

## Chapter 22

# Overview of Layer 3

Introduction .....	22-2
Internet Protocol (IP) .....	22-3
OSPF .....	22-4
Routing Information Protocol (RIP) .....	22-5
IP Multicasting .....	22-6
Configuring IGMP .....	22-7
Configuring Multicast Routing .....	22-7
Novell IPX .....	22-8
AppleTalk .....	22-10

## Introduction

---

The switch routes IP and IP multicasting traffic at wire speed between VLANs, and supports a number of other Layer 3 protocols. Once a VLAN has been created (see [“Virtual Local Area Networks \(VLANs\)” on page 8-14 of Chapter 8, Switching](#)), the VLAN name can be used wherever a logical interface is required in commands for configuring routing protocols.

VLAN names are of the form:

`VLAN-vlannname`

or

`VLANn`

where *vlannname* is the manager-assigned name of the VLAN, and *n* is the VLAN identifier (VID).

For example, to create a VLAN called “admin” with a VID of 11, and add port 3 to it, use the commands:

```
create vlan=admin vid=11
```

```
add vlan=11 port=3
```

The following names can be used to identify this VLAN in routing commands:

`vlan-admin`

`vlan11`

The following sections summarise the use of VLANs for IP, OSPF, RIP, IPX, and AppleTalk. Full details of these protocols, and all other routing protocols supported by the switch, are in individual chapters of this Software Reference.

## Internet Protocol (IP)

The switch performs IP routing at wire speed between VLANs that have been configured as IP interfaces. For example, to add the admin VLAN as an IP interface, giving it an IP address of 192.168.163.39 in the subnet 192.168.163.0, first enable IP using the command:

```
enable ip
```

Then use either of the following commands:

```
add ip interface=vlan-admin ipaddress=192.168.163.39
mask=255.255.255.0
```

```
add ip interface=vlan11 ipaddress=192.168.163.39
mask=255.255.255.0
```

The command:

```
show ip interface
```

displays the interfaces enabled for IP routing ([Figure 22-1](#)).

Figure 22-1: Example output from the **show ip interface** command.

Interface Pri. Filt	Type Pol.Filt	IP Address Network Mask	Bc Fr MTU VJC	PArp On	Filt GRE	RIP Met. OSPF Met.	SAMode DBcast	IPSc Mul.
LOCAL	-	Not Set	- n	-	---	-	-	--
---	----	-	-	-	---	-	-	---
vlan11	Static	192.168.163.39	1 y	On	---	01	Pass	--
---	---	255.255.255.0	1500	-	---	0000000001	No	On
ppp1	Dynamic	0.0.0.0	1 y	-	---	01	Pass	--
---	---	255.255.255.255	1500	Off	---	0000000001	No	On
-----								

## OSPF

---

Open Shortest Path First (OSPF) is an Internal Gateway Routing Protocol, based on Shortest Path First (SPF) or link-state technology. OSPF is a routing protocol that determines the best path for routing IP traffic over a TCP/IP network.

These features are supported by OSPF:

- Authentication of routing updates.
- Tagging of externally-derived routes.
- Fast response to topology changes with low overhead.
- Load sharing over meshed links.

OSPF supports three types of physical networks—point-to-point, broadcast and non-broadcast.

When using OSPF to route an IP packet, the switch looks up the routing table entry which best matches the destination of the packet. This routing table entry contains the interface and nexthop switch to forward the IP packet to its destination. The routing table entry that best matches the destination is determined first by the path type, then the longest (most specific) network mask. At this point there may still be multiple routing entries to the destination; if so then equi-cost multi-path routes exist to the destination. Such equi-cost routes are appropriately used to share the load to the destination.

[Chapter 29, Open Shortest Path First \(OSPF\)](#) includes examples of how to configure:

- [“Basic OSPF Network” on page 29-20](#)
- [“OSPF Network with Addressless PPP Links” on page 29-22](#)
- [“OSPF Network with Virtual Links” on page 29-23](#)

## Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is a distance vector protocol that is part of the TCP/IP protocol suite used to exchange routing information between switches. RIP determines a route based on the smallest hop count between source and destination.

Routing protocols such as RIPv1 and RIPv2 can be enabled on a VLAN. To enable RIPv2 on vlan11, enter the command:

```
add ip rip interface=vlan11 send=rip2 receive=both
```

To display information about RIP ([Figure 22-2 on page 22-5](#)), enter the command:

```
show ip rip
```

Figure 22-2: Example output from the **show ip rip** command.

Interface	Circuit/DLCI	IP Address	Send	Receive	Demand	Auth	Password
-----	-----	-----	-----	-----	-----	-----	-----
vlan11	-	-	RIP2	BOTH	NO	NO	
ppp0	-	172.16.249.34	RIP1	RIP2	YES	PASS	*****
-----	-----	-----	-----	-----	-----	-----	-----

For more information about RIP and the output from this command, see [Chapter 28, Routing Information Protocol \(RIP\)](#).

## IP Multicasting

---

IP multicasting is used to transmit packets to a group of hosts simultaneously on a TCP/IP network or sub-network. Network bandwidth is saved because files are transmitted as one data stream and are split apart by the switch to the target stations at the end of the path.

The multicast environment consists of senders (IP hosts), routers and switches (intermediate forwarding devices) and receivers (IP hosts). Any IP host can send packets to a multicast group, in the same way that they send unicast packets to a particular IP host, by specifying its IP address. A host need not belong to a multicast group in order to send packets to the multicast group. Packets sent to a group address are only received by members of the group.

For multicasting to succeed, the switch needs to know which of its interfaces are directly connected to members of each multicast group. To establish this, the switch uses Internet Group Management Protocol (IGMP) for multicast group management. IGMP is used between hosts and multicast routers and switches on a single physical network to establish hosts' membership in particular multicast groups.

The switch uses this information, in conjunction with a multicast routing protocol, to know which other routers to route multicast traffic to. The switch maintains a routing table for multicast traffic with Distance Vector Multicast Routing Protocol (DVMRP), Protocol Independent Multicast-Sparse Mode (PIM-SM), or Protocol Independent Multicast-Dense Mode (PIM-DM). You must configure IGMP and one of the multicast routing protocols before the switch can forward multicast packets. DVMRP and PIM-Sparse Mode share a separate multicast forwarding table.

When the switch receives a packet addressed to a multicast group, it forwards it to the interfaces that have group members connected to them, according to IGMP, and out other interfaces specified by the multicast routing protocol. Membership in a multicast group is dynamic; hosts can join and leave at any time. Multicast groups can be long or short lived, and can have relatively stable or constantly changing membership. There is no limit on the location or number of members in a multicast group. A host can belong to more than one multicast group at a time.

When the switch finds out from IGMP that a new host has joined a multicast group on one of its interfaces, the switch needs to receive the multicast traffic for this group, so that it can forward it to the host. The switch uses the multicast routing protocol (DVMRP, PIM-SM or PIM-DM) to notify routers closer to the sender (upstream) to forward it traffic for the group.

## Configuring IGMP

By default, IGMP is disabled on the switch and on all interfaces. To enable IGMP on the switch, enter the command:

```
enable ip igmp
```

You must enable IGMP on an interface before the interface can send or receive IGMP messages. If DVMRP is used for multicast routing, you must also enable IGMP on any interfaces used by DVMRP. For example, to enable IGMP on vlan11, enter the command:

```
enable ip igmp interface=vlan11
```

IGMP keeps the local group database up to date with current multicast group members by updating it when it hears IGMP Host Membership Reports on an interface. If the switch is the IGMP designated router for the subnetwork, it sends out IGMP Host Membership Queries at a Query Interval. If the switch does not receive a Host Membership Report for a multicast group on an interface within the Timeout period, it deletes the multicast group from its local group database. The default value of the Query Interval (125 seconds) and of the Timeout ( $2 \times (\text{Query Interval} + 10)$  seconds) will suit most networks. You should only change these defaults with caution, and if you have a sound understanding of how they affect interaction with other devices. To change the intervals, enter the command:

```
set ip igmp [timeout=1.65535] [queryinterval=1.65535]
```

To display information about IGMP and multicast group membership, enter the command:

```
show ip igmp
```

## Configuring Multicast Routing

[Chapter 27, IP Multicasting](#) includes examples of how to configure:

- Distance Vector Multicast Routing Protocol (DVMRP)—see [“Multicasting using DVMRP” on page 27-35](#)
- Protocol Independent Multicast Sparse Mode (PIM-SM)—see [“PIM-SM” on page 27-39](#)
- Protocol Independent Multicast Dense Mode (PIM-DM)—see [“PIM-DM” on page 27-43](#)

## Novell IPX

The switch's implementation of the Novell IPX protocol uses the term *circuit* to refer to a logical connection over an *interface*, similar to an X.25 permanent virtual circuit (PVC) or a Frame Relay Data Link Connection (DLC). The term *interface* is used to refer to the underlying physical interface, such as VLAN, Ethernet, Point-to-Point (PPP) and Frame Relay.

Before you start configuring IPX, collect the information that you will need. Pay particular attention to the following points:

- Each network in a Novell internet, including all LANs and WAN links, must be assigned a network number. Novell file servers also have an internal network number. These network numbers must be unique across the Novell internet—no two networks or file servers may use the same network number. All devices attached to a network must use the same network number to refer to the network. Check to see what numbers your file servers are using. Many schemes exist to ensure that numbers are kept unique, for example, using the hexadecimal representation of the IP address or the telephone number of each location.
- All switches, file servers and workstations attached to an Ethernet LAN must use the same Ethernet encapsulation or frame type. [Table 22-1 on page 22-8](#) lists the Novell frame type and the equivalent switch encapsulation. You can determine the file server name, internal network number, Ethernet frame type and Ethernet network number used by a Novell file server, by interrogating the file server itself. From the management console attached to the Novell file server, at the system console prompt type the command "config" and record the values of the fields "File server name", "IPX internal network number", "Frame type" and "LAN protocol". You can also access the system console by running the console utility from any workstation logged in as supervisor. For more details, contact your local Novell network administrator or refer to the Novell documentation.

Table 22-1: Frame type and equivalent switch encapsulation.

Novell Frame Type	Switch Encapsulation
Ethernet_802.3	802.3
Ethernet_802.2	802.2
Ethernet_II	EthII
Ethernet_SNAP	SNAP

To create IPX circuit 1 with the Novell network number 129 over vlan11, use the command:

```
add ipx circ=1 interface=vlan11 network=129 encap=802.3
```

To display information about the circuits configured for IPX ([Figure 22-3](#)), use the command:

```
show ipx circuit
```



Figure 22-3: Example output from the **show ipx circuit** command.

```
IPX CIRCUIT information

Name ..... Circuit 1
Status ..... enabled
Interface ..... vlan11    (802.3)
Network number ..... c0e7230f
Station number ..... 0000cd000d26
Link state ..... up
Cost in Novell ticks ..... 1
Type20 packets allowed ..... no
On demand ..... no

Spoofing information
Keep alive spoofing ..... no
SPX watch dog spoofing ..... no
On SPX connection failure .... UPLINK
On end of SPX spoofing ..... UPLINK

RIP broadcast information
Change broadcasts ..... yes
General broadcasts ..... yes
General broadcast interval ... 60 seconds
Maximum age ..... 180 seconds

SAP broadcast information
Change broadcasts ..... yes
General broadcasts ..... yes
General broadcast interval ... 60 seconds
Maximum age ..... 180 seconds

Filter information
Filters ..... none
```

Chapter 38, Novell IPX includes examples of how to configure:

- “Basic IPX Setup” on page 38-17
- “IPX Dial-On-Demand” on page 38-22

## AppleTalk

---

To create an AppleTalk port (interface) associated with the vlan11, use the command:

```
add apple port interface=vlan11
```

To display information about the ports configured for AppleTalk ([Figure 22-4 on page 22-10](#)), use the command:

```
show apple port
```

Figure 22-4: Example output from the **show apple port** command.

```
Appletalk Port Details
-----
Port Number ..... 1
Interface ..... vlan11
ifIndex ..... 1
Node ID ..... 217
Network Number ..... 22
Network Range Start ..... 22
Network Range End ..... 22
State ..... ACTIVE
Seed ..... NO
Seed Network Start ..... 0
Seed Network End ..... 0
Hint ..... YES
Hint Node ID ..... 179
Hint Network ..... 22
Default Zone ..... -

Zone List is Empty
-----
```

For more information about AppleTalk and the output from this command, see [Chapter 37, AppleTalk](#).