Chapter 21

Overview of Routing

Introduction

This chapter introduces some of the routing protocols supported by the router. Full details of these protocols, and all other routing protocols supported by the switch, are in individual chapters of this Software Reference.

IP Networks

TCP/IP is the most widely used network protocol. The Internet uses TCP/IP for routing all its traffic. TCP/IP provides a range of services including remote login, Telnet, file transfer (FTP), Email and access to the World-Wide Web.

The router routes TCP/IP packets:

- between switch ports in separate VLANs
- across the Wide Area Network using services like ISDN, Frame Relay and leased lines. This enables you to join remote TCP/IP LANs together as a single internet to exchange information.

Configuration Example

This example (Figure 21-1 on page 21-2) illustrates the steps required to configure TCP/IP using the router's command line interface. Two routers running TCP/IP will be connected together using the Point-to-Point Protocol (PPP) over a wide area link. Each router is associated with a VLAN.

Figure 21-1: Example configuration for an IP network

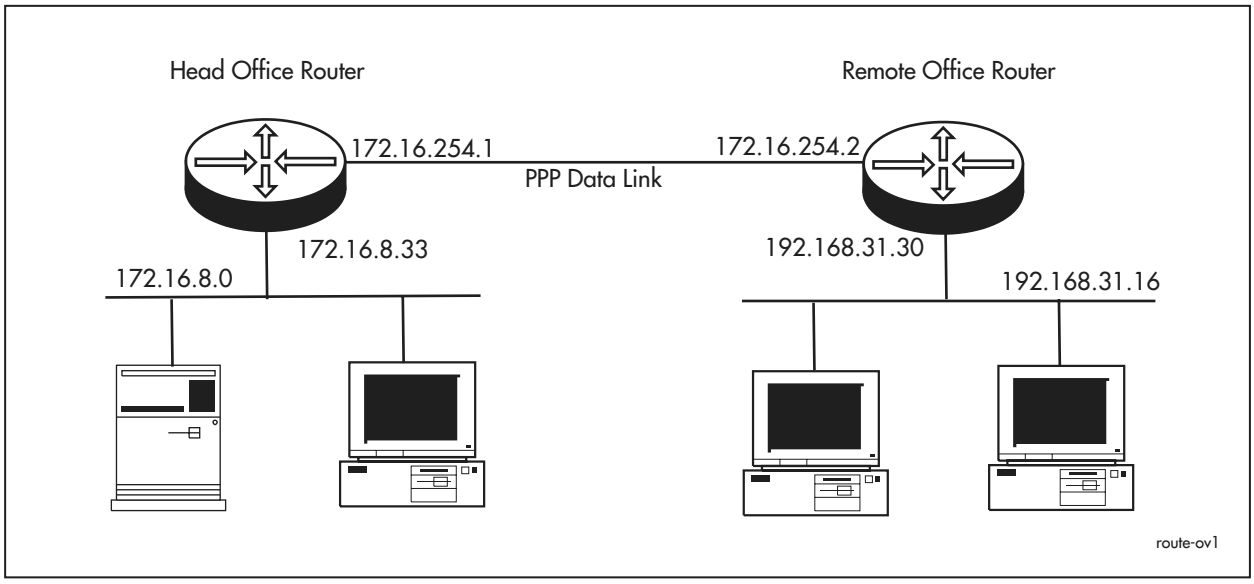

Table 21-1: Example configuration parameters for an IP network

Parameter	Head Office Router	Remote Office Router
VLAN interface	vlan2	vlan3
Ports (untagged)	Ports 2-4	Ports 1-3
VLAN interface IP address	172.16.8.33	192.168.31.30
VLAN IP subnet address	172.16.8.0	192.168.31.16
Ethernet LAN IP subnet mask	255.255.255.0	255.255.255.240
PPP interface	ppp0	ppp0
PPP interface IP address	172.16.254.1	172.16.254.2
PPP interface IP subnet address	172.16.254.0	172.16.254.1
PPP interface IP subnet mask	255.255.255.0	255.255.255.0

To configure IP follow these steps

The following steps are required:

1. Configure the PPP Link.
2. Create a VLAN and add untagged ports.
3. Configure the IP routing module on both routers.
4. Test the configuration.
5. Save the configuration.

1. Configure the PPP Link

For information on how to configure PPP interface 0 on each router to use the wide area link, see:

- "Configuration Procedures and Examples" on page 10-20 of Chapter 10, ATM over xDSL for information about configuring PPP and PPPoE over ADSL.
- "Point to Point Protocol (PPP)" on page 7-11 of Chapter 7, Overview of Physical and Layer 2 Interfaces for information about configuring PPP to use a synchronous link.
- "A Basic ISDN Setup" on page 11-49 of Chapter 11, Integrated Services Digital Network (ISDN) for information about configuring PPP to use an ISDN call.

  If the PPP interface is configured for dial-on-demand or bandwidth on demand operation, these services are automatically used by the IP routing software. For more information see "Configuring ISDN Dial on Demand" on page 11-58 and "Configuring ISDN Bandwidth on Demand" on page 11-58 of Chapter 11, Integrated Services Digital Network (ISDN).

2. Create VLANs and add untagged ports

Each new VLAN is created with a VLAN name that is unique in the router, and a VLAN Identifier (VID) that uniquely identifies the VLAN on the physical LAN. If the VLAN name begins with "vlan" and ends in a number then the number must be the same as the VID specified. To create VLANs, enter the command:

```
create vlan=vlanname vid=2..4094
```

In this example two VLANs are created by entering the commands:

```
create vlan=vlan2 vid=2
create vlan=vlan3 vid=3
```

To add untagged ports to vlan2, enter the command:

```
add vlan=vlan2 port=2-4
```

To add untagged ports to vlan3, enter the command:

```
add vlan=vlan3 port=1-3
```

For more detailed information about creating VLANs and configuring ports, see Chapter 8, Switching.

3. Configure IP Routing

To clear any pre-existing IP configuration and turn on the IP routing software on each router, enter the commands:

```
purge ip
enable ip
```

On the Head Office router define two IP interfaces, one for the VLAN and one for the wide area link:

```
add ip int=vlan2 ip=172.16.8.33 mask=255.255.255.0
add ip int=ppp0 ip=172.16.254.1 mask=255.255.255.0
```

Repeat this procedure on the Remote Office router, defining one IP interface for the VLAN and one for the wide area link:

```
add ip int=vlan3 ip=192.168.31.30 mask=255.255.255.240
add ip int=ppp0 ip=172.16.254.2 mask=255.255.255.0
```

A routing protocol, such as RIP, can be enabled so that the routers can exchange information about routes to all of the IP devices (hosts, PCs, file servers, etc.) on the internet. However, on a dial-on-demand ISDN connection this may result in excessive call charges. So for this example static routes are defined. On the Head Office router enter the command:

```
add ip route=192.168.31.0 mask=255.255.255.240 int=ppp0
   next=172.16.254.2
```

Repeat this procedure for the Remote Office router, entering the command:

```
add ip route=172.16.8.0 mask=255.255.255.0 int=ppp0
   next=172.16.254.1
```

The IP routing software is now configured and operational on both routers.

4. Test the configuration.

Check the IP configuration using the following commands and then functionally test the configuration by establishing a Telnet (remote access) connection to the remote router.

To check the routes, enter the command (on either router):

```
show ip route
```

For each router, there should be a route to the LAN and PPP interfaces on the local router and a route to the LAN interface on the remote router.

Test the PPP link between the two routers using the PING command on each router to send ping packets to the router at the remote end of the PPP link. On the Head Office router, enter the command:

```
ping 192.168.31.30
```

On the Remote Office router, enter the command:

```
ping 172.16.8.33
```

Within a few seconds the router will display a message like:

```
echo reply 1 from 172.16.8.33 time delay 20 ms
```

indicating a response was received from the router at the remote end of the PPP link.

To functionally test the connection between the two routers, use Telnet to establish a connection to the remote router. Enter the following command on the Head Office router to connect to the Remote Office router:

```
telnet 192.168.31.30
```

You will see the login screen for the Remote Office router. To connect from the Remote Office router to the Head Office router, on the Remote Office router, enter the command:

```
telnet 172.16.8.33
```

5. Save the configuration

To save the new dynamic configuration as a script, enter the command:

```
create config=ipconf.scp
```

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 router looks up the routing table entry which best matches the destination of the packet. This routing table entry contains the interface and nexthop router 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 26, Open Shortest Path First (OSPF) includes examples of how to configure:

- "Basic OSPF Network" on page 26-20
- "OSPF Network with Addressless PPP Links" on page 26-22
- "OSPF Network with Virtual Links" on page 26-24

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 routers. 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 the admin VLAN (vlan11), enter the command:

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

To display information about RIP (Figure 21-2 on page 21-6), enter the command:

```
show ip rip
```

Figure 21-2: 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 25, 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 router 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 router needs to know which of its interfaces are directly connected to members of each multicast group. To establish this, the router 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 router uses this information, in conjunction with a multicast routing protocol, to know which other routers to route multicast traffic to. The router 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 router can forward multicast packets. DVMRP and PIM-Sparse Mode share a separate multicast forwarding table.

When the router 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 router finds out from IGMP that a new host has joined a multicast group on one of its interfaces, the router needs to receive the multicast traffic for this group, so that it can forward it to the host. The router 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 router and on all interfaces. To enable IGMP on the router, 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. To enable IGMP on an interface, enter the command:

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

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 router is the IGMP designated router for the subnetwork, it sends out IGMP Host Membership Queries at a Query Interval. If the router 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*(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 24, IP Multicasting includes examples of how to configure:

- Distance Vector Multicast Routing Protocol (DVMRP)—see "Multicasting using DVMRP" on page 24-29
- Protocol Independent Multicast Sparse Mode (PIM-SM)—see "PIM-SM" on page 24-35
- Protocol Independent Multicast Dense Mode (PIM-DM)—see "PIM-DM" on page 24-39

Novell IPX

The router'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* refers 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 routers, file servers and workstations attached to an Ethernet LAN must use the same Ethernet encapsulation or frame type. Table 21-2 on page 21-8 lists the Novell frame type and the equivalent AR400 router 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 21-2: Frame type and equivalent router encapsulation

Novell Frame Type	Router 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 21-3), use the command:

```
show ipx circuit
```

Figure 21-3: 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 36, Novell IPX includes examples of how to configure:

- "Basic IPX Setup" on page 36-17
- "IPX Dial-On-Demand" on page 36-23

AppleTalk

The AppleTalk network architecture provides internetworking of Macintosh computers and other peripheral devices using LocalTalk media. AppleTalk allows seamless access to network services such as file servers and printers from the Macintosh desktop environment. The open nature of the architecture has enabled the AppleTalk network system to extended support to other media types (for example EtherTalk for Ethernet media), and a mixture of both Apple and non-Apple network devices on the same AppleTalk network.

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

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

To display information about the ports configured for AppleTalk (Figure 21-4 on page 21-10), enter the command:

```
show apple port
```

Figure 21-4: 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 35, AppleTalk.