Supporting Legacy Protocols with Catalyst 4000 Supervisor III/IV

Contents

Introduction

This document describes how legacy protocols such as IPX, AppleTalk, and Data-Link Switching (DLSw) are best supported in a Catalyst 4000/4500 switch equipped with the newer Supervisor III/IV. This Supervisor is designed to hardware switch IP Version 4 (IPv4) packets.

Prerequisites

Requirements

Readers of this document should have knowledge of how to configure IPX, AppleTalk, and DLSw. For information about these protocols, refer to these support pages:

- IPX Technology Support Page
- AppleTalk Technology Support Page
- DLSw Technology Support Page

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 4507R with Supervisor IV

- Cisco IOS® Software Release 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.

Routing IPX

Routing IPX is supported in Cisco IOS Software Release 12.1(12c)EW and later. In the initial release, the performance is in the range of 20 to 30 kpps; as of Cisco IOS Software Release 12.1(13)EW, it has been increased to 80 to 90 kpps. It is recommended that you use Cisco IOS Software Release 12.1(19)EW or later due to the availability of a software fix for Cisco bug ID CSCea85204 (registered customers only) . This forwarding rate is shared by all flows that follow through the switch. This forwarding increases the CPU load due to software processing. As such, the forwarding rate achieved is dependent on the switch CPU; for example, how many Border Gateway Protocol (BGP) policies, Enhanced Interior Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF) routes, and Switched Virtual Interfaces (SVIs) that the switch has.

Note: IPv4 packets continue to be routed in hardware, even though IPX packets are software-routed.

Supported Features

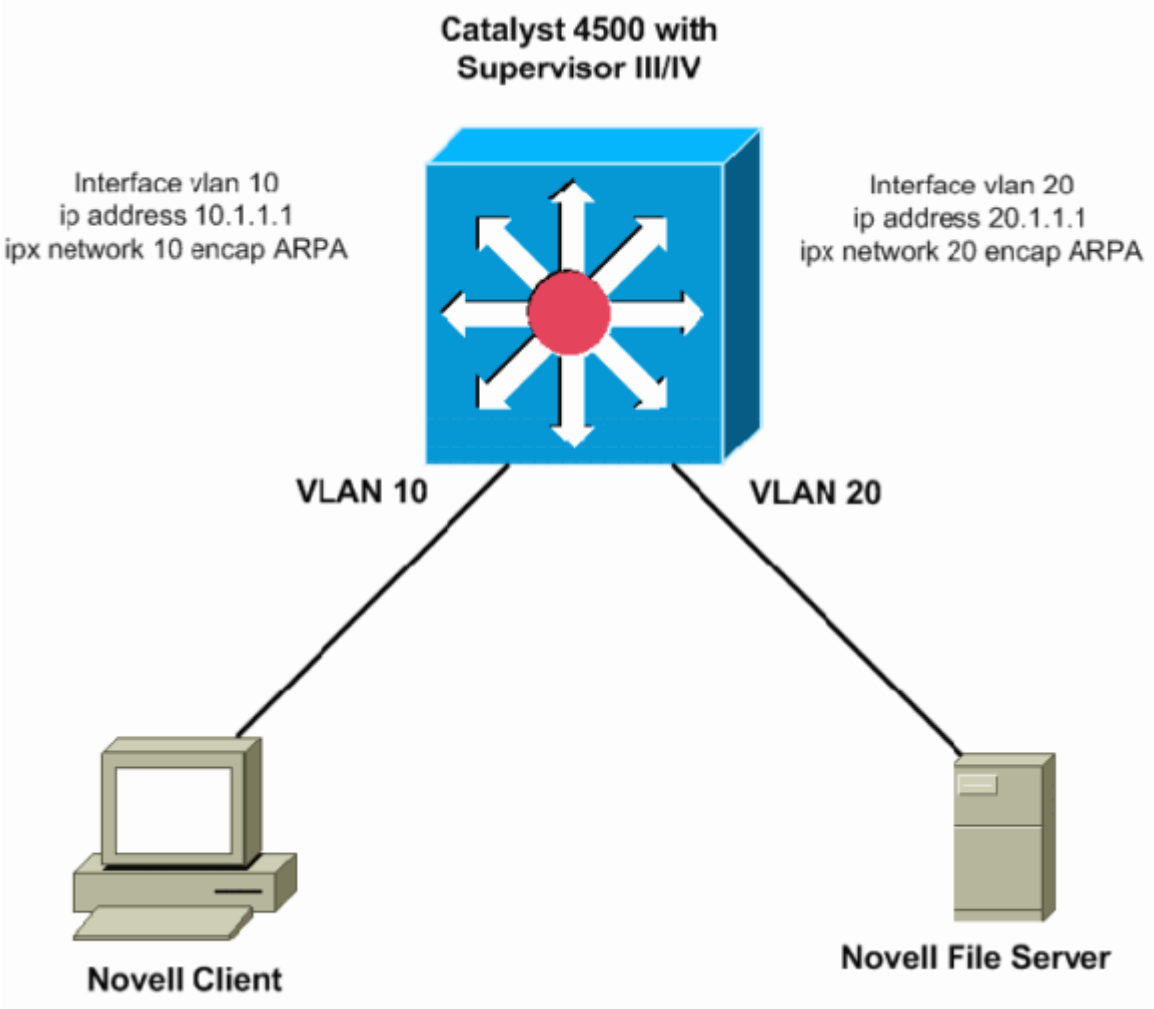
- MAC Access Control List (ACL) for IPX is supported in Cisco IOS Software Release 12.1(12c)EW and later, which can be used to control the IPX packets.
- IPX Routing Information Protocol (RIP) (Service Advertising Protocol [SAP])
- IPX Enhanced Interior Gateway Routing Protocol (EIGRP)
- header compression

Note: IPX EIGRP is the preferred routing protocol between routers for better performance, as EIGRP does incremental SAP updates. IPX EIGRP can be enabled on server-less segments. For information about IPX EIGRP, refer to Understanding IPX-EIGRP.

Limitations

- IPX routing of packets is not hardware-assisted. It is done through software processing.
- Novell IPX standard (800-899), IPX extended (900-999), Get Nearest Server (GNS), or SAP filters (1000-1099) access lists are currently not supported.
- For IPX software routing, these are not supported:
    - Next Hop Resolution Protocol (NHRP)
    - Netware Link Service Protocol (NLSP)
    - jumbo frames

This figure illustrates a typical scenario with the Catalyst 4000/4500 with Supervisor III/IV routing IPX. In this scenario, clients are in VLAN 10 and servers are in VLAN 20. IPX is configured on VLAN 10 and 20 interfaces, as shown in this diagram:



Routing AppleTalk

Routing AppleTalk is supported in Cisco IOS Software Release 12.1(12c)EW and later. In the initial release, the performance is in the range of 20 to 30 kpps; as of Cisco IOS Software Release 12.1(13)EW, it has been increased to 80 to 90 kpps. It is recommended that you use Cisco IOS Software Release 12.1(19)EW or later due to the availability of a software fix for Cisco bug ID CSCea85204 (registered customers only) . This forwarding rate is shared by all flows that follow through the switch. This forwarding increases the CPU load due to software processing. As such, the forwarding rate achieved is dependent on the switch CPU: for example, how many BGP policies, EIGRP or OSPF routes, and SVIs that the switch has.

Note: IPv4 packets continue to be routed in hardware, even though AppleTalk packets are software-routed.

Supported Features

- MAC ACL for AppleTalk is supported in Cisco IOS Software Release 12.1(12c)EW and later, which can be used to control the IPX packets.
- Datagram Delivery Protocol (DDP) routing
- Routing Table Maintenance Protocol (RTMP)
- Name Binding Protocol (NBP)
- AppleTalk Echo Protocol (AEP)
- AppleTalk EIGRP

Note: AppleTalk EIGRP is the preferred routing protocol between routers for better performance, as EIGRP

does incremental updates. For more information about AppleTalk EIGRP, refer to the Configuring AppleTalk Enhanced IGRP section of Configuring AppleTalk.

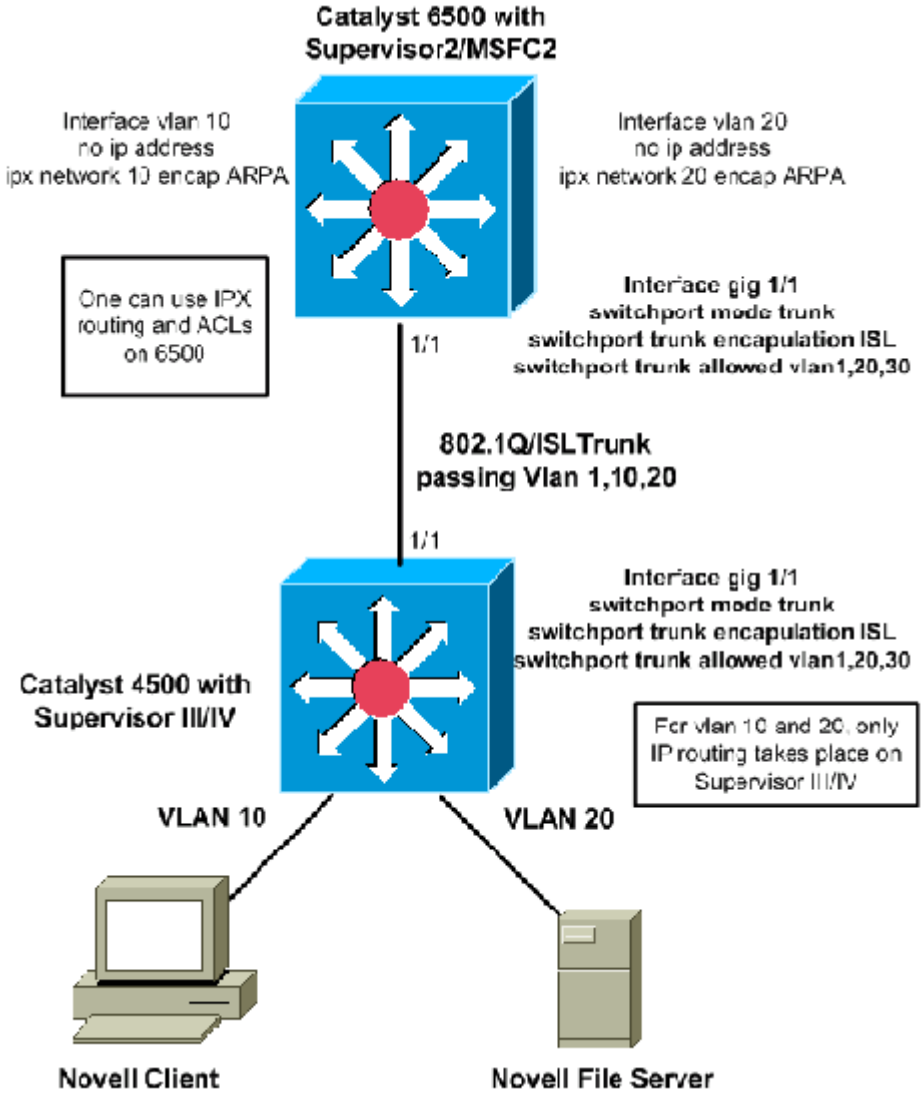
Limitations

- AppleTalk routing of packets is not hardware-assisted. It is done through software processing.
- AppleTalk ACLs are not currently supported.
- For AppleTalk software routing, these are not supported:
    - AppleTalk Update-Based Routing Protocol (AURP)
    - AppleTalk control protocol for PPP
    - jumbo frames

Routing through an External Router

If your network requires better routing performance of the legacy protocols then previously mentioned, you may want to use an external router (Layer 3 [L3] device). Such an L3 device could be a Catalyst 6000 Multilayer Switch Feature Card (MSFC), Catalyst 5000 RSM, L3 switch (such as a 2948G-L3), or any router. These devices performs routing of IPX with hardware assistance, and the performance is much greater than the Supervisor III/IV. The Supervisor III/IV can route IP in the hardware switching path, but the external device routes the legacy protocols.

The next diagram illustrates a scenario in which IPX is routed on the core/distribution Catalyst 6500 on the MSFC while IP is routed between VLAN 10 and VLAN 20 at the Catalyst 4500 with Supervisor III/IV. The two switches are trunked, which allows the required VLANs. The benefit of this type of design is the ability to use standard IPX ACLs and the performance increase due to hardware-assisted forwarding of these packets between the two VLANs. You can also use IPX routing protocols on the Catalyst 6500 or on the external router, to communicate with the peers for routing database exchange:



Additional Performance Improvements

This sections provides some additional potential performance improvements that can be made to IPX or to AppleTalk switching on the external router.

- The link between the external router and the Catalyst switch could be made into a port-channel link, to get higher bandwidth between them and to have redundancy for the link.
- IP traffic can be filtered out of the link so that all of the bandwidth is used for non-IP traffic. This is a sample configuration to filter out IP traffic through Quality of Service (QoS):

1. Issue the QoS global configuration command **qos**, to enable QoS on the Supervisor.
2. Define the ACL to match all IP traffic.

```
access-list 101 permit ip any any
```

3. Define the class-map that matches the ACL defined in Step 2.

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

4. Define the policy: define a policer that will drop all traffic for the class defined in Step 3. Police all the traffic using a minimum granularity of 32 kbps. The Supervisor will drop all the IP traffic with this policer beyond 32 kbps (Cisco IOS IP pings may not be able to go through).

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

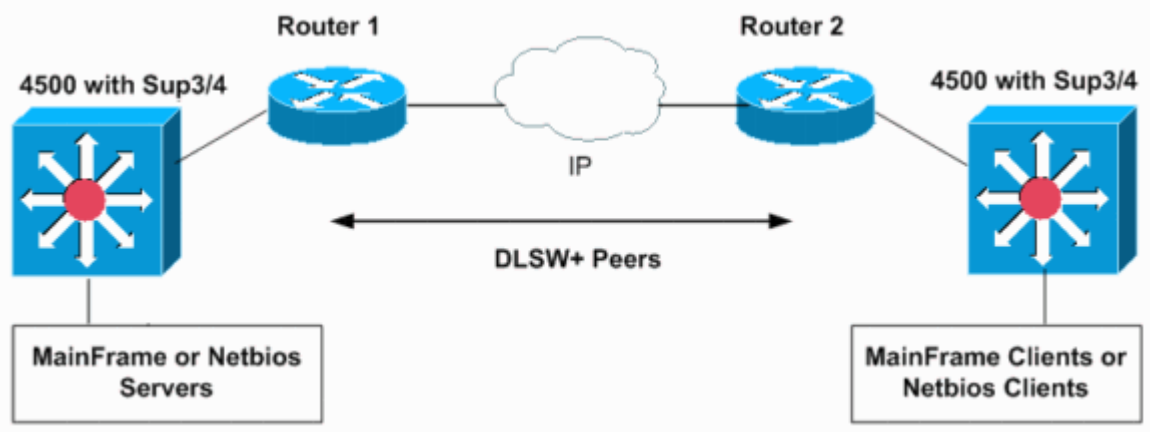
5. Apply the service policy out-bound on the interface that connects to the external router.

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

To verify the policing action, issue the **show policy-map interface *interface-id*** command.

DLSw

DLSw is not supported on the Supervisor III/IV. For networks with SNA and IP protocols, you can route the IP traffic on Catalyst 4000 Supervisor III/IV and bridge the SNA traffic with DLSw switching on Cisco IOS software on an external router:



The next configurations show how to bridge SNA traffic on VLANs 10 and 20 on two Catalyst 6500 MSFC2s in two separate SNA domains. The 802.1Q trunks on the Supervisor III/IV may be used to carry (bridge) SNA or NetBIOS traffic to a Cisco router or to Catalyst 6500 switches.

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

This shows network configurations for Catalyst 6500 switches in different domains. If VLANs 10 and 20 are on the same switch or MSFC, DLSw is not required. Simple IEEE bridge groups on one MSFC will work.

Filtering Non-IP Packets with Extended MAC ACLs and VLAN Maps

Supervisor III/IV does not support IPX, AppleTalk, or other legacy protocol ACLs. To filter them, you can use a MAC-extended ACL combined with a VLAN access map. VLAN maps can control the access of all traffic in a VLAN. You can apply VLAN maps on the switch to all packets that are routed into or out of a VLAN or are bridged within a VLAN. Unlike router ACLs, VLAN maps are not defined by direction (input or output).

In this example scenario, these two criteria are the configuration goals:

- Prevent all IPX traffic from host 000.0c00.0111 to host 000.0c00.0211, but permit all other IPX and non-IP protocol traffic through VLAN 20.
- Deny all AppleTalk traffic for VLAN 10.

Note: IP packets can not be filtered through a MAC ACL.

Note: Named MAC extended ACLs can not be applied to L3 interfaces.

1. Define extended MAC ACLs to define the interesting traffic for the VLAN maps.

```
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. Issue the **show access-list** ***access-list-name*** command to verify the configured extended MAC ACL. The ACLs in the previous example are `denyIPXACL` and `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. Define the action with the VLAN access maps.

```
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. Issue the **show vlan access-map** ***name*** command to verify the defined the VLAN access maps.

```
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. Issue the **vlan filter *name* vlan-list *vlan-list*** command to map the VLAN map to the VLANs. In this example, you want to filter IPX between specific hosts in VLAN 20 and deny AppleTalk on VLAN 10.

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

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

6. Issue the **show vlan filter vlan *vlan-id*** command to verify that the VLAN filters are in place.

```
Switch# show vlan filter vlan 20

Vlan 20 has filter denyIPX.

Switch# show vlan filter vlan 10

Vlan 10 has filter denyapple.
```

Other Unsupported Features

Supervisor III/IV does not support these features:

- Fallback bridging or inter-VLAN bridging to bridge non-routable protocols
- DECnet routing

Refer to the previous section, to see an example of how to use an external router to achieve this functionality.

High CPU After Enabling IPX or AppleTalk Routing

After you enable IPX or AppleTalk routing, the CPU usage will increase based on the amount of IPX or AppleTalk traffic that is being routed in software through the switch. If you issue the **show processor cpu** command, the output may show that the `Cat4k Mgmt LoPri` process is using the CPU. This indicates that the packets are being process switched.

```
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
```

Note: If you do not have IPX or AppleTalk routing enabled, but still see `Cat4k Mgmt LoPri` using high CPU, then you may have to troubleshoot which packets are sent to the CPU for processing. Contact Cisco Technical Support, if you need further assistance.

NetPro Discussion Forums - Featured Conversations

Related Information

- **Configuring Network Security with ACLs**
- **Catalyst 4500 Support Pages**
- **LAN Product Support Pages**
- **LAN Switching Support Page**
- **Technical Support & Documentation - Cisco Systems**
