CHAPTER 6

Configuring Networking Protocols

This chapter describes networking protocol configurations for the Layer 3 switch routers. It provides initial configuration information so you can get your Layer 3 switch router up and running. For more information about the Cisco IOS commands used in this chapter, refer to the *Cisco IOS Command Reference* publication. This chapter contains the following sections:

- Understanding IP Routing Protocols, page 6-2
- Configuring IP Routing Protocols, page 6-4
- Monitoring and Verifying IP Operation, page 6-6
- Understanding IP Uplink Redirect, page 6-6
- Configuring IP Uplink Redirect, page 6-8
- Verifying IP Uplink Redirect, page 6-8
- Understanding IP Multicast Routing, page 6-8
- Configuring IP Multicast Routing, page 6-12
- Monitoring and Verifying IP Multicast Operation, page 6-12
- Understanding IPX, page 6-12
- Configuring Novell IPX Routing, page 6-14
- Monitoring and Verifying IPX Operation, page 6-15

Note You are at Step 5 in the suggested process for configuring your Layer 3 switch router (see the "Suggested Process for Configuring the Layer 3 Switch Routers" section on page 2-1). You should have already completed general interface configurations before proceeding with configuring networking and routing protocols.

Note Layer 2 entries, IP routing, IP multicast routing, and Novell IPX routing share the 24K content addressable memory (CAM) on the Fast Ethernet ports. Layer 2 entries, IP routing, IP multicast routing, Access Control Lists (ACLs), and Novell IPX routing share the 32K CAM on the Gigabit Ethernet ports.

Understanding IP Routing Protocols

This section describes how to configure the Layer 3 switch router for supported IP routing protocols. It is intended to provide enough information for a network administrator to get the protocols up and running. However, this section does not provide in-depth configuration detail for each protocol. For detailed information, refer to the *Cisco IOS IP and IP Routing Configuration Guide* and the *Cisco IOS IP and IP Routing Command Reference* publications.

IP routing is enabled by default on the Layer 3 switch router. For IP routing, you need the following to configure your interface:

- A network address or a subnetwork address
- An IP subnet mask

You also need to set the following global configurations:

- Select a routing protocol, such as the Enhanced Interior Gateway Routing Protocol (EIGRP) or the Routing Information Protocol (RIP).
- Assign IP network numbers without specifying subnet values.

Layer 3 switching supports the routing protocols listed and described in the following sections.

Routing Information Protocol

RIP is a distance-vector, intradomain routing protocol. RIP works well in small, homogeneous networks. However, in larger, more complex internetworks, it has many limitations, such as a maximum hop count of 15, lack of support for variable-length subnet masks (VLSMs), inefficient use of bandwidth, and slow convergence. (RIP II does support VLSMs.)

Open Shortest Path First

Open Shortest Path First (OSPF) is a standards-based IP routing protocol designed to overcome the limitations of IP RIP. Because OSPF is a link-state routing protocol, it sends link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on the attached interfaces and their metrics is used in OSPF LSAs. As routers accumulate link-state information, they use the shortest path first algorithm (SPF) to calculate the shortest path to each node. Additional OSPF features include equal-cost multipath routing and routing based on the upper-layer type of service (ToS) requests.

OSPF employs the concept of an *area*, which is a grouping of contiguous OSPF networks and hosts. OSPF areas are logical subdivisions of OSPF autonomous systems whose internal topology is hidden to routers outside the area. Areas allow an additional level of hierarchy different from that provided by IP network classes, and they can be used to aggregate routing information and mask the details of a network. These features make OSPF particularly scalable to large networks.

Interior Gateway Routing Protocol

Interior Gateway Routing Protocol (IGRP) is a distance vector interior-gateway routing protocol developed by Cisco. Distance vector routing protocols call for each other to send all or a portion of its routing table in a routing update message at regular intervals to each of its neighboring routers. As routing information proliferates through the network, routers can calculate distance to all the nodes within the internetwork. IGRP uses a combination of metrics: internetwork delay, bandwidth, reliability, and load are all factored into the routing decision.

Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of IGRP that combines the advantages of link-state protocols with distance vector protocols. EIGRP incorporates the Diffusing Update Algorithm (DUAL). EIGRP includes features such as fast convergence, variable-length subnet masks, partial bounded updates, and multiple network-layer support.When a network topology change occurs, EIGRP checks its topology table for a suitable new route to the destination. If such a route exists in the table, EIGRP updates the routing table instantly.You can use the fast convergence and partial updates EIGRP provides to route IPX packets.

EIGRP saves bandwidth by sending routing updates only when routing information changes. The updates contain only information about the link that changed, not the entire routing table. EIGRP also takes into consideration the available bandwidth when determining the rate at which it transmits updates.

Note Layer 3 switching does not support the Next Hop Resolution Protocol (NHRP).

Border Gateway Protocol

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) that allows you to set up an interdomain routing system to automatically guarantee the loop-free exchange of routing information between autonomous systems. In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (called the autonomous system path), and a list of other path attributes.

Layer 3 switching supports BGP version 4, including classless interdomain routing (CIDR). CIDR lets you reduce the size of your routing tables by creating aggregate routes resulting in supernets. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. CIDR routes can be carried by OSPF, EIGRP, and RIP.

Configuring IP Routing Protocols

To configure routing protocols to run on a Fast Ethernet or Gigabit Ethernet interface, perform the following task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **router rip** Router(config)#	Define RIP as the routing protocol and start the RIP routing process.
Step 2	Router(config-router)# **network** *net-number*	Specify a directly connected network based on the Internet Network Information Center (InterNIC) network number—not a subnet number or individual address. The routing process associates interfaces with the appropriate addresses and begins processing packets on the specified network.
Step 3	Router(config-router)# **exit** Router(config)#	Return to global configuration mode.
Step 4	Router(config)# **router igrp** *autonomous-system-number* Router(config-router)#	Define IGRP as the IP routing protocol. The autonomous system number is the autonomous system to which this Layer 3 switch router belongs.
Step 5	Router(config-router) # **network** *net-number* Router(config-router) #	Define the directly connected networks that run IGRP. The network number is the number of the network that is advertised by this Layer 3 switch router.
Step 6	Router(config-router)# **exit** Router(config)#	Return to global configuration mode.
Step 7	Router(config)# **router eigrp** *autonomous-system-number* Router(config-router)#	Define EIGRP as the IP routing protocol. The autonomous system number is the autonomous system to which this Layer 3 switch router belongs.
Step 8	Router(config-router)# **network** *net-number* Router(config-router) #	Define the directly connected networks that run EIGRP. The network number is the number of the network that is advertised by this Layer 3 switch router.
Step 9	Router(config-router)# **exit** Router(config)#	Return to global configuration mode.

	Command	Purpose
Step 10	Router(config)# **router ospf** *process-ID* Router(config-router)#	Define OSPF as the IP routing protocol. The process ID identifies a unique OSPF router process. This number is internal to the Layer 3 switch router only; the process ID does not have to match the process IDs on other routers.
Step 11	Router(config-router)# **network** *net-address* | *wildcard-mask* **area** *area-ID* Router(config-router) #	Assign an interface to a specific area. • The network address is the address of directly connected networks or subnets. • The wildcard mask is an inverse mask that compares a given address with interface addressing to determine whether OSPF uses this interface. • The area parameter identifies the interface as belonging to an area. • The area ID specifies the area associated with the network address.
Step 12	Router(config-router)# **end** Router#	Return to privileged EXEC mode.
Step 13	Router# **copy running-config startup-config**	Save configuration changes to NVRAM.
Step 14	Router(config)# **router bgp** *autonomous-system-number* Router(config-router)#	Define BGP as the IP routing protocol. The autonomous system number is the autonomous system to which this Layer 3 switch router belongs.
Step 15	Router(config-router) # **network** *net-number*	Define the directly connected networks that run BGP. The network number is the number of the network that is advertised by this Layer 3 switch router.
Step 16	Router(config-router)# **exit** Router(config)#	Return to global configuration mode.

Note This section does not describe IP configuration in detail. Refer to the IP documentation on the Cisco Documentation CD for detailed conceptual and configuration information.

Monitoring and Verifying IP Operation

After IP routing is configured, you can monitor and verify the protocol operation by performing the following tasks:

Command	Purpose
Router# **show ip protocol**	Show the Layer 3 switch router values about routing timers and network information associated with the entire router. Use this information to identify a Layer 3 switch router that is suspected of delivering bad router information.
Router# **show ip route**	Show the contents of the IP routing table. The routing table contains entries for all known networks and subnetworks and contains a code that indicates how that information was learned.
Router# **show ip interfaces**	Show the status and global parameters associated with an interface. Cisco IOS automatically enters a directly connected route in the routing table if the interface allows a protocol to send and receive packets. Such an interface is marked "up." If the interface is unusable, it is removed from the routing table.

Understanding IP Uplink Redirect

The IP uplink redirect feature is supported on the Catalyst 2948G-L3 switch router only. IP uplink redirect enables traffic between Fast Ethernet interfaces to be switched through the Gigabit Ethernet interface. ACLs applied on the Gigabit Ethernet interface filter traffic switched between Fast Ethernet interfaces.

Note The IP uplink redirect feature affects only IP Layer 3-switched traffic. It has no impact on Layer 2-switched or non-IP Layer 3-switched traffic like IP Multicast or IPX.

To filter traffic between two Fast Ethernet interfaces, perform these steps:

Step 1 Disable IP traffic switching between Fast Ethernet interfaces by enabling IP uplink redirect.

```
Router(config)# ip uplink-redirect
```

When IP uplink redirect is enabled, the network routes and adjacencies configured on Fast Ethernet interfaces and the network routes learned by Fast Ethernet interfaces are not populated in the Fast Ethernet interface CAM tables. Instead, only routes and adjacencies configured or learned on Gigabit Ethernet interfaces are populated in the Fast Ethernet interface CAM tables.

Note Bridge-Group Virtual Interface (BVI) and Fast EtherChannel routes and adjacencies are not populated in Fast Ethernet interface CAM tables. Gigabit EtherChannel routes and adjacencies are populated in Fast Ethernet interface CAM tables.

Step 2 Redirect IP traffic from Fast Ethernet interfaces to the Gigabit Ethernet interface (uplink port) by configuring the default route with the next hop as the Layer 3 switch router (upstream router) connected to the Gigabit Ethernet interface.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 upstream router ip address
```

After enabling IP uplink redirect and configuring the default route, Layer 3-switched traffic originating on Fast Ethernet interfaces and destined to a Fast Ethernet interface is switched to the upstream Layer 3 switch router connected to the Gigabit Ethernet interface. The upstream Layer 3 switch router switches the traffic back to the Catalyst 2948G-L3 switch router, which then switches the traffic to the appropriate Fast Ethernet interface.

Caution The default route configuration with the next hop interface cannot be used along with the **ip uplink-redirect** command to direct Fast Ethernet traffic to the Gigabit Ethernet interface.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 g49
```

Note After the default route is configured, if the Fast Ethernet traffic is not redirected to the Gigabit Ethernet interface, verify that a valid adjacency exists for the uplink router's IP address. Also, you can create an adjacency by configuring a static ARP entry.

Step 3 Filter traffic on the Gigabit Ethernet interface by applying appropriate ACLs on the Gigabit Ethernet interface, either on the outbound or inbound direction.

Caution This solution alters the normal IP routing path for traffic switched between two Fast Ethernet interfaces and increases the number of hops.

Caution The network processor on the Fast Ethernet interface does not switch certain IP packets, for instance IP packets with options, which are CPU process switched. The CPU switches the packets based on the IOS routing table.
When the redirect feature is enabled, the network processor switched packets and the CPU process switched packets between two hosts connected to different Fast Ethernet interfaces will take different paths.
ACLs can block traffic between two Fast Ethernet interfaces allowing IP packets with options to go through because the packets will be routed by the CPU process and not redirected to the Gigabit Ethernet interface.

Caution If the upstream Layer 3 switch router has an alternative better path (than the path used by the Gigabit Ethernet interface) to the Fast Ethernet interfaces of the Catalyst 2948G-L3 switch router, it could result in routing loops.

Configuring IP Uplink Redirect

To configure IP uplink redirect, perform the following task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **ip uplink-redirect** Router(config)#	Enable IP uplink redirect. You must reset your system for IP uplink redirect to take affect.
Step 2	Router(config)# **ip route** {*dest_prefix*} {*dest_prefix_mask*} {*forward_router_ip_addr*} Router(config) #	Define the default route for the next hop.
Step 3	Router(config)# **exit** Router#	Return to privileged EXEC mode.
Step 4	Router# **write**	Save the configuration to NVRAM.
Step 5	Router(config) # **no ip uplink-redirect** Router(config) #	Disable the IP uplink redirect feature.
Step 6	Router(config)# **exit** Router(config)#	Return to privileged EXEC mode.
Step 7	Router# **write**	Save the configuration to NVRAM.

Caution The **ip uplink-redirect** command will take affect after rebooting the Layer 3 switch router.

Verifying IP Uplink Redirect

After you configure the IP uplink redirect, you can verify the operation by performing the following task:

Command	Purpose
Router# **show ip uplink-redirect**	Show the running configuration and configuration on the next reload associated with the Layer 3 switch router.

Understanding IP Multicast Routing

As networks increase in size, multicast routing becomes critically important as a means to determine which segments require multicast traffic and which do not. IP multicasting allows IP traffic to be propagated from one source to a number of destinations, or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to the multicast group identified by a single IP destination group address.

A principal component of IP multicasting is the Internet Group Membership Protocol (IGMP). Hosts identify their multicast group membership by sending IGMP messages to the Layer 3 switch router. Traffic is sent to all members of a multicast group. A host can be a member of more than one group at a time. In addition, a host does not need to be a member of a group to send data to that group. Enabling Protocol Independent Multicast (PIM) on an interface enables IGMP operation on that interface.

IP multicasting supports constrained multicast flooding over Bridge Group Virtual Interfaces (BVIs), as well as BVIs over Fast EtherChannel (FEC). Using constrained multicast flooding, the Layer 3 switch router can dynamically determine per-group membership of bridge ports and flood multicast packets only to those ports where group members reside.

Cisco Group Management Protocol (CGMP) performs tasks similar to those performed by IGMP. CGMP works in conjunction with IGMP messages to dynamically configure ports on Cisco Layer 2 switches so that IP multicast traffic is forwarded only to those ports associated with IP multicast groups. Layer 3 switching supports CGMP server functionality, which is useful in integrating IP multicast support with Catalyst wiring closet switches. CGMP and IGMP protocols are necessary not only for IP multicast clients to join groups, but also for efficient leave processing, which saves bandwidth.

Supported IP Multicast Routing Protocols

Layer 3 switch routers support the following:

- Protocol Independent Multicast, page 6-9
- Distance Vector Multicast Routing Protocol Interoperability, page 6-10

Protocol Independent Multicast

Protocol Independent Multicast (PIM) includes two different modes of behavior for dense and sparse traffic environments. These are referred to as *dense mode* and *sparse mode*.

PIM dense mode assumes that the downstream networks want to receive the datagrams forwarded to them. The Layer 3 switch router forwards all packets on all outgoing interfaces until pruning and truncating occurs. Interfaces with PIM dense mode enabled receive the multicast data stream until it times out. PIM dense mode is most useful under these conditions:

- Senders and receivers are in close proximity to each other.
- The internetwork has fewer senders than receivers.
- The stream of multicast traffic is constant.

PIM sparse mode assumes that the downstream networks do not want to forward multicast packets for a group unless there is an explicit request for the traffic. PIM sparse mode defines a rendezvous point, which is used as a registration point to facilitate the proper routing of packets.

When a sender wants to send data, it first sends the data to the rendezvous point. When a Layer 3 switch router is ready to receive data, it registers with the rendezvous point. After the data stream begins to flow from the sender to the rendezvous point and then to the receiver, Layer 3 switch routers in the data path optimize the path by automatically removing any unnecessary hops, including the rendezvous point.

PIM sparse mode is optimized for environments in which there are many multipoint data streams and each multicast stream goes to a relatively small number of LANs in the internetwork. PIM sparse mode is most useful under these conditions:

- There are few receivers in the group.
- Senders and receivers are separated by WAN links.
- The stream of multicast traffic is intermittent.

Distance Vector Multicast Routing Protocol Interoperability

Distance Vector Multicast Routing Protocol (DVMRP) uses a reverse path flooding technique to form multicast routes. The Layer 3 switch routers support interoperability with routers configured for DVMRP, but do not support a full DVMRP implementation. Layer 3 switch routers can send and receive DVMRP routing updates and can be configured to tunnel as DVMRP does, but do not run the actual routing protocol. Layer 3 switch routers forward multicast packets that have been forwarded by DVMRP routers and, in turn, forward multicast packets to DVMRP routers.

Supported IP Multicast Functionalities

Layer 3 switch routers support the following IP multicast functionalities:

- Constrained Multicast Flooding, page 6-10
- Cisco Group Management Protocol Server, page 6-11

Constrained Multicast Flooding

Constrained multicast flooding (CMF) uses CGMP or IGMP to control the flooding of IP multicast data packets to only those ports where group members reside.

Layer 3 switches logically concatenate several network segments together, and these network segments appear as a single segment to any routers attached to the Layer 3 switch. If an IP host on any switched segment joins a group, IP multicast data packets destined to that group are typically flooded by a Layer 3 switch to all switched segments.

CMF helps a switch constrain the flooding of IP multicast data packets to only those switched segments that lead toward group members by listening to CGMP or IGMP transactions between hosts and multicast routers. Constrained flooding relieves the switch of unnecessary multicast packet replication, and relieves the network of unnecessary multicast packet transmission.

Layer 3 switch routers support CMF over BVIs as well as BVIs with FECs. CMF constrains the propagation of IP multicast data packets to only those bridge ports that lead toward group members or multicast routers.The following two types of lists for CMF are maintained in a bridge group:

- A multicast router ports list, which contains ports that have received PIM queries, IGMP queries, or DVMRP probes within a given time-out interval
- A per-group group G ports list, which contains ports that have received an IGMP membership report for group G within the IGMP membership query time-out interval

When CMF is enabled and at least one of the two lists contains information, the bridge forwards the IP multicast data packets destined for group G to group G ports and the multicast router ports. If both lists do not contain any information, IP multicast data packets destined for group G are flooded to all the ports in the bridge group.

Similarly, CMF forwards multicast data packets for BVIs over FECs. For example, IP multicast data packets for group G are forwarded to a BVI (that is part of group G's corresponding multicast entry) over a FEC that is also part of this group.

CMF is disabled by default and can be enabled through the CLI by entering the **bridge cmf** command.

Cisco Group Management Protocol Server

IP multicasting consists of the transmission of IP traffic between source and destination. Multicast data is sent from the server to hosts that want to join the multicast transmission. Host groups have a Class D IP address and the server transmits one data stream to the entire host group at the same time. The propagation of multicast traffic requires coordination among all network devices such as servers, hosts, routers, and switches.

To support IP multicasting, all devices in a network must support IGMP. CGMP support is optional.

Note The Layer 3 switch routers do not support IGMP snooping.

The Layer 3 switch routers support CGMP server functionality. When a host wants to join a multicast transmission, it sends a CGMP or IGMP join message to the server. In this join message, the host specifies its MAC address and indicates the IP multicast group it wants to join. By sending the join message, the host becomes a member of a multicast host group.

Similarly, when a host wants to leave a multicast transmission, it sends an IGMP leave message to the server. The Layer 3 switch router with CGMP server functionality maintains the forwarding table for the members in a multicast group that it supports.

The IGMP-capable Layer 3 switch router sends periodic multicast group queries. When a host wants to remain in a multicast group, it responds to the query. In this case, the Layer 3 switch router does nothing. If a host does not want to remain in the multicast group, it does not respond to the query. If after a number of queries, the Layer 3 switch router receives no reports from any host in a multicast group, the Layer 3 switch router removes the host from the multicast group and updates its forwarding table.

CGMP offers the following benefits:

- Allows IP multicast packets to be switched only to those ports that have IP multicast clients.
- Saves network bandwidth on user segments by not propagating any unnecessary IP multicast traffic.
- Does not require changes to the end host systems.
- Does not incur the overhead of creating a separate VLAN for each multicast group in the switched network.

Configuring IP Multicast Routing

To configure IP multicast routing, perform the following task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **ip multicast-routing**	Enable IP multicasting on the Layer 3 switch router.
Step 2	Router(config)# **interface** *type number* Router(config-if)#	Enter interface configuration mode to configure either the Fast Ethernet or Gigabit Ethernet interface.
Step 3	Router(config-if)# **ip pim** [**dense-mode** | **sparse mode** | **sparse-dense-mode**]	Run IP multicast routing on each interface on which you enter this command. You must indicate dense mode, sparse mode, or sparse-dense mode (for internetworks that include both cases).
Step 4	Router(config-if)# **end** Router#	Return to privileged EXEC mode.
Step 5	Router# **copy running-config startup-config**	Save your configuration changes to NVRAM.

Monitoring and Verifying IP Multicast Operation

After IP multicast routing is configured, you can monitor and verify its operation by performing the following task:

Command	Purpose
Router# **show ip mroute** [*count*]	Show the complete multicast routing table and the combined statistics of packets processed.

Understanding IPX

Cisco's implementation of Novell Internetwork Packet Exchange (IPX) provides all of the functionality of a Novell *external bridge* (Novell refers to their router functionality as bridging).

IPX is a proprietary protocol. Novell IPX can be described as follows:

- A datagram, connectionless protocol that does not require an acknowledgment for each packet
- A Layer 3 (network) protocol that defines the internetwork and internode addresses
- A router specification that identifies the Novell NetWare protocol suite

Novell IPX uses the following protocols and services:

- Routing Information Protocol (RIP)—facilitates the exchange of routing information
- NetWare Core Protocol (NCP)—provides client-to-server connections and applications

- Sequenced Packet Exchange (SPX)—provides Layer 4 (Transport) connection-oriented services
- Service Advertising Protocol (SAP)—advertises NetWare services and addresses, which make service availability dynamic

Note Layer 3 switching does not support the NetWare Link Services Protocol (NLSP).

IPX Network Addresses

An IPX network address consists of a network number and a node number, expressed in the format *network.node*.

Network number — A 4-byte (32-bit) number that identifies the physical network. The network number is expressed in hexadecimal and must be unique throughout the entire IPX internetwork. When configuring an IPX network number, you can omit the leading zeros.

Node number — Dotted triplets of 4-digit hexadecimal numbers that identify a node on the network. The node number is normally the MAC address of the NetWare node or router interface.

Both the network number and the host address are needed to deliver traffic to a host. Addresses are usually given as network numbers, followed by host addresses, separated by dots, as in the example: 4a.0000.0c00.23fe. In this example, the network number is 4a, and the host address is 0000.0c00.23fe.

Global and Interface Parameters

To configure Novell IPX as a routing protocol, you must configure both global and interface parameters.

Global Configuration Parameters

To configure global parameters for Novell IPX routing, perform these steps:

Step 1 Start the IPX routing process.

Step 2 Enable load sharing if appropriate for your network.

Load sharing divides routing tasks evenly among multiple Layer 3 switch routers to balance the work and improve network performance. The Layer 3 switch router supports up to two parallel paths.

After you start IPX routing and enable load sharing (if needed) on the Layer 3 switch router, you can configure the interface for Novell IPX routing.

Interface Configuration Parameters

To configure an interface for Novell IPX routing, perform these steps:

Step 1 Assign unique network numbers to each interface.

You can assign multiple network numbers to an interface, allowing support of different encapsulation types. The IPX network number is the number of the Novell network to which the interface is attached. IPX packets received on an interface that does not have a network number are ignored.

Step 2 Set the optional encapsulation type if it is different from the default.

The default encapsulation type for the Layer 3 switch router is **novell-ether** (Ethernet_802.3).

Note This section does not describe IPX configuration in detail. Refer to the IPX documentation on the Cisco Documentation CD for detailed conceptual and configuration information.

Configuring Novell IPX Routing

To enable Novell IPX routing and configure an interface, perform the following task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **ipx routing** [*node*]	Enable Novell IPX routing, and start the IPX routing process. If no node address is specified, the Layer 3 switch router uses the MAC address of the interface.
Step 2	Router(config)# **ipx maximum-paths** *number*	Allow load sharing over parallel metric paths to the destination. The maximum number of parallel paths for gigabit interfaces is 6 and Fast Ethernet interfaces is 2; the default number is 1.
Step 3	Router(config)# **interface** *type number* Router(config-if)#	Enter interface configuration mode to configure the Fast Ethernet or Gigabit Ethernet interface.

	Command	Purpose
Step 4	Router(config-if)# **ipx network** *number* [**encapsulation** {*type*}] [*secondary*]	Enter a unique hexadecimal IPX network number (up to eight numbers in length) for each interface.The IPX network number is the number of the Novell network to which the interface is attached. Novell packets received on an interface that does not have a Novell network number are ignored. The encapsulation type is optional. You can specify one of the following types: **novell-ether** (the default), **sap**, **arpa**, or **snap**.
Step 5	Router(config-if)# **end** Router#	Return to privileged EXEC mode.
Step 6	Router# **copy running-config startup-config**	Save configuration changes to NVRAM.

Caution When you enable per-port shaping and policing on the port of a Catalyst 2948G-L3 or 4908G-L3 switch router you will be unable to use IPX routing.

Monitoring and Verifying IPX Operation

After IPX routing is configured, you can monitor and troubleshoot the protocol operation by performing the following tasks:

Command	Purpose
Router# **show ipx interfaces**	Show the status and parameters of the interfaces configured for IPX.
Router# **show ipx interface fastethernet 1**	Show the status and parameters for the specified Fast Ethernet IPX interface.
Router# **show ipx route**	Show the contents of the IPX routing table.
Router# **show ipx servers**	Show the list of IPX servers discovered through SAP advertisements, plus the network address, port number, and number of hops and ticks to the server.
Router#**show ipx traffic**	Show the number and type of IPX packets transmitted and received, as well as the number of broadcasts, SAPs, and routing packets received.

See Appendix C, “Configuration Examples,” for Catalyst 2948G-L3 switch router configuration examples.