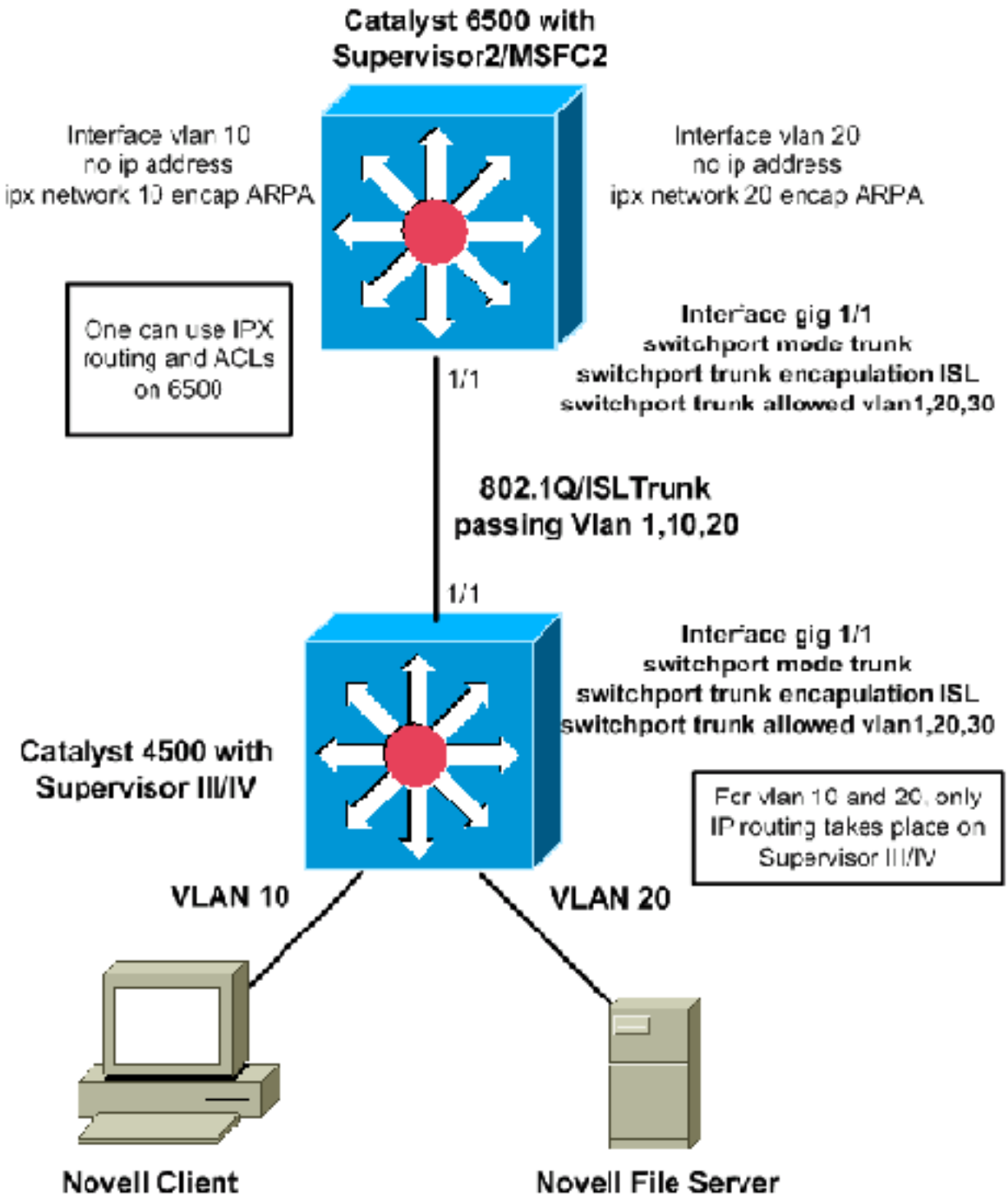
Einschränkungen

- Das AppleTalk-Routing von Paketen ist nicht hardwaregestützt. Dies erfolgt über die Softwareverarbeitung.
- AppleTalk-ACLs werden derzeit nicht unterstützt.
- Für AppleTalk-Software-Routing werden diese nicht unterstützt:AppleTalk Update-Based Routing Protocol (AURP)AppleTalk-Steuerungsprotokoll für PPPJumbo-Frames

Routing über einen externen Router

Wenn für Ihr Netzwerk eine höhere Routing-Leistung der zuvor erwähnten Legacy-Protokolle erforderlich ist, können Sie einen externen Router (Layer 3 [L3]-Gerät) verwenden. Bei einem solchen L3-Gerät kann es sich um eine Catalyst 6000 Multilayer Switch Feature Card (MSFC), einen Catalyst 5000 RSM, einen L3-Switch (z. B. einen 2948G-L3) oder einen beliebigen Router handeln. Diese Geräte führen das Routing von IPX mit Hardware-Unterstützung durch, und die Leistung ist viel größer als die von Supervisor III/IV. Der Supervisor III/IV kann die IP im Hardware-Switching-Pfad weiterleiten, das externe Gerät leitet jedoch die Legacy-Protokolle weiter.

Das nächste Diagramm zeigt ein Szenario, in dem IPX auf dem Kern/Distribution Catalyst 6500 auf der MSFC geroutet wird, während IP auf dem Catalyst 4500 mit Supervisor III/IV zwischen VLAN 10 und VLAN 20 geroutet wird. Die beiden Switches sind gebündelt, wodurch die erforderlichen VLANs möglich sind. Der Vorteil dieses Designs besteht in der Möglichkeit, Standard-IPX-ACLs zu verwenden und die Leistungssteigerung durch hardwareunterstützte Weiterleitung dieser Pakete zwischen den beiden VLANs. Sie können auch IPX-Routing-Protokolle auf dem Catalyst 6500 oder dem externen Router verwenden, um mit Peers für den Austausch von Routing-Datenbanken zu kommunizieren:



Zusätzliche Leistungsverbesserungen

In diesem Abschnitt werden einige weitere potenzielle Leistungsverbesserungen vorgestellt, die an IPX oder AppleTalk-Switching auf dem externen Router vorgenommen werden können.

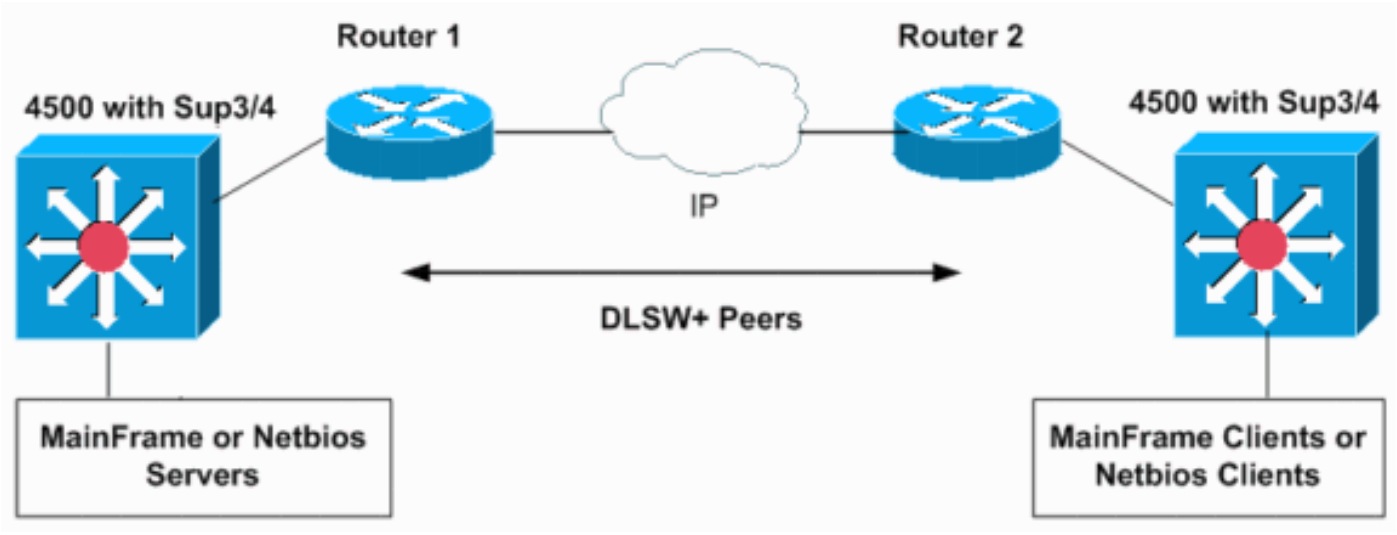
- Die Verbindung zwischen dem externen Router und dem Catalyst-Switch kann zu einer Port-Channel-Verbindung hergestellt werden, um eine höhere Bandbreite zwischen den Routern zu erhalten und Redundanz für die Verbindung zu gewährleisten.
- IP-Datenverkehr kann aus der Verbindung herausgefiltert werden, sodass die gesamte Bandbreite für Nicht-IP-Datenverkehr verwendet wird. Dies ist eine Beispielkonfiguration, um IP-Datenverkehr durch Quality of Service (QoS) zu filtern:

1. Geben Sie den globalen QoS-Konfigurationsbefehl **QoS** ein, um QoS auf dem Supervisor zu aktivieren.
2. Definieren Sie die ACL so, dass sie dem gesamten IP-Datenverkehr entspricht.
   ```
   access-list 101 permit ip any any
   ```
3. Definieren Sie die Klassenzuordnung, die mit der in Schritt 2 definierten ACL übereinstimmt.
   ```
   class-map match-any ip-drops
     match access-group 101
   ```
4. Policy definieren: Definieren Sie eine Richtlinie, die den gesamten Datenverkehr für die in Schritt 3 definierte Klasse verwirft. Die Überwachung des gesamten Datenverkehrs erfolgt mit einer Mindestgranularität von 32 Kbit/s. Der Supervisor verwirft den gesamten IP-Datenverkehr mit dieser Richtlinie über 32 Kbit/s (Cisco IOS IP-Pings können möglicherweise nicht durchgestellt werden).
   ```
   policy-map drop-ip
     class ip-drops
       police 32000 bps 1000 byte conform-action drop exceed-action drop
   ```
5. Wenden Sie die Service-Richtlinie ausgehend an die Schnittstelle an, die mit dem externen Router verbunden ist.
   ```
   interface GigabitEthernet 1/1
       service-policy output drop-ip
   ```

Führen Sie zum Überprüfen der Richtlinienaktion den **Befehl show policy-map interface *interface-id* aus.**

DLSw

DLSw wird von der Supervisor III/IV nicht unterstützt. Bei Netzwerken mit SNA- und IP-Protokollen können Sie den IP-Datenverkehr über den Catalyst 4000 Supervisor III/IV routen und den SNA-Datenverkehr mit DLSw-Switching über die Cisco IOS-Software auf einem externen Router überbrücken:



Die nächsten Konfigurationen zeigen, wie SNA-Datenverkehr in den VLANs 10 und 20 auf zwei Catalyst 6500 MSFC2-Routern in zwei separaten SNA-Domänen überbrückt wird. Die 802.1Q-Trunks auf dem Supervisor III/IV können verwendet werden, um (Bridge) SNA- oder NetBIOS-Datenverkehr an einen Cisco Router oder an Catalyst 6500-Switches zu übertragen.

`hostname MSFCRouter-1`
`interface loopback1`
`ip address 1.1.1.1`
	`hostname MSFCRouter-2`
	`interface loopback1`
	`ip address 2.2.2.2`

! 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	! 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

Dies zeigt Netzwerkkonfigurationen für Catalyst 6500-Switches in verschiedenen Domänen. Wenn sich die VLANs 10 und 20 auf demselben Switch oder MSFC befinden, ist kein DLSw erforderlich. Einfache IEEE Bridge-Gruppen auf einer MSFC funktionieren.

Filtern von Nicht-IP-Paketen mit erweiterten MAC-ACLs und VLAN-Zuordnungen

Supervisor III/IV unterstützt keine IPX-, AppleTalk- oder andere Legacy-Protokoll-ACLs. Um diese zu filtern, können Sie eine MAC-erweiterte ACL in Kombination mit einer VLAN-Zugriffskarte verwenden. VLAN-Maps können den Zugriff auf den gesamten Datenverkehr in einem VLAN steuern. Sie können VLAN-Maps auf den Switch auf alle Pakete anwenden, die in ein oder aus einem VLAN geroutet oder innerhalb eines VLAN überbrückt werden. Im Gegensatz zu Router-ACLs werden VLAN-Karten nicht nach Richtung (Eingabe oder Ausgabe) definiert.

In diesem Beispielszenario sind die folgenden beiden Kriterien die Konfigurationsziele:

- Verhindern Sie den gesamten IPX-Datenverkehr vom Host 000.0c00.011 zum Hosten von 000.0c00.0211, lassen Sie jedoch alle anderen IPX- und Nicht-IP-Protokolldatenverkehr über VLAN 20 zu.
- Verweigern Sie den gesamten AppleTalk-Datenverkehr für VLAN 10.

Hinweis: IP-Pakete können nicht über eine MAC-ACL gefiltert werden.

Hinweis: Named MAC Extended ACLs können nicht auf L3-Schnittstellen angewendet werden.

1. Definieren Sie erweiterte MAC-ACLs, um den interessanten Datenverkehr für die VLAN-Zuordnungen zu definieren.

```
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. Geben Sie den **Befehl show access-list *access-list-name* ein, um die konfigurierte erweiterte MAC-ACL zu überprüfen.** Die ACLs im vorherigen Beispiel sind `denyIPXACL` und `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. Definieren Sie die Aktion mithilfe der VLAN-Zugriffzuordnungen.

```
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. Geben Sie den Befehl **show vlan access-map *name* ein, um die definierten VLAN-Zugriffzuordnungen zu überprüfen.**

```
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. Geben Sie den Befehl **vlan filter *name* vlan-list *vlan-list* ein, um die VLAN-Zuordnung den VLANs zuzuordnen.** In diesem Beispiel möchten Sie IPX zwischen bestimmten Hosts in VLAN 20 filtern und AppleTalk in VLAN 10 ablehnen.

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

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

6. Geben Sie den Befehl **show vlan filter vlan *vlan-id* ein, um** zu überprüfen, ob die VLAN-Filter

vorhanden sind.

```
Switch# show vlan filter vlan 20

Vlan 20 has filter denyIPX.

Switch# show vlan filter vlan 10

Vlan 10 has filter denyapple.
```

Weitere nicht unterstützte Funktionen

Supervisor III/IV unterstützt folgende Funktionen nicht:

- Fallback-Bridging oder Inter-VLAN-Bridging zur Überbrückung nicht routingfähiger Protokolle
- DECnet-Routing

Im vorherigen Abschnitt finden Sie ein Beispiel für die Verwendung eines externen Routers, um diese Funktionalität zu erreichen.

Hohe CPU nach Aktivierung von IPX oder AppleTalk-Routing

Nachdem Sie IPX oder AppleTalk-Routing aktiviert haben, erhöht sich die CPU-Auslastung basierend auf der Menge an IPX- oder AppleTalk-Datenverkehr, der in der Software über den Switch geleitet wird. Wenn Sie den Befehl **show processor cpu** (Prozessor-CPU **anzeigen**) eingeben, kann die Ausgabe zeigen, dass der `Cat4k Mgmt LoPri`-Prozess die CPU verwendet. Dies weist darauf hin, dass die Pakete vertauscht werden.

```
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
```

Hinweis: Wenn Sie IPX oder AppleTalk-Routing nicht aktiviert haben, jedoch `Cat4k Mgmt LoPri` mit hoher CPU immer noch sehen, müssen Sie möglicherweise eine Fehlerbehebung durchführen, welche Pakete zur Verarbeitung an die CPU gesendet werden. Wenden Sie sich an den technischen Support von Cisco, wenn Sie weitere Unterstützung benötigen.

Zugehörige Informationen

- Konfigurieren der Netzwerksicherheit mit ACLs
- Support-Seiten für Catalyst 4500
- Support-Seiten für LAN-Produkte
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems