通过 Catalyst 4000 Supervisor III/IV 支持早期协议

目录

简介

本文档介绍在配备了较新的Supervisor III/IV的Catalyst 4000/4500交换机中如何最好地支持IPX、AppleTalk和数据链路交换(DLSw)等传统协议。此Supervisor专为硬件交换机IP版本4(IPv4)数据包而设计。

先决条件

要求

本文档的读者应了解如何配置IPX、AppleTalk和DLSw。有关这些协议的信息，请参阅以下支持页：

- IPX技术支持页
- AppleTalk技术支持页
- DLSw技术支持页

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带管理引擎IV的Catalyst 4507R
- 思科IOS®软件版本12.1(13)EW

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

路由 IPX

Cisco IOS软件版本12.1(12c)EW及更高版本支持路由IPX。在初始版本中，性能在20至30 kpps之间；自Cisco IOS软件版本12.1(13)EW起，已增加到80至90 kpps。建议您使用Cisco IOS软件版本12.1(19)EW或更高版本，因为Cisco Bug ID CSCea85204(仅限注册客户)的软件修复程序可用。 此转发速率由流经交换机的所有流共享。此转发会增加由软件处理引起的CPU负载。因此，实现的转发速率取决于交换机CPU;例如，交换机有多少边界网关协议(BGP)策略、增强型内部网关路由协议(EIGRP)或开放最短路径优先(OSPF)路由和交换虚拟接口(SVI)。

注意：即使IPX数据包是软件路由的，IPv4数据包仍在硬件中路由。

支持的功能

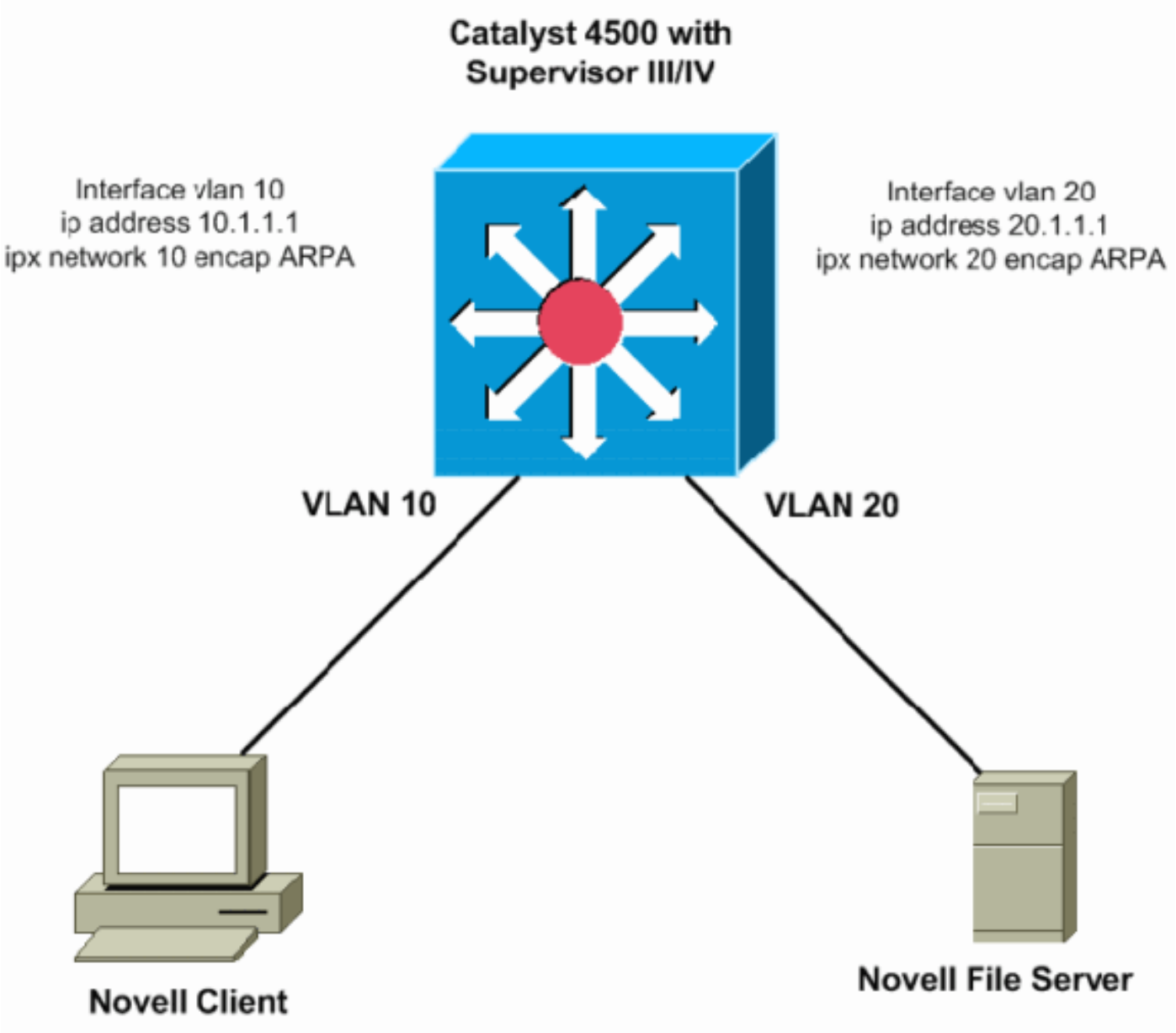
- Cisco IOS软件版本12.1(12c)EW及更高版本支持IPX的MAC访问控制列表(ACL)，该版本可用于控制IPX数据包。
- IPX路由信息协议(RIP)（服务通告协议[SAP]）
- IPX增强型内部网关路由协议(EIGRP)
- 报头压缩

注意：IPX EIGRP是路由器之间的首选路由协议，因为EIGRP执行增量SAP更新。IPX EIGRP可在无服务器网段上启用。有关IPX EIGRP的信息，请参阅了解IPX-EIGRP。

限制

- 数据包的IPX路由不由硬件支持。通过软件处理完成。
- 目前不支持Novell IPX标准(800-899)、IPX扩展(900-999)、获取最近服务器(GNS)或SAP过滤器(1000-1099)访问列表。
- 对于IPX软件路由，不支持以下内容：下一跳解析协议 (NHRP)Netware链路服务协议(NLSP)巨型帧

此图说明了Catalyst 4000/4500与Supervisor III/IV路由IPX的典型场景。在此场景中，客户端位于VLAN 10中，服务器位于VLAN 20中。IPX配置在VLAN 10和20接口上，如下图所示：



路由 AppleTalk

Cisco IOS软件版本12.1(12c)EW及更高版本支持路由AppleTalk。在初始版本中，性能在20至30 kpps之间；自Cisco IOS软件版本12.1(13)EW起，已增加到80至90 kpps。建议您使用Cisco IOS软件版本12.1(19)EW或更高版本，因为Cisco Bug ID CSCea85204(仅限注册客户)的软件修复程序可用。 此转发速率由流经交换机的所有流共享。此转发会增加由软件处理引起的CPU负载。因此，实现的转发速率取决于交换机CPU:例如，交换机有多少个BGP策略、EIGRP或OSPF路由和SVI。

注意：IPv4数据包在硬件中继续路由，即使AppleTalk数据包是软件路由的。

支持的功能

- Cisco IOS软件版本12.1(12c)EW及更高版本支持用于AppleTalk的MAC ACL，该版本可用于控制IPX数据包。
- 数据报传输协议(DDP)路由
- 路由表维护协议 (RTMP)
- 名称绑定协议(NBP)
- AppleTalk回声协议(AEP)

- AppleTalk EIGRP

注意：AppleTalk EIGRP是路由器之间首选的路由协议，因为EIGRP执行增量更新，所以可以获得更好的性能。有关AppleTalk EIGRP的详细信息，请参阅配置AppleTalk的配置AppleTalk增强版IGRP部分。

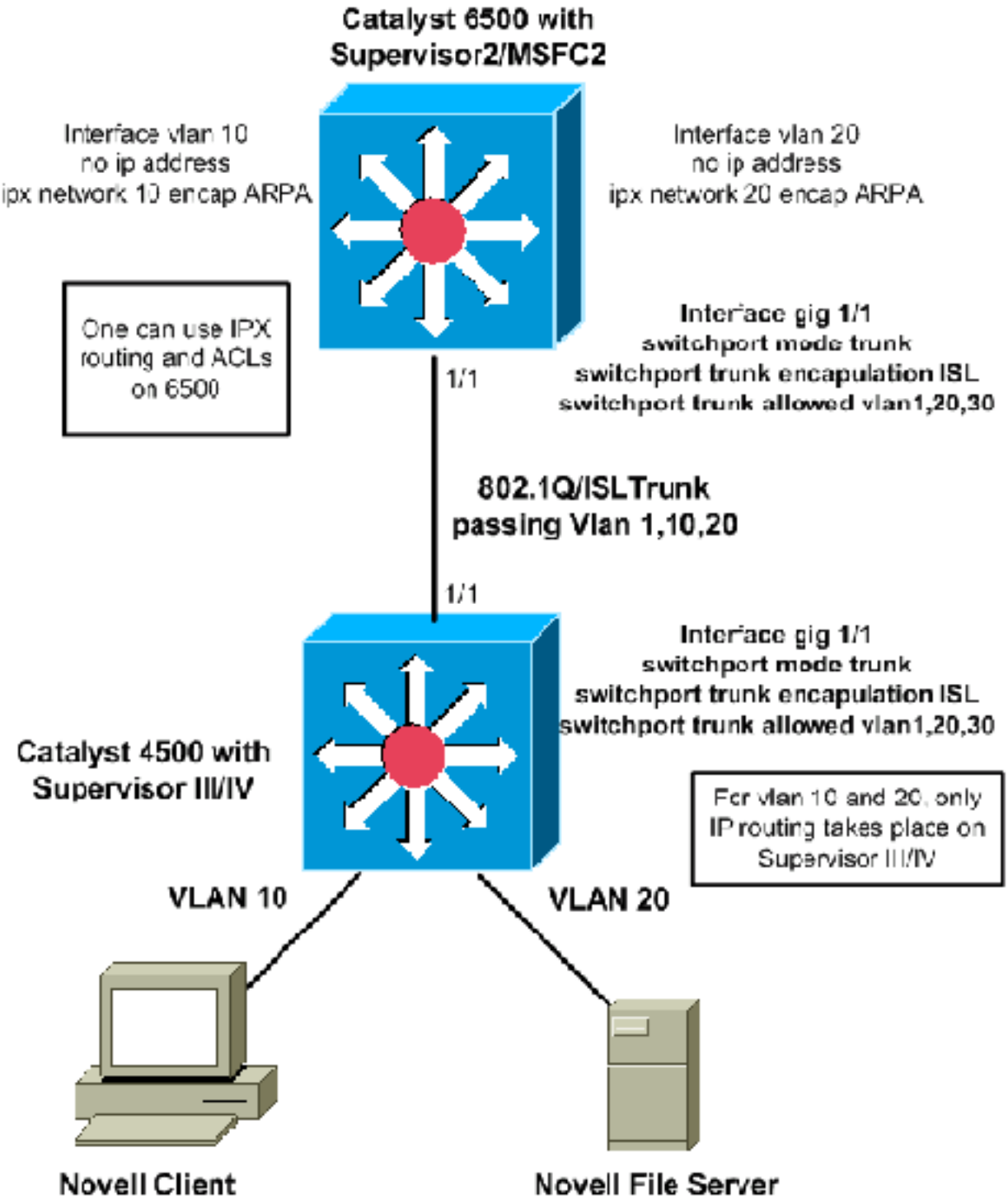
限制

- 数据包的AppleTalk路由不由硬件支持。通过软件处理完成。
- 当前不支持AppleTalk ACL。
- 对于AppleTalk软件路由，不支持以下内容：基于AppleTalk更新的路由协议(AURP)PPP的AppleTalk控制协议巨型帧

通过外部路由器进行路由

如果网络需要较好的传统协议路由性能，则您可能希望使用外部路由器（第3层[L3]设备）。 此类L3设备可以是Catalyst 6000多层交换功能卡(MSFC)、Catalyst 5000 RSM、L3交换机（如2948G-L3）或任何路由器。这些设备在硬件协助下执行IPX路由，其性能比Supervisor III/IV高得多。Supervisor III/IV可以在硬件交换路径中路由IP，但外部设备路由传统协议。

下图说明了在MSFC的核心/分布层Catalyst 6500上路由IPX，而在带Supervisor III/IV的Catalyst 4500上在VLAN 10和VLAN 20之间路由IPX的场景。两台交换机是中继的，这允许所需的VLAN。这种设计的好处是能够使用标准IPX ACL，并且由于硬件辅助在两个VLAN之间转发这些数据包而提高了性能。您还可以在Catalyst 6500或外部路由器上使用IPX路由协议与对等体通信以进行路由数据库交换：



其它性能改进

本部分提供一些可对外部路由器上的IPX或AppleTalk交换进行的其他潜在性能改进。

- 外部路由器和Catalyst交换机之间的链路可以建立为端口通道链路，以获得更高的带宽，并为链路提供冗余。
- IP流量可以从链路中过滤出来，以便所有带宽都用于非IP流量。以下是通过服务质量(QoS)过滤IP流量的示例配置：

1. 发出QoS全局配置命令**qos**，以在管理引擎上启用QoS。
2. 定义ACL以匹配所有IP流量。
   ```
   access-list 101 permit ip any any
   ```
3. 定义与步骤2中定义的ACL匹配的类映射。

```
class-map match-any ip-drops
  match access-group 101
```

4. 定义策略：定义一个监察器，该监察器将丢弃步骤3中定义的类的所有流量。使用最小粒度32 kbps对所有流量进行管制。管理引擎将丢弃此监察器超过32 kbps的所有IP流量（Cisco IOS IPping可能无法通过）。

```
policy-map drop-ip
  class ip-drops
    police 32000 bps 1000 byte conform-action drop exceed-action drop
```

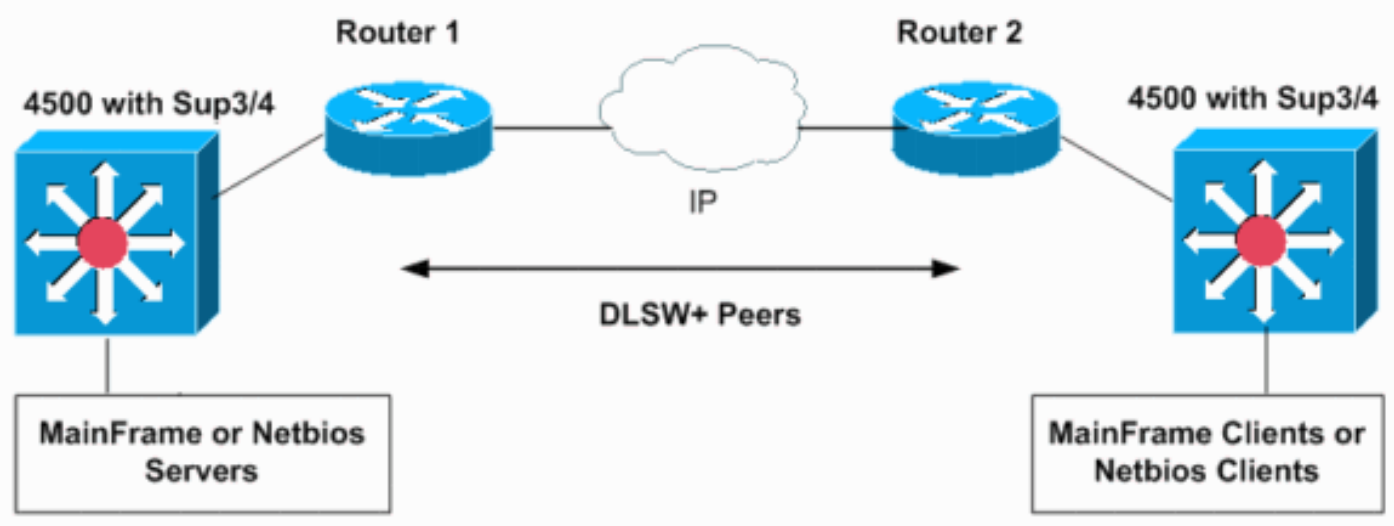
5. 在连接到外部路由器的接口上应用服务策略出站。

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

要验证策略操作，请发出**show policy-map interface interface-*id*命**令。

DLSw

管理引擎III/IV不支持DLSw。对于使用SNA和IP协议的网络，您可以在Catalyst 4000 Supervisor III/IV上路由IP流量，并在外部路由器的Cisco IOS软件上使用DLSw交换桥接SNA流量：



接下来的配置显示了如何在两个独立SNA域中的两个Catalyst 6500 MSFC2上桥接VLAN 10和20上的SNA流量。Supervisor III/IV上的802.1Q中继可用于将（网桥）SNA或NetBIOS流量传输到Cisco路由器或Catalyst 6500交换机。

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

这显示了不同域中Catalyst 6500交换机的网络配置。如果VLAN 10和20位于同一交换机或MSFC上，则不需要DLSw。一个MSFC上的简单IEEE网桥组将工作。

使用扩展MAC ACL和VLAN映射过滤非IP数据包

Supervisor III/IV不支持IPX、AppleTalk或其他传统协议ACL。要过滤这些流量，可以使用MAC扩展ACL和VLAN访问映射。VLAN映射可以控制VLAN中所有流量的访问。您可以将交换机上的VLAN映射应用于路由到VLAN或路由到VLAN或在VLAN内桥接的所有数据包。与路由器ACL不同，VLAN映射不是按方向（输入或输出）定义的。

在本示例场景中，以下两个标准是配置目标：

- 阻止从主机000.0c00.0111到主机000.0c00.0211的所有IPX流量，但允许通过VLAN 20的所有其他IPX和非IP协议流量。
- 拒绝VLAN 10的所有AppleTalk流量。

注意：IP数据包无法通过MAC ACL过滤。

注意：命名MAC扩展ACL不能应用于L3接口。

1. 定义扩展MAC ACL以定义VLAN映射的相关流量。

```
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. 发出**show access-list access-*list-name*命**令以验证已配置的扩展MAC ACL。上例中的ACL是denyIPXACL和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. 使用VLAN访问映射定义操作。

```
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. 发出**show vlan access-map *name*命**令以验证已定义的VLAN访问映射。

```
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. 发出**vlan filter *name* vlan-list vlan-list *命令将VLAN映射***映射到VLAN。在本例中，您要过滤VLAN 20中特定主机之间的IPX并拒绝VLAN 10上的AppleTalk。

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

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

6. 发出**show vlan filter vlan vlan *vlan-id命***令以验证VLAN过滤器是否就位。

```
Switch# show vlan filter vlan 20

Vlan 20 has filter denyIPX.

Switch# show vlan filter vlan 10

Vlan 10 has filter denyapple.
```

其它不支持的功能

管理引擎III/IV不支持以下功能：

- 回退桥接或VLAN间桥接到桥接不可路由协议
- DECnet 路由

请参阅上一节，查看如何使用外部路由器实现此功能的示例。

启用 IPX 或 AppleTalk 路由后引发的高 CPU 利用率

启用IPX或AppleTalk路由后，CPU使用率将根据在软件中通过交换机路由的IPX或AppleTalk流量量增加。如果发出**show processor cpu**命令，则输出可能显示`Cat4k Mgmt LoPri`使用CPU。这表示数据

包正在进行进程交换。

```
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
```

注意：如果您没有启用IPX或AppleTalk路由，但仍然看到`Cat4k Mgmt LoPri`使用高CPU，则可能必须排除哪些数据包发送到CPU进行处理的故障。如需进一步帮助，请联系思科技术支持。

相关信息

- 用 ACL 配置网络安全
- Catalyst 4500支持页
- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems