Part No. 314722-A Rev 00
September 2002

4655 Great America Parkway
Santa Clara, CA 95054

# Configuring IPX Routing Operations

*Passport 8000 Series Switch*
*Software Release 3.3*

NORTEL NETWORKS™

## Copyright © 2002 Nortel Networks



The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

## Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Passport, and Alteon are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

SSH is a registered trademark and SSH Secure Shell is a registered trademark of SSH Communications Security Corp (www.ssh.com). The use of these trademarks is permitted to describe a product that conforms to the SSH standard and protocol.

The asterisk after a name denotes a trademarked item.

## Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## Nortel Networks Inc. software license agreement

**NOTICE:** Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

**1. License grant.** Nortel Networks Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

**2. Restrictions on use; reservation of rights.** The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals

or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

**3. Limited warranty.** Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

**4. Limitation of liability.** IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

# Contents

# Figures

# Tables

# Preface

This guide provides information about using the features and capabilities of the Device Manager graphical user interface (GUI) to perform general network management operations on an 8000 Series Switch. The guide also provides instructions for using the CLI to perform basic switch management for the 8000 Series Switch.

For more information about using a 8000 Series Switch, a list of publications can found in the Related Publications section of the release notes that accompany your software, or on the Nortel Networks documentation Web site at www.nortelnetworks.com/documentation; search term: Passport 8000.

## Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Experience with windowing systems or GUIs

# Text conventions

| | |
|---|---|
| angle brackets (< >) | Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.<br>Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12` |
| **`bold Courier text`** | Indicates command names and options and text that you need to enter.<br>Example: Use the **`dinfo`** command.<br>Example: Enter **`show ip`** {**`alerts`**\|**`routes`**}. |
| braces ({}) | Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.<br>Example: If the command syntax is:<br>`action <action choice>`, the options for <action choice> are {none\|flushMacFdb\|flushArp \|flushIp\|flushAll\|triggerRipUpdate} |
| brackets ([ ]) | Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.<br>Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`. |
| *italic text* | Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by a hyphen.<br>Example: If the command syntax is:<br>`show at` *`valid-route`*`>`, *`valid-route`* is one variable and you substitute one value for it. |

| | |
|---|---|
| `plain Courier text` | Indicates command syntax and system output, for example, prompts and system messages.<br>Example:<br>`8000 Series Switch-8600# show config verbose` |
| vertical line \| | Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.<br>Example: If the command syntax is:<br>`config cli more <true\|false>`, you must enter either `config cli more true` or `config cli more false`, but not both. |

# How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

| Technical Solutions Center | Telephone |
|---|---|
| Europe, Middle East, and Africa | (33) (4) 92-966-968 |
| North America | (800) 4NORTEL or (800) 466-7835 |
| Asia Pacific | (61) (2) 9927-8800 |
| China | (800) 810-5000 |

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

# Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

# Chapter 1
# IPX routing concepts

This chapter describes IPX routing concepts, and discusses the following topics:



## IPX protocol overview

The 8000 Series Switch implementation of IPX supports four Ethernet frame formats:

- Ethernet II
- 802.2-LLC
- 802.3-RAW
- 802.3-SNAP

Frame translations from one frame format to another frame format are supported. However, the IPX host format must match the defined protocol frame format of the interface to which the host is connected.

In the 8000 Series Switch, IPX is supported on routed VLANs. IPX routing does not support brouter ports, but an IPX-protocol VLAN can exist on a brouter port.

This chapter discusses the following topics and includes IPX features that the 8000 Series Switch supports:



# IPX protocol

The Internetwork Packet Exchange (IPX) Protocol is the Novell, Inc. adaptation of the Xerox Network System (XNS) Protocol.

IPX is a connectionless datagram type of service that does not guarantee delivery of packets. Upper-layer protocols are responsible for reliability. The upper-layer protocols that IPX uses are SPX and NCP. IPX uses the Internet Data Packet (IDP) format.

IPX is the network layer routing protocol used in the NetWare environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. The network interface card (NIC) in a client provides network node addressing.

IPX defines the *internetwork* and *intranode* addressing as follows:

- *Network addresses* form the basis of the IPX internetwork addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address that routers use to forward packets to their final destinations. A network address in the NetWare environment consists of 8 hexadecimal characters. In this example, *0x* indicates that it is a hexadecimal number, and *n* is any hexadecimal character:

  *0xnnnnnnnn*

- *Socket numbers* are the basis for an IPX intranode address, that is, the address of an individual entity within a node. They allow a process (for example, RIP or SAP) to distinguish itself to IPX. To communicate on the network, the process must request a socket number. Any packets that IPX receives addressed to that socket are then passed on to the process within the node.

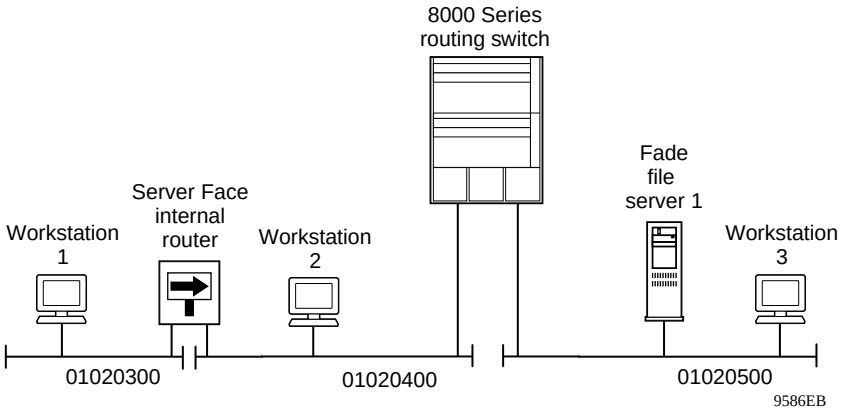
The most basic network configuration consists of a single client and a file server. The following are major server characteristics:

- Server name — a logical entity used to aid in managing services and devices
- Internal network address
- MAC address — a 6-byte PROM based in the NIC
- Server type — automatically assigned by Novell based on services offered (such as print server, file server, or application server)

An internetwork is created when two or more networks are joined together by a router. In an internetwork, each network segment maintains all the properties of a multiple server network with the connection device (the router) distinguishing one segment from another by its network address.

In Figure 1, networks 01020300, 01020400, and 01020500 are joined by routers. Each segment has its own unique network address, which is assigned for each interface of the routing device and is used to identify each network segment. Routing devices can be file servers acting as a router (internal routers) or dedicated routers, such as a 8600 Switch.

**Figure 1** IPX internetwork




Network layer addresses use hexadecimal characters and are one to eight digits in length. Valid addresses are 00000001 to FFFFFFFD; address FFFFFFFE is reserved for the default route. Network addresses, commonly called external addresses, are assigned to NICs during installation. In addition, most Novell routing devices are also assigned an internal address, the logical network where all file server services reside.

Figure 1 shows a three-segment Novell internetwork. Network 01020300 contains workstation 1 and the left half of the internal router (Fade). Network 01020400 includes the right half of the internal router (Face), workstation 2, and the left side of the 8600 Switch. Network 01020500 consists of the right side of the 8600 Switch, file server 1 (Fade), and workstation 3. The internal network addresses, Face and Fade, are assigned to the file servers. Clients are not assigned network layer addresses but rather acquire them from the nearest routing device.

File servers provide shared services to network users. File servers enable network users to share common network services and devices as well as network applications loaded on the file server. All services are advertised by SAP using Split Horizon techniques and are tied to a network address. To discover the network address of the closest server containing the services you require, the IPX client issues a Get Nearest Server (GNS) request. The GNS request contains the

nearest server's name, its full internetwork address, and the number of hops required to reach that server. Applications are statically stored on the server; when network users log on to the server and request to use an application, the application is downloaded and executed within the memory of the workstation.

Communication between a server and client requires the use of numerous protocols. As data makes its way through the protocol stack of one device on the way to another device, the data is continuously enveloped by various protocol headers until it is sent to the destination device. When the destination device is reached, the headers that were added by the source device are sequentially stripped away.

## IPX packets

An IPX packet consists of two major parts: a 30-byte header and the data portion. The destination and source network, node, and socket addresses make up the IPX packet header. The header contains fields with the following information:

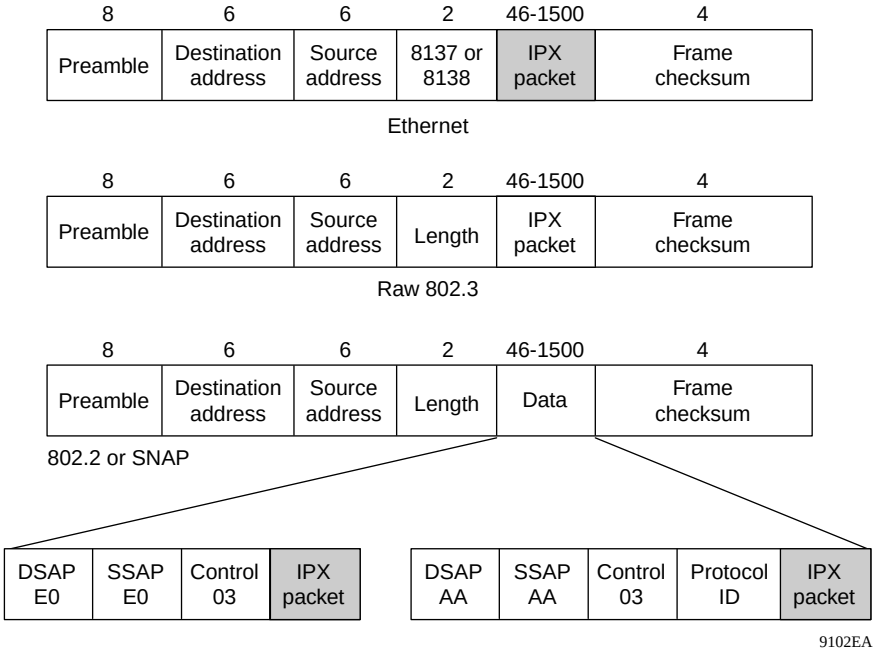
- Checksum
- Packet length (Total length can range from 30 to 64,535 bytes.)
- Transport control — indicating how many routers an IPX packet has passed through on its way to the destination network (When the value reaches 16, the packet is discarded.)
- Packet type — a 1-byte field (Novell-specified) to indicate the type of service such as RIP (1), SAP (4), NetBIOS (20), NCP (17), and unknown (0)
- Destination network, destination node, and destination socket
- Source network, source node, and source socket

Figure 2 shows the contents of the header, and Figure 3 shows the contents of the four supported types of IPX packets.

**Figure 2** IPX internetwork packet exchange header

| | |
|---|---|
| Checksum = FFFF | 2 bytes |
| Packet length | 2 bytes |
| Transport control | 1 byte |
| Packet type | 1 byte |
| Destination network | 4 bytes |
| Destination node | 6 bytes |
| Destination socket | 2 bytes |
| Source network | 4 bytes |
| Source node | 6 bytes |
| Source socket | 2 bytes |
| Data | |

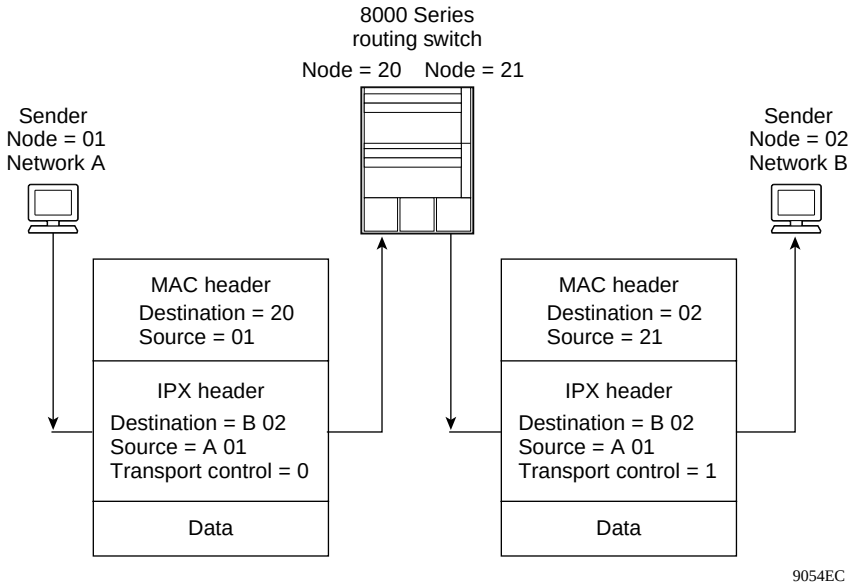
**Figure 3** IPX packets



# IPX traffic

IPX devices communicate through an IPX router. Figure 4 shows a typical example.

**Figure 4** IPX addressing




The sender and receiver can be any type of Novell device (for example, two workstations, two routers, two file servers, or a workstation and a server). The sender obtains information on its own segment and then prepares its packet to send. The sending node places the destination node internetwork address (network address, node address, and socket number) in the destination address fields of the IPX header and its own internetwork address in the source address fields.

In the MAC header, it places the node address of the router that responded to its RIP request in the destination field and its own node address in the source address field. It then sends the packet through the network media.

When the router receives the packet, if it is directly connected to the packet's destination segment, it places the destination node address from the IPX header in the destination address fields of the MAC header and increments the hop count in the transport control field by one. It then places its own node address into the source address field of the MAC header and transmits the packet.

If the router is not directly connected to the destination network segment, it passes the packet to the next router in the path to the destination node, by placing the next router node address into the destination address field of the MAC header. It places its own node address in the source address field, increments the hop count by one, and sends the packet to the next router.

When the packet arrives at the final destination, the MAC header is stripped out by the packet driver in the receiving node, the IPX header is stripped out by the IPX protocol, and the data is passed to the receiving node.

## 8000 Series Switch IPX network-layer support

An 8000 Series Switch running IPX provides the following network-layer support:

- Dynamic routing of IPX packets
- Up to four IPX network addresses to an interface
- Routing Information Protocol (RIP)
- Service Advertisement Protocol (SAP)
- Static route support
- Default route support

## Routing Information Protocol (RIP)

In a Novell internetwork, routers use the Routing Information Protocol (RIP) to exchange routing information. One RIP broadcast packet can contain up to 50 sets of network number information (routes). RIP packets do the following:

- Enable workstations to locate the fastest route to a network by broadcasting a route request
- Allow routers to update internal routing tables by broadcasting a route request
- Allow routers to respond to route requests from workstations and other routers
- Allow routers to perform periodic broadcasts to inform all other routers of the internetwork configuration

- Allow routers to perform broadcasts whenever they detect a change in the internetwork configuration

Figure 5 shows the contents of the IPX-RIP packet.

**Figure 5** IPX-RIP packet

| | |
|---|---|
| Operation | 2 bytes |
| Network number | 4 bytes |
| Hop count | 2 bytes |
| Tick count | 2 bytes |
| Up to 50 sets | |

When RIP packets are encapsulated in the data field of the IPX packet, the packet type field is set to one to indicate that the data field contains RIP information. The destination and source socket fields are set to 453 (hexadecimal) to indicate that the source device is sending a request to the routing process on the destination node via the RIP socket number. This procedure is called peer-to-peer processing. The operation field of an IPX packet indicates whether the packet is a request or response. Request packets can be specific (about specific networks) or general (about all networks on an internetwork); response packets can be specific, general, or informational (whenever a router is first started, shut down, or becomes aware of a routing change in the internetwork).

Routers constantly exchange information with one another to ensure that their routing tables reflect up-to-date changes. IPX routers perform RIP broadcasts at the following times:

- Initial broadcasts of directly connected network segments
- Initial requests to receive routing information from other routers
- Periodic broadcasts (every 60 seconds) of the current list of active network numbers
- Broadcast of changes in the internetwork configuration
- Final broadcast when a router or routing device is brought down

Each RIP broadcast is a local broadcast, addressed so that it is not passed on by the routers that receive it. All Novell routing devices use Split Horizon to advertise RIP and SAP information.

# Service Advertising Protocol (SAP)

The Service Advertising Protocol (SAP) lets service-providing nodes advertise their services and internetwork addresses. Examples of service-providing nodes are file servers, print servers, and queue servers. Through the use of SAP advertisements, SAP agents build and maintain a database of internetworking service information known as a server information table. As servers are initialized, they use SAP to advertise their services. When servers are taken down using the down command, they use SAP to indicate that their services are no longer available.

Each client on the network must first obtain the address of a server before it can access any network services. Clients build their own cache tables for up to seven servers. The SAP packet structure allows the following functions:

- A workstation request for the name and address of the nearest server of a certain type
- A general request by a router for names and addresses of all servers or servers of a certain type
- A response to either a nearest server request or a general request
- A 60-second periodic broadcast by servers or routers
- A broadcast of changed server information

As with RIP packets, the SAP packet is encapsulated in the data fields of the IPX packet and the packet type field is then set to 4 to indicate that the data field contains SAP information. Also as with RIP, the destination and source socket fields are set to 453 (hexadecimal) to indicate peer-to-peer processing. Instead of the network number entries found in a RIP packet, SAP response packets can contain from one to seven server entries, whereas SAP request packets contain only the operations field and server type field.

SAP packets contain an operation field that identifies whether the packet is a request (general or specific) or a response. Two other operations are Get Nearest Server request or response. The SAP packet also identifies the type of service (such as print queue, file server, job server, print server, archive server, including unknown) and includes the server name with network, node, and socket address and number of hops to the server.

Figure 6 shows the contents of the IPX-SAP packet.

**Figure 6** IPX-SAP packet

| | |
|---|---|
| Operation | 2 bytes |
| Service type | 2 bytes |
| Server name | 48 bytes |
| Network address | 4 bytes |
| Node address | 6 bytes |
| Socket address | 2 bytes |
| Hops to server | 2 bytes |
| Maximum of 7 sets | |

SAP broadcasts are similar to RIP broadcasts and include informing the network that a new server is available, general requests for information, responses to general requests, and 60-second broadcasts containing updated SAP information using split horizon.

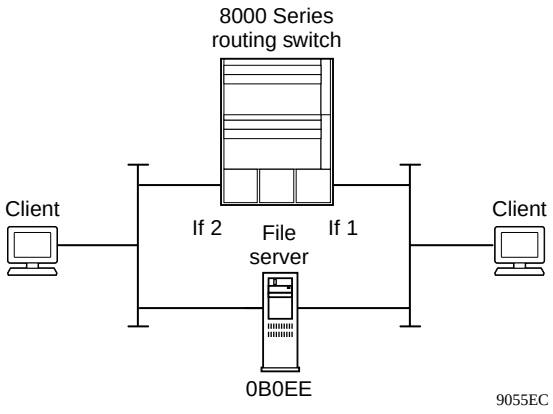
# Broadcast techniques

RIP and SAP broadcasts are sent out from the routers and servers using the best route algorithm and split horizon techniques.

## Best route algorithm

The best route algorithm for Novell routing devices states: If two paths exist, the best route is the one with the least number of ticks. A tick is 1/18th of a second. For local LAN segments with more than 1 MB of bandwidth for each second of bandwidth, the router assumes that the delivery time is one tick. Figure 7 illustrates an example of a best route algorithm.

**Figure 7** Best route algorithm




If the number of ticks is equal, the best route is the one with fewer hops. A hop is counted each time the packet passes through a router.

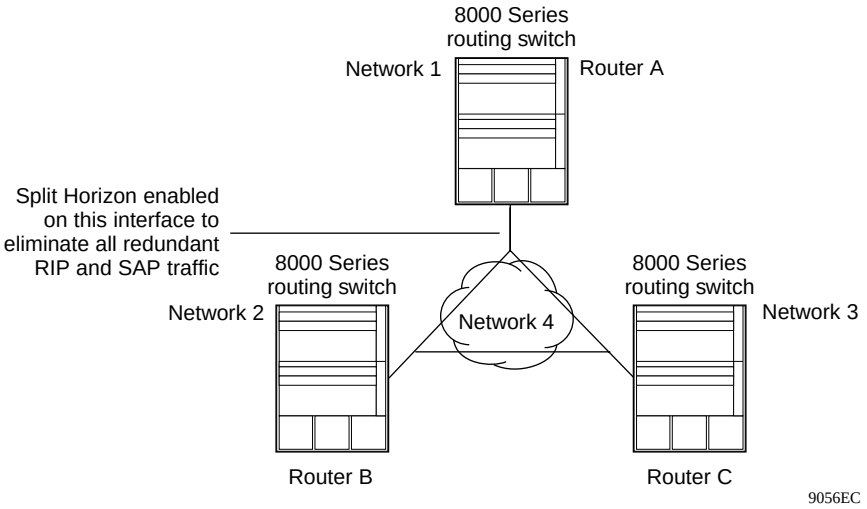
If both ticks and hops are equal, the router chooses the first route. When responding to RIP requests and sending informational RIP broadcasts, routers advertise only the best route.

## Split horizon

When routers are initialized, they build a routing table based on their directly connected interfaces. The file server also builds a routing table, and all devices send routing information and service advertising updates using the best route algorithm and split horizon techniques. Split horizon helps reduce bandwidth and speeds up information distribution by advertising only the routing or service information obtained from other interfaces. Information learned from an interface is never advertised out that same interface.

In Figure 8, split horizon is enabled between router A and network 4 to eliminate redundant RIP and SAP traffic. If split horizon was disabled on that interface, router B would learn all about network 3 and router C would learn all about network 2.

**Figure 8** Split horizon enabled

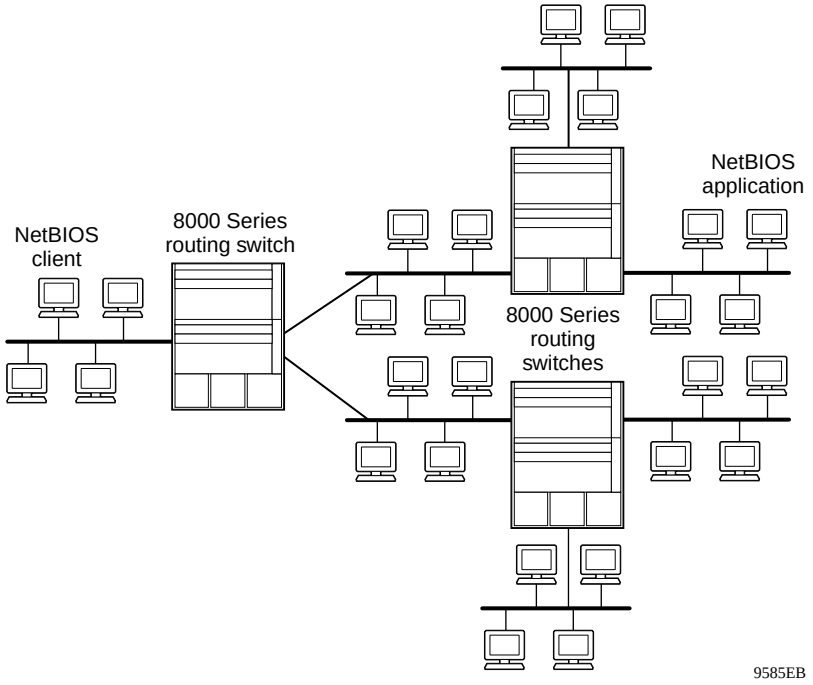



# NetBIOS

The network basic input/output system (NetBIOS) is a connection-less communications protocol jointly developed by Sytek Incorporated and IBM. Novell NetWare provides a NetBIOS emulation package that runs on top of the packet exchange protocol (PEP), which provides a service similar to SAP. After processing NetBIOS calls, PEP sends them to IPX. In the NetWare environment, NetBIOS communicates by establishing a logical connection between two NetBIOS-defined names. NetBIOS sets up a logical channel for higher-layer protocols to use for communication.

Figure 9 shows a typical environment supporting NetBIOS. When the NetBIOS client wants to make a logical connection to the NetBIOS application running on the server, the client sends a NetBIOS name propagation packet (type 14 hexadecimal).

**Figure 9** NetBIOS support in a NetWare environment




The network is established in the following manner:

- Intervening routers examine the transport control field to determine the number of routers traversed and the number of network number fields that contain information.
- Intervening routers compare the network number entries to the network number of the segment where the packet was received. If there is a match, the packet is discarded. If not, the router places the network segment address where the packet arrived into the next available network number field.
- The router increments the transport control field and sends the packet to all directly connected networks not included in the network number fields.
- When the name propagation packet reaches the application server, the server stores the required name and address information and issues a connection number to the client.

- All further communications between the client and server use a standard IPX header with header socket numbers set to 455 hexadecimal to indicate that the packet contains NetBIOS data.

# Static routes

You can configure a static route on each logical IPX interface that the router supports. Using static routes allows you to:

- Direct to an adjacent host all IPX traffic destined to a given network
- Reduce routing traffic by disabling the RIP supply function on a subset of attached interfaces configured with static routes
- Control the size of the routing tables

A static route remains in the routing table until it is deleted or until the router learns a better path based on the selected routing method (hops or RIP ticks).

## Static SAP services

The ability to statically configure services allows services to be advertised locally without the SAP traffic that would be required to learn about the service. A static service is listed in the router SAP table if a route to the network associated with the service exists in the route table. The network associated with the static service must be reachable from the router. A static service remains in the SAP table until you delete it or until the network associated with it becomes unreachable.

## IPX default static routes

By default, the 8600 Switch does not contain a default route address in its route table. Without a default static route, the packet is sent to the switch CPU, where it is dropped unless otherwise configured. You can create a default route when adding a static route by using the value of 0xFFFFFFFE as the target network field. IPX uses the reserved network address 0xFFFFFFFE for default routes.

# IPX RIP/SAP filters

With the IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) protocol route filter policies, you can configure route filters to give you greater control over the learning and announcing of IPX RIP/SAP routes from one area of an IPX internetwork to another. Using route filters helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by restricting a user's view of other networks.

You can configure inbound and outbound route filters on a per-interface basis, instructing the interface to advertise, accept, or drop filtered IPX RIP/SAP packets. The action parameter that you define for the filter determines whether the router advertises, accepts, or drops IPX RIP/SAP routes that match the filter.

A Service Advertisement Protocol (SAP) filter is a pattern for matching a service name or service network. The 8000 Series Switch software scans incoming and outgoing SAP packets to see whether certain fields in the packet match the filter. When you configure the filter, you can specify what the 8600 Switch does with the services in the packet when it finds a match. You can use SAP filters to control the size of resident SAP service tables and reduce bandwidth usage on your network due to SAP broadcast overhead.

You can also create SAP filters as a security mechanism to restrict a user's view of services located elsewhere on the network. As a result, you can tailor SAP filters to your site requirements, improving network security by controlling access and preserving bandwidth by limiting the SAP packet traffic.

IPX RIP/SAP route filtering is accomplished by creating and maintaining Network, Service, and Policy tables.

## Announce/Out policy implementation

The policy implementation consists of two parts:

- Selecting a matching policy
- Applying a policy

### Selecting a matching policy

Matching criteria are applied to select a policy that suits the given route/service. Select the policy group from the Out-policy table for the interface at which the packet is to be sent. Apply matching criteria in each of the policy in the selected policy group. A policy is considered as a possible match to be used to announce or ignore the route/service only if the route satisfies all the matching criteria in the policy.

The matching parameters for announce policy are:

- Enable - The Policy should be enabled.
- Route Source - The route source of the RIP/SAP Packet should match the route source of the policy or the route source of the policy is 'any'.
- Network list - Considered match if the network ID in the RIP/SAP PDU falls in the range specified by the policy or the list is empty.
- Service List - Considered match if the service type and service name of the SAP PDU matches one of the lists of service range and service name specified in policy or the list is empty. For service name the ‘*’ is used for wildcard matching. '*' is supported only at the end of the service name. Also, matching is CASE SENSITIVE.

If more than one policy matches all the above criteria, then the policy with lower sequence number will be taken as best match policy.

If the matching process fails to produce a best match, the default behavior (to announce the route) is applied.

### Applying a policy

The packet is announced only if the action field of best match policy is 'permit'. Otherwise, the packet is dropped.

For RIP, the ticks of the route is updated with the ticks field of matching policy and the hops of the route is updated with the hops field of the matching policy. Both the hop and tick fields are updated irrespective of the value of routing method.

For SAP, the hop field is updated with the hops field of the matching policy. The route is updated only if the hops or ticks value of the matching policy is not zero.

## Accept/In policy implementation

The policy implementation consists of two parts:

- Selecting a matching policy
- Applying a policy

### Selecting a matching policy

Matching criteria are applied to select a policy that suits the given route/service. Select the policy group from the In-policy table for the interface at which the packet is received. Apply matching criteria in each of the policy in the selected policy group. A policy is considered as a possible match to be used to accept or ignore the route/service if and only if the route satisfies all the matching criteria in the policy.

The matching parameter for announce policy are:

- Enable: The Policy should be enabled.
- Network list: Considered match if the network ID in the RIP/SAP PDU falls in the range specified by the policy or the list is empty.
- Service List: Considered match if the service type and service name of the SAP PDU matches one of the lists of service range and service name specified in policy or the list is empty. For service name the ‘*’ is used for wildcard matching. '*' is supported only at the end of the service name. Also, matching is case sensitive.

If more than one policy matches all the above criteria, then the policy with lower sequence number will be taken as best match policy.

If the matching process fails to produce a best match, the default behavior (to accept the route) is applied.

### Applying a policy

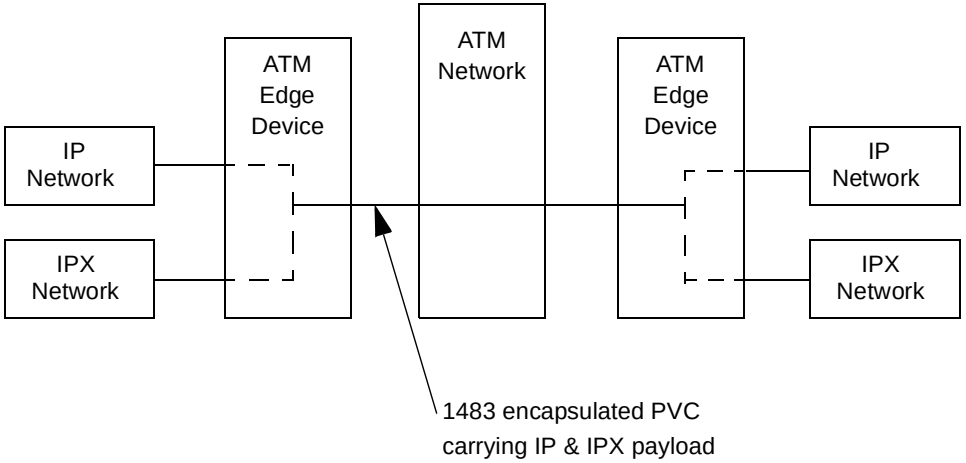
The packet is accepted only if the action field of best match policy is 'permit'. Otherwise, the packet is dropped.

## IP/IPX over single ATM PVC

The IP/IPX over single PVC feature allows you to create a muxIpIpx ELAN. A muxIpIpx ELAN multiplexes only IP and IPX protocols over a single ATM PVC through 1483 LLC encapsulation. The muxIpIpx ELAN does not support bridging.

You can configure a muxIpIpx ELAN on a PVC with LLC/SNAP encapsulation. RFC 1483 LLC/SNAP encapsulation is required to multiplex IP and IPX protocols over a single ATM PVC (Figure 10).

**Figure 10** MuxIpIpx ELAN




You can configure up to 200 PVCs as muxIpIpx ELAN per 8000 system. A 8000 system supports up to 500 VLANs with routed interfaces, where one ELAN is associated with one VLAN. Therefore, if a you configure 200 muxIpIpx ELANs, then 300 VLANs with routed interfaces remain available.

For more information about the 8000 Series Switch IP/IPX over single PVC protocol features, concepts and terminology, refer to *Using the 8672ATME and 8672ATMM modules*.

# Chapter 2
# Configuration considerations and limitations

This chapter describes configuration limitations and interoperability issues that you should consider when configuring IPX.

## Changing the IPX forwarding state

Changing the state on IPX forwarding with a large number of IPX routes may spike the CPU to 100% utilization.

## LLC encapsulation and gigabit Ethernet ports

On a Passport 8000 Series switch, excluding the Passport E-modules, IPX translation between LLC encapsulation and any other encapsulation is not supported on gigabit Ethernet ports.

# Chapter 3
# Configuring IPX using Device Manager

This chapter describes using Device Manager to configure the Internet Packet Exchange (IPX) protocol, the Novell Inc. adaptation of the Xerox Network System (XNS) protocol.

Implementation of IPX on the 8600 Switch supports the following four Ethernet frame formats:

- Ethernet II
- 802.2-LLC
- 802.3-RAW
- 802.3-SNAP

Frame translations from one frame format to another are supported, but the IPX host format must match the defined protocol frame format of the interface to which the host is connected.

An 8600 Switch supports IPX as routed VLANs, if IPX routing is enabled on the VLAN.

The following topics are discussed:

# Configuring and managing IPX routing

The following topics describe using Device Manager to manage and configure IPX routing on the switch:



## Settings globals for IPX routing circuits and routing method

Use the IPX Global tab to globally enable or disable IPX routing on the defined IPX circuit.

To enable IPX circuits globally:

1 From the Device Manager menu bar, choose IPX Routing > IPX.

The IPX dialog box opens with the Globals tab displayed (Figure 11).

**Figure 11** IPX dialog box—Globals tab


2 Select RoutingEnable (the default is disabled).

3 Click Apply.

Table 1 describes the Globals tab field.

**Table 1** Globals tab field

| Field | Description |
|---|---|
| RoutingEnable | Enables IPX routing on the interface. |
| RoutingMethod | Enables the Routing Method to use ticks or hops.<br>This field sets the value of the routing method to ticks or hops and is used to select the best route. If the routing method is hops, then the route with fewer hops will be taken as best route and if the routing method is tick, then the route with fewer ticks will be used.<br>The default is ticks. |

## Globally enabling the IPX routing method

Use the IPX Global tab to globally enable the IPX routing method.

To enable the IPX routing method:

1. From the Device Manager menu bar, choose IPX Routing > IPX.

   The IPX dialog box opens with the Globals tab displayed (Figure 11).
2. Select RoutingMethod.
3. Click Apply.

## Configuring the IPX interface

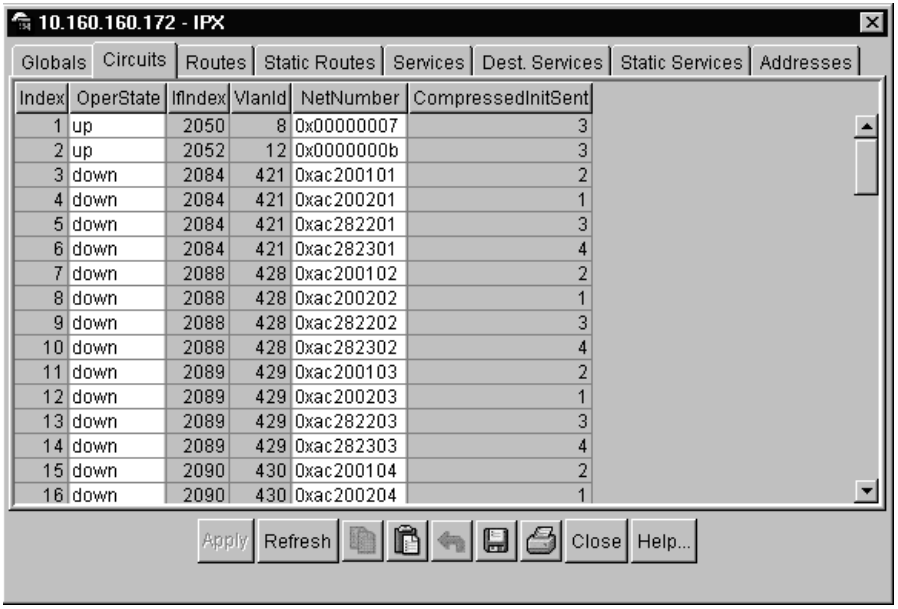
To configure the IPX interface:

1. From the Device Manager menu bar, choose IPX Routing > IPX.

   The IPX dialog box opens with the Globals tab displayed (Figure 11).
2. Click the Circuits tab.

   The Circuits tab opens (Figure 12). The term “circuit” refers to the IPX network interface.

**Figure 12** IPX dialog box—Circuits tab




3 In the OperState field, use the pull-down menus to select the options.

4 In the IfIndex field, use the pull-down menus to select the options.

5 In the NetNumber field, use the pull-down menus to select the options.

6 Click Apply.

Table 2 describes the fields in the Circuit tab.

**Table 2** Circuit tab fields

| Field | Description |
|---|---|
| Index | The index number automatically assigned when the interface was created. |
| OperState | Select down or up; sleeping indicates it is set for up, but there are no connections to the interface. The normal state is up. |
| IfIndex | VLAN interface index; not used in IPX. |
| CompressedInitSent | The number of compressed packets sent. |
| NetNumber | The IPX circuit network number in an octet string: xx.xx.xx.xx. |

**Note:** For port-based VLANs, an IPX circuit is “on” only when a link is up in the VLAN. For protocol-based VLANs, a circuit is “on” only after the VLAN receives a packet of the specified protocol type.

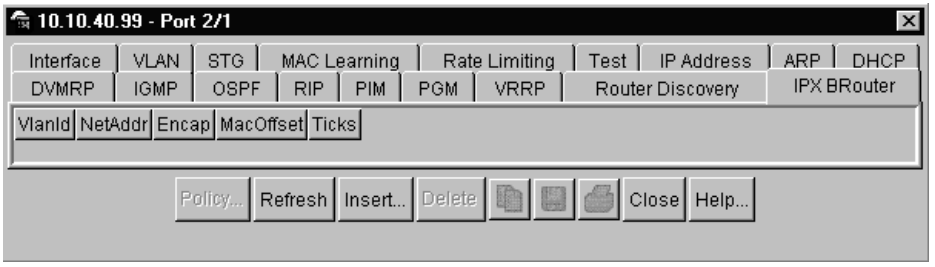
## Creating IPX brouter interface on a port using Device Manager

To configure the IPX brouter interface:

1. Select a port or ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed (Figure 13).

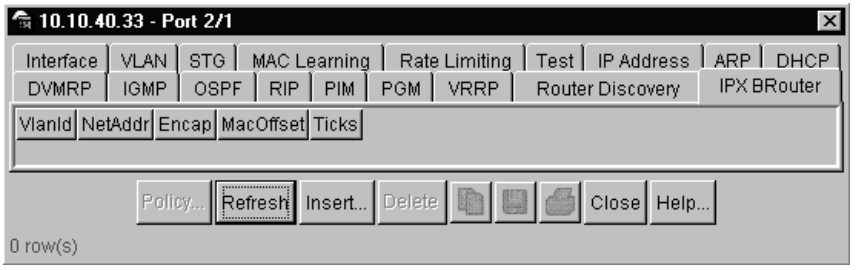
**Figure 13** Port dialog box—Interface tab




3. Click the IPX BRouter tab.

   The IPX BRouter tab opens (Figure 14).

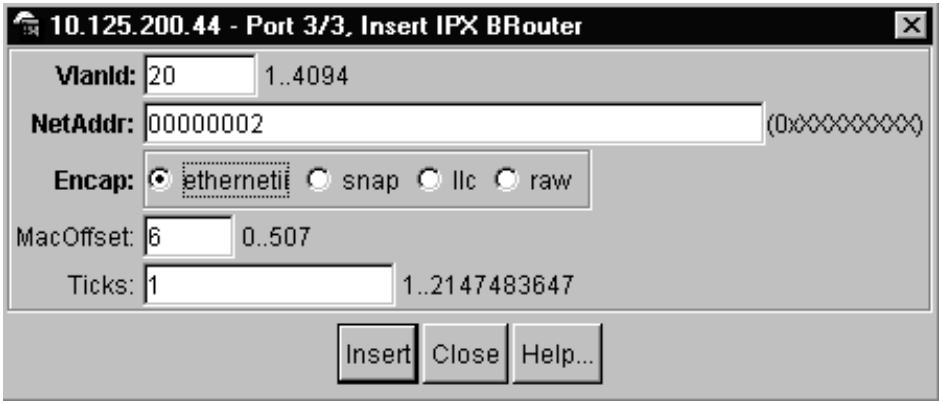
**Figure 14** Port dialog box—IPX BRouter tab



4 Click Insert.

The Port, Insert IPX BRouter dialog box opens (Figure 15).

**Figure 15** Port, Insert IPX BRouter dialog box




5 In the VlanId text box, type a valid VLANId.

6 In the NetAddr text box, type the network address.

7 Select an encapsulation method.

8 In the MacOffset text box, type a valid MacOffset number.

9 In the Ticks text box, type the number of ticks.

10 Click Insert.

Table 3 describes the Port, Insert IPX BRouter tab fields.

**Table 3** Port, Insert IPX BRouter tab fields

| Field | Description |
|---|---|
| VlanId | The VLAN id. |
| NetAddr | The IPX network address value. |
| Encap | The encapsulation method. |

**Table 3** Port, Insert IPX BRouter tab fields

| Field | Description |
|---|---|
| MacOffset | The mac_offset is a optional parameter that allows you to manually change the default MAC address for a logical or physical interface. Value is an integer from 0 to 507. The default is the next available value. |
| Ticks | The value that determines the best route for the IPX routed VLAN. The lower the tick value the better the route. Enter a tick value with the range of 1 to 32767. If you enter a value larger than 32767, an error message will display alerting you that the value has been changed to 32767, and a log message is generated. |

# Configuring IP/IPX over single PVC

This section describes how to use Device Manager to configure the following IP/IPX over single PVC options:

## *Prerequisites*

Before you can configure an IP/IPX VLAN, you must:

- Configure a VLAN with IP and IPX configured. The IPX encapsulations should match the ATM 1483 ELAN encapsulation.
- Configure the ATM port as a member of that VLAN.
- Configure the ATM PVC.

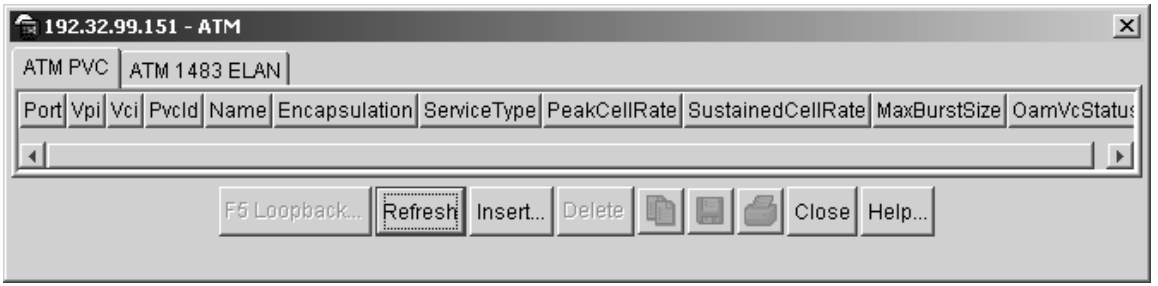
**Note:** Choose an IP ELAN over a muxIpIpx ELAN for IP protocol only, since IP ELAN offers faster throughput. Likewise, choose an IPX ELAN over a muxIpIpx ELAN for IPX protocol only. Make sure that the IPX encapsulations match the ATM 1483 ELAN encapsulation.

To configure IP/IPX over single PVC:

**1** From the Device Manager menu bar, choose Edit > ATM.

The ATM dialog box opens with the ATM PVC tab displayed (Figure 16).

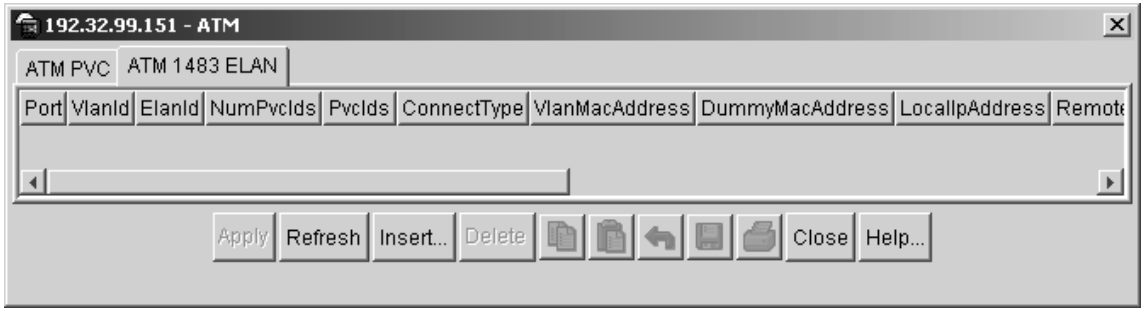
**Figure 16** ATM dialog box — ATM PVC tab




**2** Click the ATM 1483 ELAN tab.

The ATM 1483 ELAN tab opens (Figure 17).

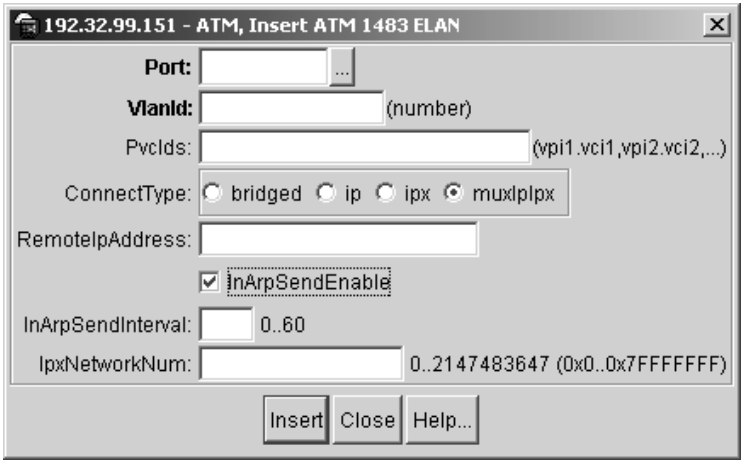
**Figure 17** ATM dialog box — ATM 1483 ELAN tab




**3** Click Insert.

The ATM, Insert ATM 1483 ELAN dialog opens (Figure 18).

**Figure 18** ATM, Insert ATM 1483 ELAN dialog box




**4** Select a port.

**5** Enter an Vlanid number.

**6** Enter a PvcIds.

**7** Select a ConnectType of muxipipx.

**8** Enter a remote IP address.

**9** If desired, select InArpSendEnable.

**10** Specify an InArpSend Interval.

**11** Enter an IPX network number.

**12** Click Insert.

**13** Click Close.

Table 4 describes the ATM 1483 tab fields.

**Table 4** ATM, Insert ATM 1483 ELAN fields

| Field | Description |
|---|---|
| Port | Specifies the number of the port for which you are configuring the ATM PVC. |
| VlanId | Specifies the vlan id you created. |
| PvcIds | Displays the PVC ID. |
| ConnectType | NEED INFO |
| RemoteIpAddress | NEED INFO |
| InArpSendEnable | Enables InArpSend. |
| InArpSendInterval | Specifies the InArpSend interval. |
| IpxNetworkNum | The IPX network number. |

## Changing parameters on either an IP or an IPX interface

If you change parameters on either an IP or an IPX interface (such as the IPX encapsulation in the IPX interface) on a VLAN associated with an ELAN, you must:

1. Delete the ELAN associated with this VLAN.

   When you delete a VLAN associated with an ELAN, the associated ELAN is automatically removed.
2. Delete the routed interface to be changed.
3. Re-create the routed interface with new parameters.
4. Re-create the ELAN.

## Viewing the IPX routing table

To view the IPX routing table:

1 From the Device Manager menu bar, choose IPX Routing > IPX.

The IPX dialog box opens with the Globals tab displayed (Figure 11).

2 Click the Routes tab.

The Routes tab opens (Figure 19).

**Figure 19** IPX dialog box—Routes tab


Table 5 describes the fields in the Routes tab.

**Table 5** Routes tab fields

| Field | Description |
|---|---|
| NetNum | The destination IPX network number for this route. |
| Protocol | The routing protocol through which this route was learned (local or RIP). |
| Ticks | The number of ticks to the destination network. A tick is 1/18th of a second. |
| HopCount | The number of hops (passes through a router) required to arrive at the destination network. |
| NextHopCircIndex | The IPX circuit index of the next hop router. |
| NextHopNICAddress | The network interface card (NIC) address of the next hop router. |
| NextHopNetNum | The network number of the next hop router. |

## Configuring and viewing static routes on an interface

You can display the current static routes and specify a route for an interface. In addition, you can configure a static route on each logical IPX interface.

To configure static routes:

1. From the Device Manager menu bar, choose IPX Routing > IPX.

   The IPX dialog box opens with the Globals tab displayed (Figure 11).

2. Click the Static Routes tab.

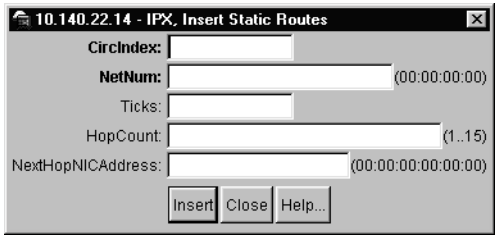
   The Static Routes tab opens (Figure 20).

**Figure 20** IPX dialog box—Static Routes tab


3. Click Insert.

   The IPX, Insert Static Routes dialog box opens (Figure 21).

**Figure 21** IPX, Insert Static Routes dialog box




4. In the CircIndex text box, type the IPX circuit index number.
5. In the NetNum text box, type IPX network number.
6. In the Ticks text box, type the number of ticks.

7 In the HopCount text box, type the number of hops.

8 In the NextHopNICAddress text box, type the number of next hops.

9 Click Insert.

Table 6 describes the IPX, Insert Static Routes tab fields.

**Table 6** IPX, Insert Static Route tab fields

| Field | Description |
|---|---|
| CircIndex | The IPX circuit index number that corresponds to the network number. |
| NetNum | The IPX network number of the destination network. To create a default route, use the value FF:FF:FF:FE. |
| Ticks | The number of ticks allowed to reach the destination network. A tick is 1/18th of a second. |
| HopCount | The number of hops (passes through a router) allowed to reach the destination tab (1–15). |
| NextHopNICAddress (insert dialog box only) | The next hop NIC address. |

## Viewing IPX services

You can view the IPX services available on the network. This information is also displayed in the Dest. Services (destination services) tab (Figure 23) and the Static Services tab (Figure 24), with different sort conditions.

To view the IPX services:

1 From the Device Manager menu bar, choose IPX Routing > IPX.

The IPX dialog box opens with the Globals tab displayed (Figure 11).

2 Click the Services tab.

The Services tab opens (Figure 22).

**Figure 22** IPX dialog box—Services tab

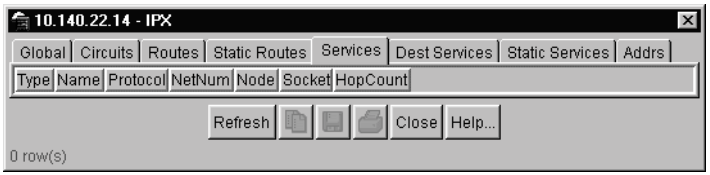



Table 7 defines the Services tab fields.

**Table 7** Services tab fields

| Field | Description |
|---|---|
| Type | Type of service provided (in hex). |
| Name | The name of the service (48 byte field). |
| Protocol | The protocol through which this service was learned (RIP or static). This field is a display field only. |
| NetNum | The IPX network number where this service is available. |
| Node | The 6-byte node address. The node and netnum fields correspond to the IPXhost parameter in the CLI. |
| **Note:** The NetNum and Node make up the IPX host address where the service is available. | |
| Socket | The socket address of the service (in hex). |
| HopCount | The number of intermediate networks that must be passed through to reach the server. |

## Viewing IPX services by destination network number

You can view IPX services information organized by destination network number. This view lists the types of services available at each network destination.

To view IPX services information by destination network number:

1. From the Device Manager menu bar, choose IPX Routing > IPX.

   The IPX dialog box opens with the Globals tab displayed (Figure 11).

2. Click the Dest. Services tab.

   The Dest. Services tab opens (Figure 23).

**Figure 23** IPX dialog box—Dest. Services tab

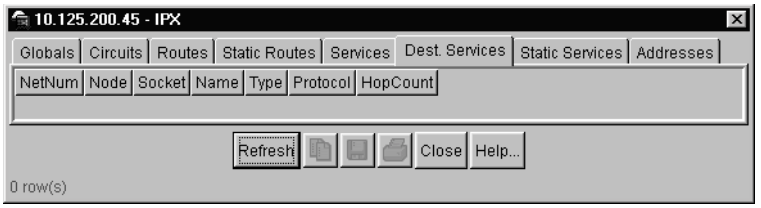



Table 8, describes the Dest. Services tab fields.

**Table 8** Dest. Services tab fields

| Field | Description |
|---|---|
| Type | Type of service provided (in hex). |
| Name | The name of the service (48 byte field). |
| Protocol | The protocol through which this service was learned (RIP or static). This field is a display field only. |
| NetNum | The IPX network number where this service is available. |
| Node | The 6-byte node address. The node and netnum fields correspond to the IPXhost parameter in the CLI. |
| **Note:** The NetNum and Node make up the IPX host address where the service is available. | |
| Socket | The socket address of the service (in hex). |
| HopCount | The number of intermediate networks that must be passed through to reach the server. |

## Viewing IPX services by circuit index number

You can view IPX services information organized by circuit index number. This view lists the types of services available at each network destination.

To view IPX service information, organized by circuit index number:

1 From the Device Manager menu bar, choose IPX Routing > IPX.

The IPX dialog box opens with the Globals tab displayed (Figure 11).

**2** Click the Static Services tab.

The Static Services tab opens (Figure 24).

**Figure 24** IPX dialog box—Static Services tab


**Note:** To insert a static service, a route to that service must exist (either statically or dynamically).

Table 9 describes the fields in the Static Services tab.

**Table 9** Static Services tab fields

| Field | Description |
|---|---|
| CircIndex | The circuit index number corresponding to the network number. |
| Name | The name of the service (48 byte field). |
| Type | The type of service provided (in hex). |
| NetNum | The IPX network number where this service is available. |
| Node | The 6-byte node address. The Node and NetNum fields correspond to the IPX host parameter in the CLI. |
| **Note**: The NetNum and Node make up the IPX host address where the service is available. | |
| Socket | The socket address of the service (in hex). |
| HopCount | The number of intermediate networks that must be passed through to reach the server. |

## Viewing locally configured IPX addresses

To view a summary of locally configured IPX addresses:

1. From the Device Manager menu bar, choose IPX Routing > IPX.

   The IPX dialog box opens with the Globals tab displayed (Figure 11).

2. Click the Addresses tab.

   The Addresses tab opens (Figure 25).

**Figure 25** IPX dialog box—Addresses tab

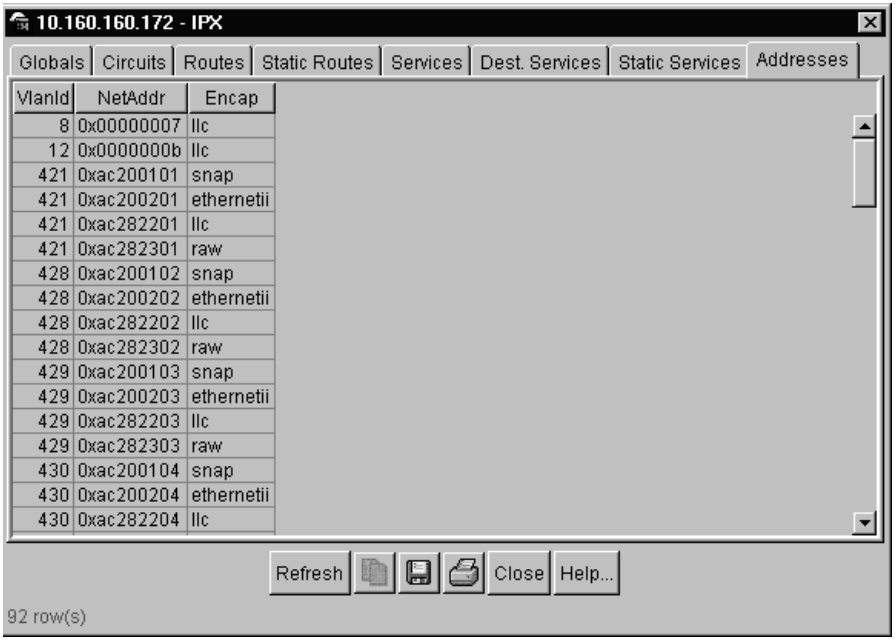


Table 10 describes the Addresses tab fields.

**Table 10** Addresses tab fields

| Field | Description |
|---|---|
| VlanId | The VLAN ID. |
| NetAddr | The network address of the VLAN. |
| Encap | The encapsulation method used:<br>• Ethernet II<br>• snap: 802.3<br>• llc: 802.2<br>• raw: 802.3 raw |

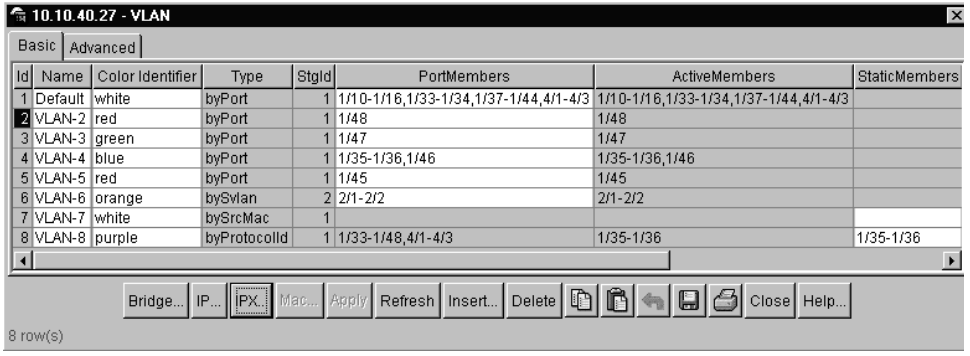
## Creating an IPX circuit on a VLAN

To create a VLAN that defines the ports in an IPX circuit:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed (Figure 24).

**Figure 26** VLAN dialog box—Basic tab

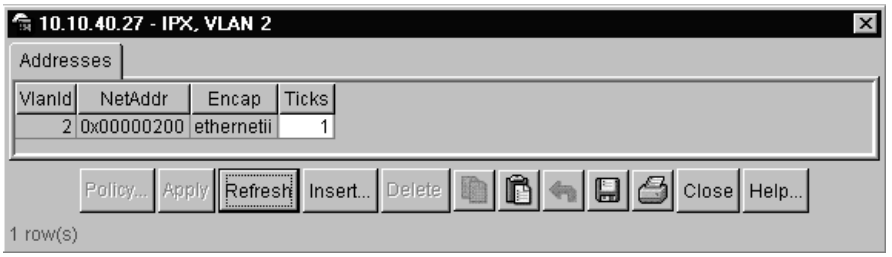


2 Select a VLAN.

3 Click IPX.

The IPX, VLAN dialog box opens (Figure 27).

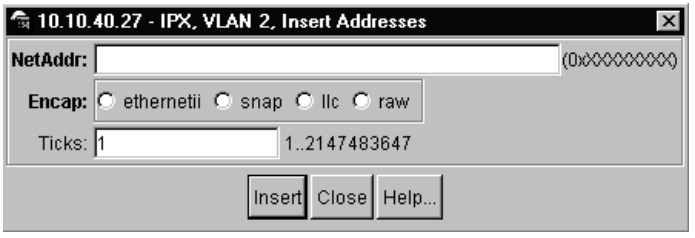
**Figure 27** IPX, VLAN dialog box




4 Click Insert.

The IPX, VLAN, Insert Addresses dialog box opens (Figure 28).

**Figure 28** IPX, VLAN, Insert Addresses dialog box




5 In the NetAddr field, type the IPX network address.

6 In the Encap field, select the encapsulation method (ethernetii, snap, llc, or raw).

The VLAN must be either protocol based (Ethernet2, SNAP, LLC, or RAW) or port based:

- For a protocol-based VLAN, this method must match the selected protocol.
- For a port-based VLAN, select the preferred frame format.

7 Click Insert.

# Editing RIP routing

This section describes using Device Manager to configure and display IPX RIP circuit and interface information.

The following sections describe using Device Manager to manage and configure IPX routing on the switch:

- "Viewing and editing RIP circuits," next
- "Viewing and editing RIP interface" on page 62

## Viewing and editing RIP circuits

To edit RIP routing circuits:

➔ From the Device Manager menu bar, choose IPX Routing > RIP.

The IPX_RIP dialog box opens with the Circuit tab displayed (Figure 29).

**Figure 29** IPX,_RIP dialog box—Circuit tab

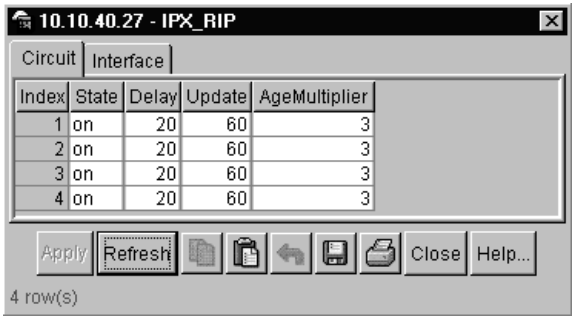


Table 11 describes the IPX_RIP Circuit tab fields.

**Table 11** IPX_RIP dialog box—Circuit tab fields

| Field | Description |
|---|---|
| Index | The index number assigned to the interface. |
| State | The current state of RIP on the interface: on, off, auto-on, auto-off. The default is off. |
| Delay | Frame rate. Default is 20 frames per second; delay time range is 1 to 1000 ms. |
| Update | Time period (in seconds) after which periodic updates of the current list of active network numbers is sent. Default is 60 seconds with a range of 1 to 2147483647. |
| AgeMultiplier | The hold multiplier timing parameter. Default is 3 with a range of 1 to 2147483647. |

## Viewing and editing RIP interface

Use the IPX_RIP dialog box to view and edit routing information protocol (RIP) parameters.

To configure RIP on the interface:

1. From the Device Manager menu bar, choose IPX Routing > RIP.

   The IPX_RIP dialog box opens, with the Circuit tab displayed (Figure 29).

2. Click Interface

   The Interface tab is displayed (Figure 30).

**Figure 30** IPX_RIP dialog box—Interface tab

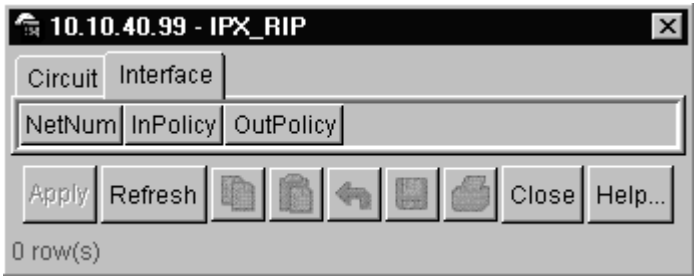


Table 12 describes the RIP interface fields.

**Table 12** RIP dialog box—interface fields

| Field | Description |
|---|---|
| NetNum | The interface to which the policy is applied |
| InPolicy | The In policy name |
| OutPolicy | The Out policy name |

# Editing SAP routing

This section describes using Device Manager to configure and display IPX SAP circuit and interface information.

The following sections describe using Device Manager to manage and configure IPX routing on the switch:

- "Viewing and editing SAP circuits," next
- "Viewing and editing SAP interface" on page 65

## Viewing and editing SAP circuits

To edit service advertisement protocol (SAP) parameters:

➔ From the Device Manager menu bar, choose IPX Routing > SAP.

The IPX_SAP dialog box opens, with the Circuit tab (Figure 31).

**Figure 31** IPX_SAP dialog box—Circuit tab

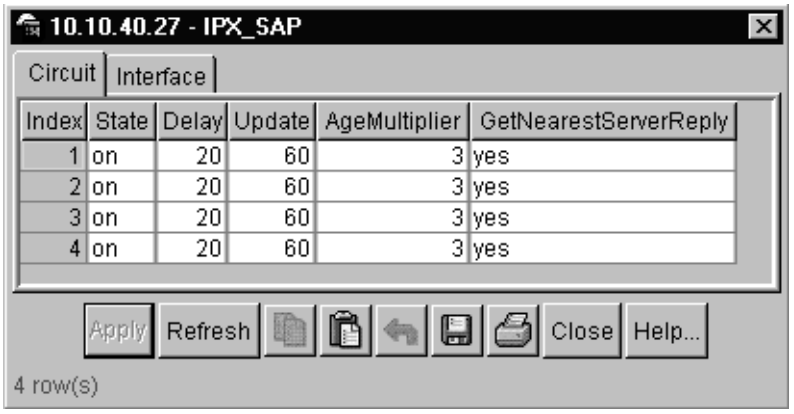



Table 13 describes the fields in the IPX_SAP Circuit tab.

**Table 13** IPX_SAP dialog box—circuit fields

| Field | Description |
|---|---|
| Index | The index number of the server. |
| State | The current state of SAP on the interface: on, off, auto-on, auto-off. The default is off. |
| Delay | Frame rate. Default is 20 frames per second; delay time range is 1 to 1000 ms. |
| Update | Time period (in seconds) after which periodic updates of the current list of active network numbers is sent. Default is 60 seconds with a range of 1 to 2147483647. |
| AgeMultiplier | The hold multiplier timing parameter. Default is 3 with a range of 1 to 2147483647. |
| GetNearestServerReply | Yes or No to enable or disable server replies. |

## Viewing and editing SAP interface

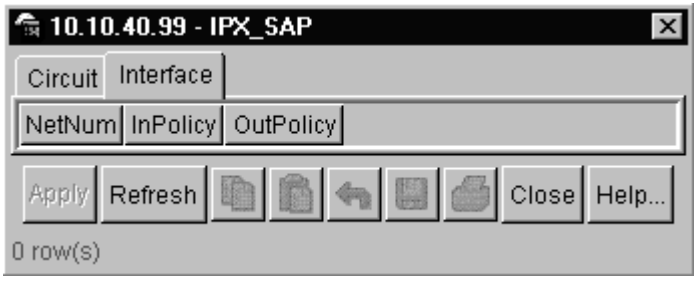
Use the IPX_SAP dialog box interface tab to view and edit the service advertisement protocol (SAP) parameters.

To open the IPX_SAP dialog box interface tab:

1 From the Device Manager menu bar, choose IPX Routing > SAP.

The IPX_SAP dialog box opens, with the Circuit tab displayed (Figure 31).

**Figure 32** IPX_SAP dialog box—Interface tab




2 Click Interface.

Table 14 describes the IPX_SAP dialog box—Interface fields.

**Table 14** IPX_SAP dialog box—Interface fields

| Field | Description |
|---|---|
| NetNum | The interface to which the policy is applied. |
| InPolicy | The In policy name. |
| OutPolicy | The Out policy name. |

# Chapter 4
# IPX RIP/SAP Route Filter Policy Features

With the IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) protocol route filter policies, you can configure route filters to give you greater control over the learning and announcing of IPX RIP/SAP packets from one area of an IPX internetwork to another. Using route filters helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by restricting a user's view of other networks.

This chapter describes IPX RIP/SAP route policy filter features for the 8000 Switch Series, and includes the following topics:



## Configuring the Network list

The network list table contains a set of IPX network addresses that can be used by both RIP and SAP policies. Each entry in the table represents either a single IPX network address or a range of IPX network addresses. Each set of IPX network addresses is represented by a unique Id and name. There is a 1-to-1 relationship between the network list Id and name.

The Network List Table is used when doing a match on the *match-netlist* field in the route policy table.

## Defining the Network list

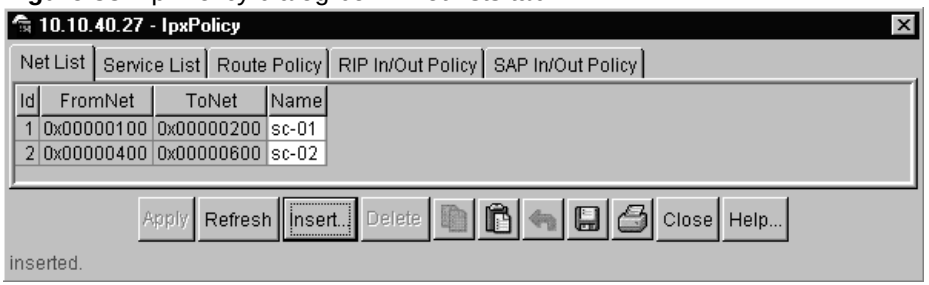
A network list stores a set of IPX network addresses. Each entry represents 0 or more IPX network addresses. An IPX range can be one or more network list entries.

To define network lists:

1 From the Device Manager menu bar, choose IPX Routing > Policy.

The IpxPolicy dialog box opens with the Net List tab displayed (Figure 33).

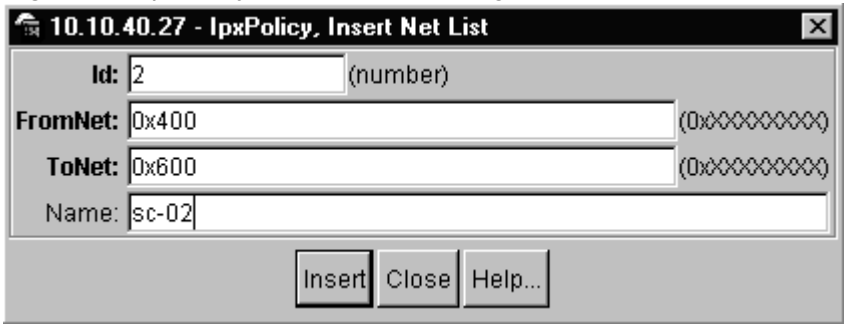
**Figure 33** IpxPolicy dialog box—NetLists tab




2 Click Insert to add a network list.

The IpxPolicy, Insert Net List dialog box opens (Figure 34).

**Figure 34** IpxPolicy, Insert Net List dialog box




3 Enter information.

4 Click Insert.

The new entry appears in the Net List tab of the IpxPolicy dialog box (Figure 33).

Table 15 describes the Net List tab fields.

**Table 15** IpxPolicy dialog box—Net List tab fields

| Field | Description |
|---|---|
| Id | Unique ID to represent the entry in the table. |
| FromNet | IPX Network Address. |
| ToNet | Used to specify a range of IPX network addresses. This is an optional parameter. The default value is NetAddr. In that case the entry refers to a single IPX network. |
| Name | Name of the list. |

# Configuring the Service list

A service list contains a set of IPX service information. Each IPX service information contains a set of service type and service name. Service Name is optional. The default value is '*' which is to match for all service names. Also '*' can be used for wildcard matching for service name. This is supported only at the end of the name. Each IPX service list entry is represented by a unique name and an Id. There is a one-to-one relation between service list name and ID.

## Defining a Service Lists

To define service lists:

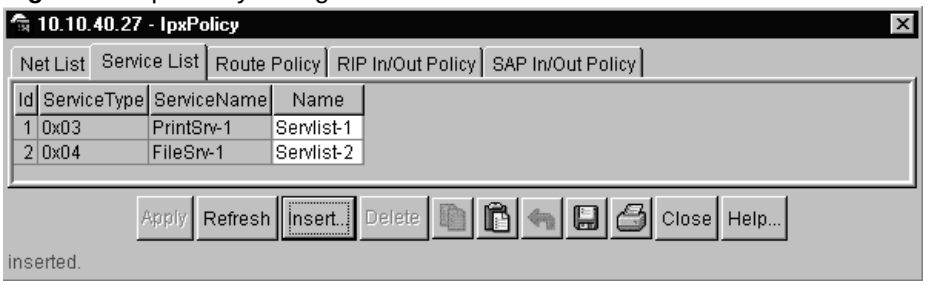
1. From the Device Manager menu bar, choose IPX Routing > Policy.

   The IpxPolicy dialog box opens with the Net List tab displayed (Figure 33).

2. Click the Service List tab.

   The Service List tab opens (Figure 35).

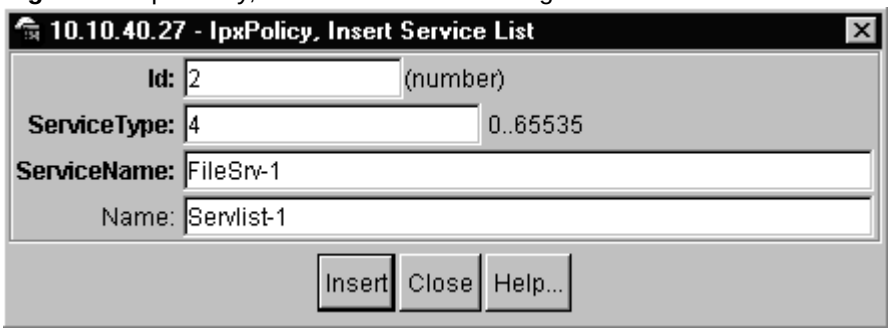
**Figure 35** IpxPolicy dialog box—Service List tab




**3** Click Insert.

The IpxPolicy, Insert Service List dialog box opens (Figure 36).

**Figure 36** IpxPolicy, Insert Service List dialog box




**4** Enter information.

**5** Click Insert.

The new entry appears in the Service List tab of the IpxPolicy dialog box (Figure 35).

Table 16 describes the Service List tab fields.

**Table 16** IpxPolicy dialog box—Service List tab fields

| Field | Description |
|---|---|
| Id | Unique number to represent the entry. |
| ServiceType | Service type information. |
| ServiceName | Service name information. If not entered, '*' is taken as default value. This is matched to any service name. Also, '*' can be used to match wildcard characters. This is supported only at the end of the service name. For example: Printer* will be matched to Printer1, Printer2, Printer*n*. Service Name matching is case-sensitive. |
| Name | Name of the list. |

# Configuring IPX route policies

This section describes using Device Manager to configure IPX route policy features supported on 8000 Switch Series. The accept and announce policies are configured for the 8000 Series Switch based on the selected protocol (SAP or RIP).

This section includes the following topics:

## Configuring a route policy

A policy table contains a set of policy groups that can be used by both RIP and SAP protocols. Each policy group can contain a number of policies with different MATCH & SET parameters. Each policy group is identified with a unique name. The policy name is mapped into a unique ID. There is a one-to-one relation between policy group name and policy group Id. Each policy within a group is identified with a unique sequence number. Different policy groups can have same sequence number, whereas within a group the sequence number must be unique.

## Defining a route policy

To define a route policy:

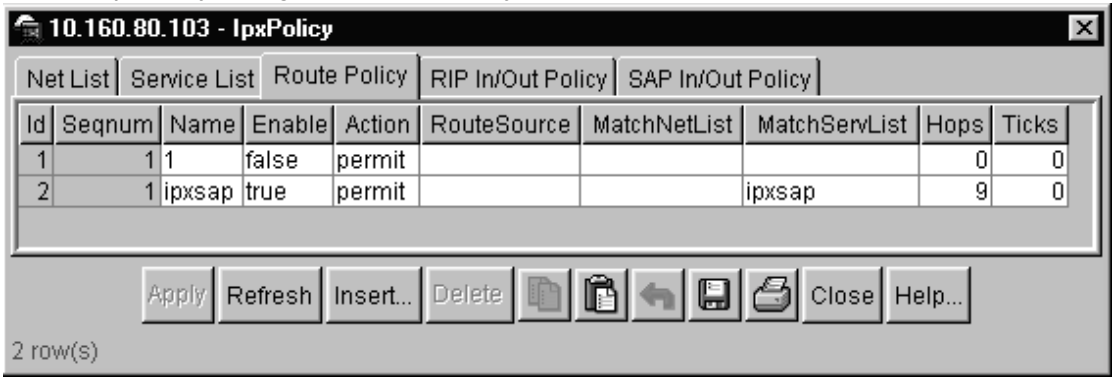
1. From the Device Manager menu bar, choose IPX Routing > Policy.

   The IpxPolicy dialog box opens with the Net List tab displayed (page 68).

2. Click the Route Policy tab.

   The Route Policy tab opens (Figure 37).

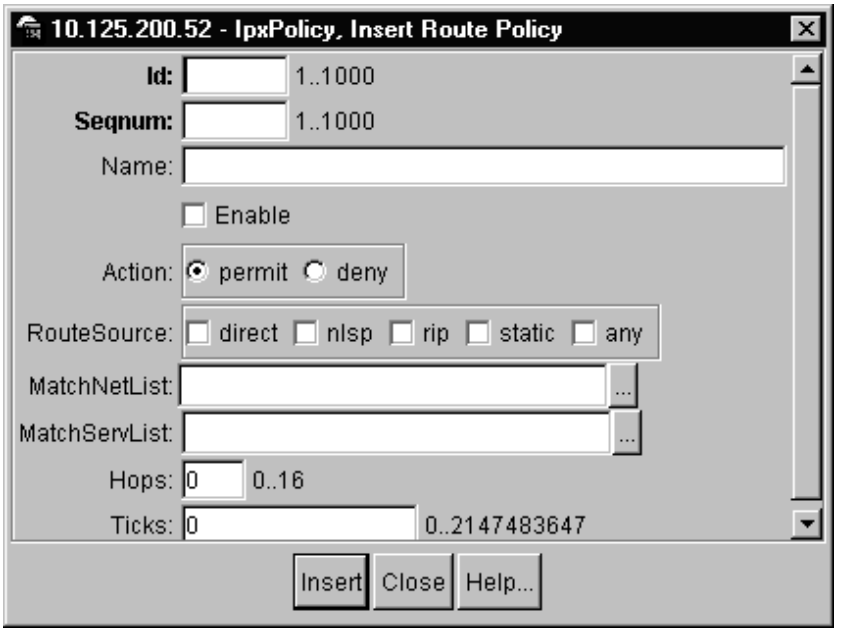
**Figure 37** IpxPolicy dialog box—Route Policy tab




3. Click Insert to add a route policy.

   The IpxPolicy, Insert Route Policy dialog box opens (Figure 38).

**Figure 38** IpxPolicy, Insert Route Policy dialog box




**4** Enter information.

**5** Click Insert.

The new entry appears in the Route Policy tab of the IpxPolicy dialog box (Figure 37).

Table 17 describes the Route Policy tab fields.

**Table 17** IpxPolicy dialog box—Route Policy tab fields

| Field | Description |
|---|---|
| Id | Displays the unique number that identifies the route policy group. |
| Seqnum | Displays a second number that identifies a specific policy within the route policy group (grouped by Id). This field allows you to specify different match and set parameters and an action. You can also use this field to resolve a tie between 2 matching policies. The policy with the lower sequence number is used. |
| Name | Allows you to modify the unique name that represents the policy group. There is a one-to-one relationship between Id and Name. |

**Table 17** IpxPolicy dialog box—Route Policy tab fields (continued)

| Field | Description |
|---|---|
| Enable | Allows you to modify whether the policy is enabled (true) or not (false). If disabled, the policy should not be used.<br>The default value is *false* (disabled). |
| Action | Allows you to modify how the RIP/SAP packet is processed. The route/service is announced or accepted only if the value is set to *permit*. The route/service is ignored if the value is set to *deny*.<br>The default value is *permit*. |
| RouteSource | Allows you to modify the route source of the packet. Use this field only for announce policies. (This field ignores accept policies.)<br>Accepted values are:<br>• direct<br>• nlsp<br>• rip<br>• static<br>• any |
| MatchNetList | Allows you to modify the number(s) of the networks to which this policy should be applied. The network list name is used to refer the range of networks. If not set or if the network list table entry is empty, then this policy is applied to all networks. You can set a maximum of 4 network lists for a policy. |
| MatchServList | Allows you to modify the service types and service names to which this policy is to be applied. The service list name is used to represent the service type and service name. If not set, or if the Service List Table entry is empty, then this policy is applied to all service types and service names. You can set a maximum of 4 service lists for a policy.<br>Note: This field is valid only for SAP policies. |
| Hops | The value used as the hops in announce policies. The hop count is updated with this value for matching RIP/SAP routes. If this value is 0, then hop count is not modified. This field is applicable for announce policies only. Enter a value from 0 to 16. The default value is 0. |
| Ticks | Value used as ticks in Rip Announce policies. For RIP Announce policies, if the routing method is ticks, the ticks of the route is updated with this value. If the value is 0, then ticks of the route is not modified. This field is applicable only for RIP Announce policy. Enter a value from 0 to 2147483647. The default value is 0. |

## Configuring policies to ingressing and egressing RIP packets

To configure what policies to apply to ingressing and egressing RIP packets:

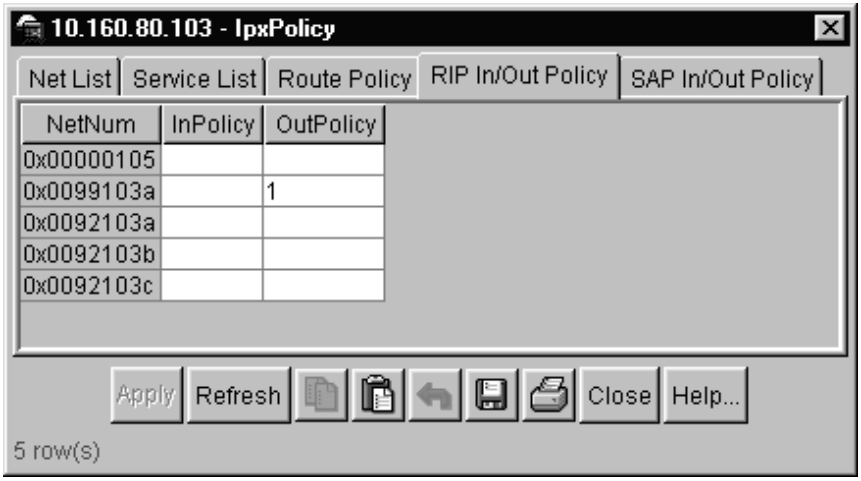
1. From the Device Manager menu bar, choose IPX Routing > Policy.

   The IpxPolicy dialog box opens with the Net List tab displayed (Figure 33).

2. Click the RIP In/Out Policy tab.

   The RIP In/Out Policy tab opens (Figure 39).

**Figure 39** IpxPolicy dialog box—RIP In/Out Policy tab




3. Enter information.
4. Click Apply.

Table 18 describes the RIP In/Out Policy tab fields.

**Table 18** IpxPolicy dialog box—RIP In/Out Policy tab fields

| Field | Description |
|---|---|
| NetNum | The interface to which the policy is applied. |
| InPolicy | The In policy name. |
| OutPolicy | The Out policy name. |

## Configuring policies to ingressing and egressing SAP packets

To configure what policies to apply to ingressing and egressing SAP packets:

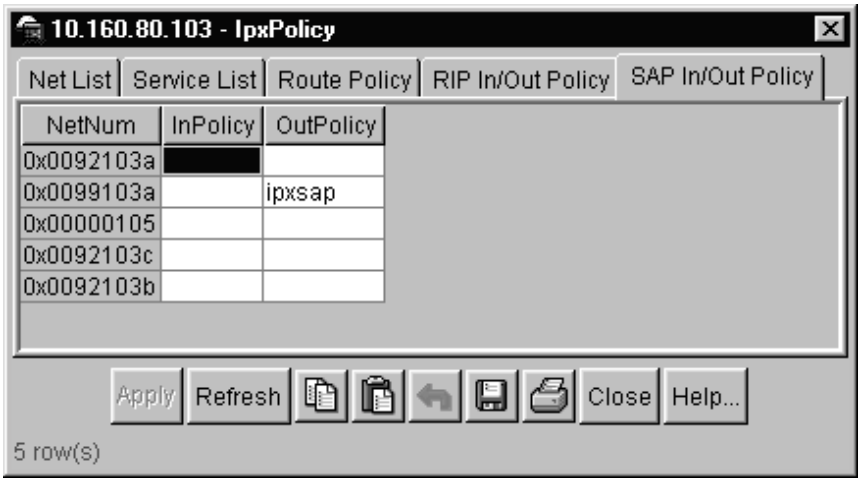
1 From the Device Manager menu bar, choose IPX Routing > Policy.

The IpxPolicy dialog box opens with the Net List tab displayed (Figure 33).

2 Click the SAP In/Out Policy tab.

The SAP In/Out Policy tab opens (Figure 40).

**Figure 40** IpxPolicy dialog box—SAP In/Out Policy tab




3 Enter information.

4 Click Apply.

Table 19 describes the SAP In/Out Policy tab fields.

**Table 19** IpxPolicy dialog box—SAP In/Out Policy tab fields

| Field | Description |
|---|---|
| NetNum | The interface to which the policy is applied. |
| InPolicy | The In policy name. |
| OutPolicy | The Out policy name. |

# Chapter 5
# Configuring IPX using the CLI

This chapter provides information about using the Run-Time CLI for configuring and displaying the Internet Packet Exchange (IPX) protocol, the Novell Inc. adaptation of the Xerox Network System (XNS) protocol. The 8000 Series Switch implementation of IPX supports four Ethernet frame formats:

- Ethernet II (ipxEthernet2)
- 802.2-LLC (ipx802dot2)
- 802.3-RAW (ipx802dot3)
- 802.3-SNAP (ipxSnap)

This chapter includes the following topics that describe how to set up your IPX configuration.

# Roadmap of IPX commands

The following roadmap lists some of the IPX commands and their parameters. Use this list as a quick reference or click on any command or parameter entry for more information.

| Command | Parameter |
|---|---|
| config ethernet <ports> ipx | info |
| | create <IPX network-number> <vlan_id> <encapsulation> [mac_offset <value>] [tick <value>] |
| | delete <IPX network-number> |
| config ipx forwarding | info |
| | disable [<IPX-network-number>] |
| | enable [<IPX-network-number>] |
| config ipx info | |
| config ipx rip | info |
| | default-delay <delay-timer> |
| | default-hold-multiplier <hold-multiplier> |
| | default-interval <interval-timer> |
| | hold-multiplier <IPX-network-number> <hold-multiplier> |
| | state <IPX-network-number> <on\|off> |
| | update-delay <IPX-network-number> <delay-timer> |
| | update-interval <IPX-network-number> <interval-timer> |
| config ipx sap | info |

| Command | Parameter |
| --- | --- |
| | create <service-type> <service-name> <ipxhost> <socket-number> <hop-count> |
| | delete <service-name> |
| | default-delay <delay-timer> |
| | default-hold-multiplier <hold-multiplier> |
| | default-interval <interval-timer> |
| | hold-multiplier <IPX-network-number> <hold-multiplier> |
| | sapgnstiebreaker <alphabetical \| round-robin> |
| | state <IPX-network-number> <on\|off> |
| | update-delay <IPX-network-number> <delay-timer> |
| | update-interval <IPX-network-number> <interval-timer> |
| config ipx set | info |
| | max-route <max_entries> |
| | max-sap <max_entries> |
| | max-static-route |
| | max-static-sap <max_entries> |
| | netbios <on\|off> |
| | learnafterincrement <on\|off> |
| | routing-method <tick\|hop> |
| config ipx static-route | info |
| | create <IPX-network-number> <nexthop> <hop-count> <tick-count> |

| Command | Parameter |
|---|---|
| | delete <IPX-network-number> |
| config vlan <vid> ipx | info |
| | create <IPX network-number> <encapsulation> [mac_offset <value>] [tick <value>] |
| | delete <IPX network-number> |
| | encapsulation <IPX network-number> <encapsulation> |
| config atm <ports> pvc 1483 ipx | info |
| | create <vid> <vpi.vci > [<ipx >] |
| | delete <vid > |
| config atm <ports> pvc 1483 muxIpIpx | info |
| | create <vid> <vpi.vci > <remoteip> [<ipx >] [<InArpSend enable \| disable>] [<arp send rate>] |
| | delete <vid > |
| show ports info ipx <ports> | |
| show ipx circuit [<IPX-network-number>] | |
| show ipx config [<IPX-network-number>] | |

| Command | Parameter |
|---|---|
| show ipx default | |
| show ipx route [<IPX-network-number>] [<IPX-network-number>] | |
| show ipx sap [<service-name>] | |
| show ipx stats [<IPX-network-number>] | |
| show ipx routingmethod | |
| show vlan info ipx [<vid>] | |

# Configuring IPX commands

This section includes the following commands:

## Configuring IPX brouter interface commands

A brouter is a single port VLAN, which can route packets of particular protocol and bridge packets for other protocols. The brouter is not part of any spanning tree group (STG) and it is always in the forwarding state.

The IPX brouter bridges packets of any other protocol. The IPX brouter is similar to an IP brouter in its functionality. The basic difference between IP and IPX brouter is that, the IPX packet can be of any one among four Ethernet frame formats namely: EthernetII, 802.2-LLC, 802.3-RAW, and 802.3-SNAP.The protocol used is determined by the encapsulation that you specify

A single port can act both as an IP and an IPX brouter port and can also be part of any other port-based VLAN.

A single port can also be a member of more than one IPX brouter port if the encapsulation method is different.

To create an IPX brouter interface, use the following CLI command:

```
config ethernet <ports> ipx
```

This command includes the following parameters.

| **config ethernet <ports> ipx** followed by: | |
|---|---|
| info | Displays all IPX brouter information for an ethernet port (Figure 41). |
| create<br>*<IPX network-number>*<br>*<vlan_id>*<br>*<encapsulation>*<br>*[mac_offset <value>]*<br>*[tick <value>]* | Creates a new IPX brouter port entry.<br>*<IPX network-number>* is the network address value.<br>*<vlan_id>* is the VLAN id.<br>*<encapsulation>* is one of the following encapsulation methods:<br>- ethernet-ii<br>- snap<br>- llc<br>- raw<br>*[mac_offset <value>]* The mac_offset is an optional parameter that allows you to manually change the default MAC address for a logical or physical interface. Value is an integer from 0 to 507. Default is the next available value.<br>*[tick <value>]* is the value that determines the best route for the IPX routed VLAN. The lower the tick value the better the route. Enter a tick value with the range of 1 to 32767. If you enter a value larger than 32767, an error message will display alerting you that the value has been changed to 32767, and a log message is generated. Default is 1. |
| delete<br>*<IPX network-number>* | Deletes an ethernet IPX interface.<br>*<IPX netrwork_number>* is the network address value. |

Figure 41 displays sample output using the **config ethernet <ports> ipx create** and **info** CLI commands.

**Figure 41** config ethernet <ports> ipx create and info command sample output

```
8010:5# config ethernet 3/3 ipx create 00000002 20 ethernet-ii

8010:5# config ethernet 3/3 ipx info
            IPX-network-number - 0x00000002
                           vid - 20
                 encapsulation - Ethernet-II
                    Mac_offset - 6
                         Ticks - 1
```

## Configuring IPX VLAN interface commands

Use the config vlan <vid> ipx commands to create and define an IPX VLAN interface.

To create an IPX VLAN interface, use the following CLI command:

```
config vlan <vid> ipx
```

The general **`config vlan <vid> ipx`** command includes the following options.

| **`config vlan <vid> ipx`** followed by: | |
|---|---|
| `info` | Displays all IPX vlan ipx information for a port (Figure 42). |
| `create`<br>*`<IPX network-number>`*<br>*`<encapsulation>`*<br>*`[mac_offset <value>]`*<br>*`[tick <value>]`* | Creates a new IPX vlan port entry.<br>*`<IPX network-number>`* is the network address value.<br>*`<encapsulation>`* is one of the following encapsulation methods:<br>- ethernet-ii<br>- snap<br>- llc<br>- raw<br>*`[mac_offset <value>]`* The mac_offset is an optional parameter that allows you to manually change the default MAC address for a logical or physical interface. Value is an integer from 0 to 507. Default is the next available value.<br>*`[tick <value>]`* is the value that determines the best route for the IPX routed VLAN. The lower the tick value the better the route. Enter a tick value with the range of 1 to 2147483647. Default is 1. |
| `delete`<br>*`<IPX network-number>`* | Deletes an ethernet IPX interface.<br>*`<IPX netrwork_number>`* is the network address value. |
| `encapsulation`<br>*`<IPX network-number>`*<br>*`<encapsulation>`* | Allows you to change the encapsulation method of a VLAN.<br>*`<IPX network-number>`* is the network address value.<br>*`<encapsulation>`* is one of the following encapsulation methods:<br>- ethernet-ii<br>- snap<br>- llc<br>- raw |

Figure 42 displays sample output using the **config vlan <vid> ipx create** and **info** CLI commands.

**Figure 42** config vlan <vid> ipx create and info command sample output

```
BW140:6/config/vlan/57/ipx# create 0x12341234 snap mac_offset 6
tick 1
BW140:6/config/vlan/57/ipx# info

              create :
            IPX-network-number  - 0x12341234
                          vid - 57
                 encapsulation  - SNAP
                    mac_offset  - 6
                         Ticks  - 1
```

## Modifying VLAN ipx encapsulation command

You can now change the IPX encapsulation of a VLAN without first having to delete and then recreate the VLAN.

To change the encapsulation method, use the following CLI command:

```
config vlan <vid> ipx encapsulation <IPX-network-number>
<encapsulation>
```

## Modifying VLAN ipx ticks command

IPX-routed VLANs have a default tick value of 1. In the 8000 Series Switch, when you configure an IPX address to a VLAN, you can assign a tick value within the range of 1 to 2147483647. A tick value determines the best route for the IPX-routed VLAN; the lower the tick value the better the route.

To change the tick value, use the following CLI command:

```
config vlan <vid> ipx create <IPX-network-number> [<encapsulation>]
[mac_offset<value>] [tick <value>]
```

## Configuring ipx forwarding command

The config ipx forwarding command allows you to enable or disable IPX forwarding globally or on a specified IPX network.

To configure ipx forwarding parameters, use the following command:

```
config ipx forwarding
```

The command includes the following parameters:

| **config ipx forwarding** followed by: | |
|---|---|
| `info` | Displays current config ipx forwarding info command output (Figure 43). |
| `disable [<IPX-network-number>]` | Disables IPX forwarding.<br>• *IPX-network-number* is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> } |
| `enable [<IPX-network-number>]` | Enables IPX forwarding.<br>• *IPX-network-number* is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> } |

Figure 43 shows **`config ipx forwarding info`** command output.

**Figure 43** config ipx forwarding info command output

```
8606:6# config ipx forwarding info


          forwarding : enable

              enable :
            IPX-network-number - 0x00000100
            IPX-network-number - 0x00000200
            IPX-network-number - 0x00001234
            IPX-network-number - 0x00000044

             disable :
```

## Configuring ipx info command

The **config ipx info** command (Figure 44) displays the current IPX configuration.

The command uses the syntax:

```
config ipx info
```

Figure 44 shows sample output for the **config ipx info** command.

**Figure 44** config ipx info command output

```
8606:6# config ipx info

              create :
            IPX-network-number - 0x00000100
                          vid - 1
                encapsulation - Ethernet-II
                   mac_offset - 1

            IPX-network-number - 0x00000200
                          vid - 2
                encapsulation - Ethernet-II
                   mac_offset - 5

            IPX-network-number - 0x00001234
                          vid - 3
                encapsulation - SNAP
                   mac_offset - 6

            IPX-network-number - 0x00000044
                          vid - 5
                encapsulation - SNAP
                   mac_offset - 7

              delete : N/A
```

## Configuring ipx rip command

The **config ipx rip** command allows you to configure Routing Information Protocol (RIP) on IPX interfaces and set the IPX RIP interface values.

**Note:** Three timing parameters (hold-multiplier, delay-timer, and interval-timer) control IPX RIP behavior. If you do not use the factory defaults and change global default parameters, you should set the global parameters prior to setting individual interface parameters.

To configure RIP parameters, use the following command:

```
config ipx rip
```

The **config ipx rip** command includes the following parameters:

| **config ipx rip** followed by: | |
|---|---|
| info | Displays the IPX RIP configuration (Figure 45). |
| default-delay <*delay-timer*> | Sets the delay timer default values in milliseconds.<br>• <*delay-timer* > is the range of 1 to 1000 with the default of 50 ms. |
| default-hold-multiplier <*hold-multiplier*> | Sets the hold multiplier default value.<br>• <*hold-multiplier* > is the range of 1 to 2147483647 with the default of 3. |
| default-interval <*interval-timer*> | Sets the interval timer default values in seconds.<br>• <*interval-timer* > is the range of 1 to 2147483647 with the default of 60 seconds. |
| hold-multiplier <*IPX-network-number*> <*hold-multiplier*> | Sets the hold multiplier value for the IPX interface.<br>• <*IPX-network-number*> is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> }<br>• <*hold-multiplier*> is the range of 1 to 2147483647 with the default of 3. |
| state <IPX-network-number> <on\|off> | Sets the RIP state on or off.<br>• <*IPX-network-number*> is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> }<br>• *on*\|*off* is the RIP State value (on or off). |

| **config ipx rip**<br>followed by: | |
|---|---|
| update-delay<br><*IPX-network-number*><br><*delay-timer*> | Sets the update delay timer for the IPX interface.<br>• <*IPX-network-number*> is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> }<br>• <*delay-timer* > is the range of 1 to 1000 ms with the default of 50 ms. |
| update-interval<br><*IPX-network-number*><br><*interval-timer*> | Sets the update interval for the IPX interface in seconds.<br>• <*IPX-network-number*> is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> }<br>• <*interval-timer*> is the range of 1 to 2147483647 with the default of 60 seconds. |

Figure 45 shows **config ipx rip info** command output.

**Figure 45** config ipx rip info command output

```
8606:6# config ipx rip info

                default-delay : 50 msec
       default-hold-multiplier : 3
              default-interval : 60 sec

           rip-state :
            IPX-network-number - 0x00000100
                         state : on
update-delay :
            IPX-network-number - 0x00000100
                  update-delay - 50 msec

     update-interval :
            IPX-network-number - 0x00000100
               update-interval - 60 sec
```

## Configuring ipx sap command

The **config ipx sap** command allows you to configure Service Advertisement Protocol (SAP) on IPX interfaces and set the global default values.

**Note:** Three timing parameters (hold-multiplier, delay-timer, and interval-timer) also control IPX SAP behavior. If you do not use the factory defaults and change global default parameters, you should set the global parameters prior to setting individual interface parameters.

To configure IPX sap parameters, use the following command:

```
config ipx sap
```

The **config ipx sap** command includes the following parameters:

| **config ipx sap** followed by: | |
|---|---|
| info | Displays the IPX SAP configuration (Figure 46). |
| create <*service-type*><br><*service-name*><br><*ipxhost*><br><*socket-number*><br><*hop-count*> | Creates a static SAP entry where:<br>• <*service-type*> is an integer between 1 and 65535. Some well-known service examples are:<br>0000h = unknown<br>0003h = print queue<br>0004h = file server<br>0005h = job server<br>0007h = print server<br>0009h = archive server<br>0024h = remote bridge server<br>0047h = advertising print server<br>• <*service-name* > is a character string (1 to 47 characters).<br>• <*ipxhost*> is the network and node network = IPX network number between 1 and 2147483647 node = xx:yy:zz:uu:vv:ww, where xx, yy, zz, uu, yy, and ww are 2-digit hexadecimal numbers.<br>• <*socket-number*> is a number between 0 and 65535.<br>• <*hop-count* > is a number between 1 and 15. |
| delete <*service-name*> | Deletes a static SAP entry. |

| **config ipx sap**<br>followed by: | |
|---|---|
| default-delay<br><*delay-timer*> | Sets the delay timer default values in milliseconds.<br>• *delay-timer* is a number between 1 and 1000 with the default of 50 ms. |
| default-hold-multiplier<br><*hold-multiplier*> | Sets the hold multiplier default value.<br>• *hold-multiplier* is a number between 1 and 2147483647 with a default of 3. |
| default-interval<br><*interval-timer*> | Sets the interval timer default values in seconds.<br>• *interval-timer* is a number between 1 and 2147483647 with a default of 60 seconds. |
| hold-multiplier<br><*IPX-network-number*><br><*hold-multiplier*> | Sets the hold multiplier value for the IPX interface.<br>• <*IPX-network-number*> is the IPX network number {0x00:0x00:0x00:0x00}.<br>• <*hold-multiplier* > is a number between 1 and 2147483647 with a default of 3. |
| sapgnstiebreaker<br><*alphabetical* \|<br>*round-robin*> | Sets the Get-Nearest-Server (GNS) tie-breaker, which takes effect when there are more than two equal-cost servers exiting.<br>• <*alphabetical*> specifies choosing the server in alphabetical order of the server names.<br>• <*round-robin*> specifies choosing the next server from the server list. |
| state<br><IPX-network-number><br><on\|off> | Sets the SAP state on or off.<br>• <*IPX-network-number*> is the IPX network number {0x00000000 \| 00:00:00:00 \| <value> }<br>• <*on*\|*off*> is the RIP State value (on or off). |
| update-delay<br><*IPX-network-number*><br><*delay-timer*> | Sets the update delay timer for the IPX interface.<br>• <*IPX-network-number*> is the IPX network number {0x00:0x00:0x00:0x00}.<br>• <*delay-timer* > is a number between 1 and 1000 with the default of 50 ms. |
| update-interval<br><*IPX-network-number*><br><*interval-timer*> | Sets the update interval for the IPX interface in seconds.<br>• <*IPX-network-number* > is the IPX network number {0x00:0x00:0x00:0x00}.<br>• <*interval-timer*> is a number between 1 and 2147483647 with the default of 60 seconds. |

Figure 46 shows **config ipx sap info** command output.

**Figure 46** config ipx sap info command output

```
8606:6# config ipx sap info

                 default-delay : 50 msec
       default-hold-multiplier : 3
              default-interval : 60 sec
              SapGnsTieBreaker : Alphabetical
              create :
                forwarding-cid - 0x0001
                  service-type - 0x0001
                  service-name - test
                       ipxhost - 0x00001234.11:22:33:44:44:44
                   socket-number - 0x0008
                       hop-count - 5
                forwarding-cid - 0x0001
                  service-type - 0x0002
                  service-name - test
                       ipxhost - 0x00001234.22:44:44:44:44:44
                   socket-number - 0x0008
                       hop-count - 2
                forwarding-cid - 0x0001
                  service-type - 0x7432
                  service-name - tes
                       ipxhost - 0x00001234.22:22:22:22:22:22
                   socket-number - 0x0009
                       hop-count - 2
              delete :
hold-multiplier :
            IPX-network-number - 0x00000100
               hold-multiplier - 3
sap-state :
            IPX-network-number - 0x00000100
                         state : on
update-delay :
            IPX-network-number - 0x00000100
                  update-delay - 50 msec
update-interval :
            IPX-network-number - 0x00000100
               update-interval - 60 sec
```

## Configuring ipx set command

The **config ipx set** command allows you to configure maximum entries for IPX parameters.

To configure and set maximum entries for IPX parameters, use the following command:

```
config ipx set
```

The **config ipx set** command includes the following parameters:

| **config ipx set**<br>followed by: | |
|---|---|
| info | Displays current maximum entries set on the switch (Figure 47). |
| max-route <*max_entries*> | Sets the maximum number of IPX routes that can be learned by the switch.<br>**Note**: To take effect, save the configuration and reset the switch.<br>• *max_entries* is an integer value with a range of 128 to 8000 entries. The default value is 128. |
| max-sap <*max_entries*> | Sets the maximum number of SAPs.<br>**Note**: To take effect, save the configuration and reset the switch.<br>• *max_entries* is an integer value with a range of 64 to 8000 entries. The default value is 64. |
| max-static-route <*max_entries*> | Sets the maximum number of static IPX routes that can be configured on the switch.<br>**Note**: To take effect, save the configuration and reset the switch.<br>• *max_entries* is an integer value with a range of 64 to 500 entries. The default value is 64. |
| max-static-sap <*max_entries*> | Sets the maximum number of static SAPs.<br>**Note**: To take effect, save the configuration and reset the switch.<br>• *max_entries* is an integer value with a range of 32 to 500 entries. The default value is 32. |

| **config ipx set**<br>followed by: | |
|---|---|
| netbios <on\|off> | Turns on or off IPX NetBIOS (type 20) propagation on all the switch's IPX interfaces.<br>**Note:** Nortel Networks recommends that care should be taken when deploying NetBIOS. |
| learnafterincrement <on\|off> | Turns IPX on or off. |
| routing-method <tick\|hop> | Sets the IPX routing method to tick or hop. |

Figure 47 shows sample output for the **config ipx set info** command.

**Figure 47** config ipx set info command output

```
8606:6# config ipx set info
                      max-route - 4000
                        max-sap - 6000
               max-static-route - 128
                 max-static-sap - 64
                        netbios - ON
            learnafterincrement - ON
                 routing-method - TICKS
```

## Globally enabling the IPX routing method

The **config ipx set routing-method** command allows you to globally set the IPX routing method. If the routing method is hops, then the route with fewer hops will be taken as best route and if the routing method is tick, then the route with fewer ticks will be used.

To globally set the routing method, use the following CLI command:

config ipx set routing-method <tick|hop>

where

*<tick|hop>* sets the routing method to ticks or hops. Default value is ticks.

To verify the selected routing method, use the CLI command **show ipx routingmethod** as shown in Figure 48.

**Figure 48** show ipx routingmethod command sample output

```
8606:6# config ipx set routing-method tick

8606:6# show ipx routingmethod
                          Routing Method : Ticks
```

## Configuring ipx static-route command

The **config ipx static-route** command allow you to create or delete a static IPX network route.

To configure ipx static route parameters, use the following commands:

```
config ipx static-route
```

The command includes the following parameters:

| **config ipx static-route** followed by: | |
|---|---|
| info | Displays IPX routes created and/or deleted. (Figure 49) |
| create <*IPX-network-number*> <*nexthop*> <*hop-count*> <*tick-count*> | Creates a static IPX network route where:<br>• <*IPX-network-number*> is the IPX network number {0x00:0x00:0x00:0x00}.<br>• <*nexthop*> is the IPX address of the next router.<br>• <*hop-count*> is the number of passes through a router.<br>• <*tick-count*> is the number of ticks (1/18th of a second).<br>To create a default route, enter FF:FF:FF:FE as the IPX network number. |
| delete <*IPX-network-number*> | Deletes the static IPX network route.<br>• <*IPX-network-number*> is the IPX network number {0x00:0x00:0x00:0x00}. |

Figure 49 shows sample output for the **config ipx static-route info** command.

**Figure 49** config ipx static-route info command output

```
8610# config ipx static-route info

Sub-Context:
Current Context:

              create :
              delete : N/A
```

## Configuring IPX over single ATM PVC using 1483 encapsulation

To configure IP/IPX over single ATM on the 8000 Series switch, use the following command:

```
config atm <ports> pvc 1483 ipx
```

The command includes the following parameters:

| **config atm <ports> pvc 1483 ipx** followed by: | |
|---|---|
| `info` | Displays the ELAN information. (Figure 50) |
| `create <vid> <vpi.vci > [<ipx >]` | Creates a ELAN where:<br>• `< vid >` is the VLAN id.<br>• `<vpi.vci >` specifies a Vpi and Vci value. The ranges are (0 to 255. 0-4095)<br>• `<ipx >` is the IPX network number {0x00:0x00:0x00:0x00}. |
| `delete <vid >` | Deletes the ELAN.<br>• `<vid >` is the VLAN id. |

Figure 50 shows sample output for the **`config atm <ports> pvc 1483 ipx info`** command.

**Figure 50** config atm <ports> pvc 1483 ipx info command output

```
Passport-8610:5/config/atm/8/5/pvc/1483/ipx# create 2 0.50
0x00000050
Passport-8610:5/config/atm/8/5/pvc/1483/ipx# info

Sub-Context:
Current Context:

Port 8/5:
                    1483 IPX
                      VlanId : 2
                     Vpi.Vci : 0.50
              IPX Net Number : 0x50
              Dummy MAC Addr : 00:e0:ff:7b:8a:3c
```

## Configuring multiplex IPX over a single ATM PVC

The IPX over single PVC feature allows you to create a muxIpIpx ELAN. A muxIpIpx ELAN multiplexes only IP and IPX protocols over a single ATM PVC through 1483 LLC encapsulation.

To create a muxIpIpx on the 8000 Series switch, use the following command:

```
config atm <ports> pvc 1483 muxIpIpx
```

The command includes the following parameters:

| **config atm <ports> pvc 1483 muxIpIpx** followed by: | |
|---|---|
| `info` | Displays the mulipipx ELAN information. (Figure 51) |
| `create <vid> <vpi.vci > <remoteip> [<ipx >] [<InArpSend enable \| disable>] [<arp send rate>]` | Creates an IPX muxIpIpx ELAN where:<br>• `< vid >` is the VLAN id.<br>• `<vpi.vci >` specifies a Vpi and Vci value. The ranges are (0 to 255. 0-4095)<br>• `< remoteip >` specifies the remote IP address.<br>• `<ipx >` is the IPX network number {0x00:0x00:0x00:0x00}. Optional parameter.<br>• `<InArpSend enable \| disable>` enable or disable ARP send.<br>• `<arp send rate>` specifies the arp send rate. |
| `delete <vid >` | Deletes the mulipipx ELAN.<br>• `<vid >` is the VLAN id. |

Figure 51 shows sample output for the **config atm <ports> pvc 1483 muxIpIpx info** command.

**Figure 51** config atm <ports> pvc 1483 muxIpIpx info command output

```
8610:5/config/atm/7/5/pvc/1483/muxIpIpx# create 1 0.33
128.125.9.3 0x00000012

8610:5/config/atm/7/5/pvc/1483/muxIpIpx# info

Sub-Context:
Current Context:

Port 7/5:
               1483 muxIpIpx
                      VlanId : 1
                     Vpi.Vci : 0.33
              Remote IP Addr : 128.125.9.3
              IPX Net Number : 0x12
              Dummy MAC Addr : 00:e0:ff:7b:8a:3c
```

**Note:** The Dummy MAC Address is used as a source MAC address when an ARP response is sent

# Show IPX commands

These commands display the configuration of IPX on the switch.

This section includes the following commands:



## Show ports info ipx command

To view information about the IPX brouter interfaces, use the following command:

```
show ports info ipx <ports>
```

Figure 52 displays sample output using the **`show port info ipx <ports>`** CLI command.

**Figure 52** show ports info ipx <ports> command sample output

```
8610:5# show ports info ipx 3/1

================================================================
                        Port Ipx
================================================================
PORT     IPX_ADDRESS ENCAP
----------------------------------------------------------------
3/1      0x00000001  LLC
3/1      0x00000002  SNAP
----------------------------------------------------------------
```

## Show ipx circuit command

The **show ipx circuit** command displays general IPX circuit information for the switch or for a specified IPX network number.

The command uses the syntax:

`show ipx circuit [<IPX-network-number>]`

Figure 53 shows sample output for the **show ipx circuit** command.

**Figure 53** show ipx circuit command output

```
8010# show ipx circuit

================================================================================
                                        Ipx Circuit
================================================================================
CID OPER_STATE IFINDEX VLANID  NETNUMBER ENCAPSULATION
--------------------------------------------------------------------------------
  1 UP            258   1016  0x0008081c SNAP
  2 UP            259   1028  0x0008183a RAW
  3 UP            260   1032  0x0008184b LLC
  4 UP            261   2050  0x0008187a RAW
  5 UP            261   2050  0x0008187b LLC
  6 UP            261   2050  0x0008187c SNAP
  7 UP            262   2080  0x0008193a RAW
  8 UP            262   2080  0x0008193b LLC
  9 UP            262   2080  0x0008193c SNAP
```

Table 20 describes the show ipx circuit command fields.

**Table 20** show ipx circuit fields

| Field | Description |
|---|---|
| CID | Circuit ID. The index number automatically assigned when the interface was created. |
| OPER_STATE | The operating state. It is either down or up; sleeping indicates it is set for up, but there are no connections to the interface. The normal state is up. |
| IFINDEX | VLAN interface index. |
| VLANID | The VLAN id. |
| NETNUMBER | The IPX circuit network number in an octet string: xx.xx.xx.xx. |
| ENCAPSULATION | The encapsulation method. |

## Show ipx config command

The **show ipx config** command displays general IPX configuration information for the switch or for a specified IPX network number.

The command uses the syntax:

```
show ipx config [<IPX-network-number>]
```

Figure 54 shows sample output for the **show ipx config** command.

**Figure 54** show ipx config command output

```
8610/show/ipx# config

================================================================================
                                Ipx Config
================================================================================
CID NETNUM     ENCAPSULATION   RIP STATUS   UPD HLD DLY SAP STATUS   UPD HLD
DLY
--------------------------------------------------------------------------------
  1 0x00004444 LLC            RIP Enabled   60   3  20 SAP Enabled   60   3  20
  2 0x00005555 SNAP           RIP Enabled   60   3  20 SAP Enabled   60   3  20
```

Table 21 describes the show ipx config command fields.

**Table 21** show ipx config command fields

| Field | Description |
|---|---|
| CID | Circuit ID. The index number automatically assigned when the interface was created. |
| NETNUM | The IPX circuit network number in an octet string: xx.xx.xx.xx. |
| ENCAPSULATION | The encapsulation method. |
| RIP STATUS | The status of RIP. The value is Enabled or Disabled. |
| UPD | Update delay. |
| HLD | Hold multiplier. |
| DLY | Update interval. |
| SAP STATUS | The status of SAP. The value is Enabled or Disabled. |
| UPD | Update delay. |

**Table 21** show ipx config command fields (continued)

| Field | Description |
|---|---|
| HLD | Hold multiplier. |
| DLY | Update interval. |

## Show ipx default command

The **`show ipx default`** command displays the current IPX RIP and SAP timer default values on the switch.

The command uses the syntax:

```
show ipx default
```

Figure 55 shows sample output for the **`show ipx default`** command.

**Figure 55** show ipx default command output

```
8606:6# show ipx default

================================================================
                                          Ipx Default Values
================================================================
RIP Hold-Multiplier: 3
RIP Delay-Timer:     50 msec (20 per sec)
RIP Update-Timer:    60 sec
SAP Hold-Multiplier: 3
SAP Delay-Timer:     50 msec (20 per sec)
SAP Update-Timer:    60 sec
SAP GNS Tie Breaker  : Alphabetical

Legend
GNS =Get Nearest Server
```

## Show ipx route command

The **show ipx route** command displays information about the IPX route(s) on the switch or a specific IPX route, including the type, hop count, and ticks.

The command syntax is:

```
show ipx route [<IPX-network-number>] [<IPX-network-number>]
```

Figure 56 shows sample output for the **show ipx route** command.

**Figure 56** show ipx route command output

```
8610/show/ipx# route

================================================================================
                                Ipx Route
================================================================================
IPX_NET  NEXT_HOP                    TYPE   HOPS  TICS  PORT TTL
--------------------------------------------------------------------------------
00004444 00004444.00:80:2d:23:02:00 Local  1         1
00005555 00005555.00:80:2d:23:02:01 Local  1         1
00008888 00004444.00:80:2d:23:02:00 Static 1         2  cpp

3 out of 3 routes displayed.

Legend
TTL =Time To Life
```

## Show ipx sap command

The **show ipx sap** command displays information about IPX SAP on the switch for all SAP services or a specified service.

The command uses the syntax:

```
show ipx sap [<service-name>]
```

Figure 57 shows sample output for the **show ipx sap** command.

**Figure 57** show ipx sap command output

```
8010# show ipx sap

================================================================================
                                      Ipx Sap
================================================================================
SERVICE TYPE IPX HOST                  SOCKET HOPS TTL NAME
--------------------------------------------------------------------------------
Dynamic 0100 1100001a.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000000
Dynamic 0100 1100001b.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000001
Dynamic 0100 1100001c.00:00:00:00:00:01 aabb 10   163 qfe1_e2_000002
Dynamic 0100 1100001d.00:00:00:00:00:01 aabb 10   163 qfe1_e2_000003
Dynamic 0100 1100001e.00:00:00:00:00:01 aabb 10   161 qfe1_e2_000004
Dynamic 0100 1100001f.00:00:00:00:00:01 aabb 10   161 qfe1_e2_000005
Dynamic 0100 11000020.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000006
Dynamic 0100 1100001a.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000007
Dynamic 0100 1100001b.00:00:00:00:00:01 aabb 10   164 qfe1_e2_000008
Dynamic 0100 1100001c.00:00:00:00:00:01 aabb 10   164 qfe1_e2_000009
Dynamic 0100 1100001d.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000010
Dynamic 0100 1100001e.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000011
Dynamic 0100 1100001f.00:00:00:00:00:01 aabb 10   163 qfe1_e2_000012
Dynamic 0100 11000020.00:00:00:00:00:01 aabb 10   163 qfe1_e2_000013
Dynamic 0100 1100001a.00:00:00:00:00:01 aabb 10   161 qfe1_e2_000014
Dynamic 0100 1100001b.00:00:00:00:00:01 aabb 10   161 qfe1_e2_000015
Dynamic 0100 1100001c.00:00:00:00:00:01 aabb 10   162 qfe1_e2_000016
```

Table 22 describes the show ipx sap command fields.

**Table 22** show ipx sap command fields

| Field | Description |
|---|---|
| SERVICE | The service name. |
| TYPE | The service type. |
| IPX HOST | The IPX network number. |
| SOCKET | The socket number. |
| HOPS | Hop count. |
| TTL | Time to life. |
| NAME | The service list name. |

## Show ipx stats command

The **`show ipx stats`** command displays IPX statistics for the specified IPX network number.

The command uses the syntax:

`show ipx stats [<IPX-network-number>]`

Figure 58 shows sample output for the **`show ipx stats`** command.

**Figure 58** show ipx stats command output

```
8010# show ipx stats
CIRCUIT_ID     NETNUM     RIP_TX     RIP_RX     SAP_TX     SAP_RX
1          0x0008081c         57        873         37       6205
2          0x0008183a        869          0       6037          0
3          0x0008184b        899         30       6039          1
4          0x0008187a        898        847       6039       6487
5          0x0008187b        898        847       6039       6549
6          0x0008187c        898        846       6039       6326
7          0x0008193a        870        120       6039       6064
8          0x0008193b        870        120       6039       3319
9          0x0008193c        870        119       6039       2740

---------------------------Total-------------------------------
                           7129       3802      48347      37691

Bad checksum         0
Received packet      83470
Too many hops        0
Header error         0
Unknown socket       0
Input discard        0
Forward packet       0
Output request       60119
Output no route      0
```

Table 23 describes the show ipx stats command fields.

**Table 23** show ipx stats command fields

| Field | Description |
|---|---|
| CIRCUIT_ID | Circuit ID. The index number automatically assigned when the interface was created. |
| NETNUM | The IPX circuit network number in an octet string: xx.xx.xx.xx. |
| RIP_TX | The number of RIP updates transmitted by the interface. |
| RIP_RX | The number of RIP updates received by the interface. |
| SAP_TX | The number of SAP updates transmitted by the interface. |
| SAP_RX | The number of SAP updates received by the interface. |
| Bad checksum | The number of packets received with a bad check sum. |
| Received packet | The total number of IPX packets received. |

**Table 23** show ipx stats command fields (continued)

| Field | Description |
|---|---|
| Too many hops | The number of IPX packets discarded due to exceeding the maximum hop count. |
| Header error | The number of packets with a corrupt header. |
| Unknown socket | The number of IPX packets discarded because the destination socket was not open. |
| Input discard | The number of IPX packets received but discarded due to reasons other than those accounted for by Header error or Unknown socket. |
| Forward packet | The number of IPX packets forwarded. |
| Output request | The number of IPX packets supplied locally for transmission, not including any packets counted in Forward packet. |
| Output no route | The number of times no route to a destination was found. |

## Show ipx routingmethod command

The **`show ipx routingmeethod`** command displays the selected IPX routing method.

The command uses the syntax:

```
show ipx routingmethod
```

Figure 59 shows sample output for the **`show ipx routingmethod`** command.

**Figure 59** show ipx routingmethod command sample output

```
8606:6# show ipx routingmethod
                          Routing Method : Ticks
```

## Show vlan info ipx command

The **show vlan info ipx** command displays VLAN IPX information for the specified VLAN or all VLANs on the switch.

The command syntax is:

```
show vlan info ipx [<vid>]
```

Figure 60 displays the headings for the **show vlan info ipx** command.

**Figure 60** show vlan info ipx command output

```
8610# show vlan info ipx

================================================================
                              Vlan Ipx
================================================================
VLAN-ID VLAN-TYPE      IPXNET     ENCAPSULATION  ROUTING
----------------------------------------------------------------
```

## Show port info atm 1483 command

The **show port info atm 1483** command displays 1483 muxIpIpx information.

The command syntax is:

```
show port info atm 1483
```

Figure 61 displays the headings for the **show port info atm 1483** command.

**Figure 61** show port info atm 1483 command output

```
8610:5# show port info atm 1483

================================================================
                    1483 MUX IP & IPX
================================================================
PORT   VLAN   PVC       VLAN              REMOTE       IPX NETWORK
IPX
NUM    ID     VPI.VCI   MAC ADDRESS       IP ADDRESS   NUMBER
ENCAP
----------------------------------------------------------------
3/7    37     0.37      00:e0:7b:7B:52:07 10.10.37.20 0X39
eth-ii
```

# Chapter 6
# Configuring IPX RIP/SAP route policies using the CLI

This chapter describes IPX RIP/SAP route policy filter features for the 8000 Series Switch and includes the following topics:



## Roadmap of IPX commands

The following roadmap lists some of the IPX commands and their parameters. Use this list as a quick reference or click on any command or parameter entry for more information.

| Command | Parameter |
|---|---|
| `config ethernet <ports> ipx rip` | `info` |
| | `in-policy <IPX-network-number> <policy-name>` |
| | `out-policy <IPX-network-number> <policy-name>` |
| `config ethernet <ports> ipx sap` | `info` |
| | `in-policy <IPX-network-number> <policy-name>` |

| Command | Parameter |
|---|---|
| | out-policy <IPX-network-number> <policy-name> |
| config ipx netlist <netlistname> | info |
| | add-network <IPX network-number> [to <value>] |
| | delete |
| | name <netlistname> |
| | remove-network <IPX network-number> [to <value>] |
| config ipx rip interface <IPX-network-number> | info |
| | in-policy <policy-name> |
| | out-policy <policy-name> |
| config ipx route-policy <policy-name> seq <seqnum> | info |
| | action<permit\|deny> |
| | create |
| | delete |
| | Enable |
| | Disable |
| | match-netlist <list-name/id> [clear] |
| | match-routesource <Route Source> [clear] |
| | match-servlist <list-name/id> [clear] |
| | set-hops <hops_count> |
| | set-ticks <tick_value> |
| config ipx sap interface <IPX-network-number> | info |
| | in-policy <policy-name> |
| | out-policy <policy-name> |

| Command | Parameter |
|---|---|
| config ipx servlist <servlistname> | info |
| | add-service <service-type> |
| | delete |
| | name servlist-name |
| | remove-service <servtype> [<servname]> |
| config vlan <vid> ipx rip | info |
| | in-policy <IPX-network-number> <policy-name> |
| | out-policy <IPX-network-number> <policy-name> |
| config vlan <vid> ipx sap | info |
| | in-policy <IPX-network-number> <policy-name> |
| | out-policy <IPX-network-number> <policy-name> |
| Show ipx list-policy command | |
| Show ipx network-list command | |
| Show ipx route-policy info command | |
| Show ipx service-list command | |
| Show vlan info rip command | |
| Trace ipx policy rip in-policy command | |
| Trace ipx policy rip out-policy command | |
| Trace ipx policy sap in-policy command | |
| Trace ipx policy sap out-policy command | |

# Configuring IPX commands

This section includes the following commands:



## Configuring a RIP in/out policy command

You can create a RIP in/out policy on an ethernet, IPX, or VLAN interface.

To create a RIP in/out policy on an ethernet interface (IPX brouter ports only), use the following command:

```
config ethernet <ports> ipx rip
```

To create a RIP in/out policy on an ethernet interface:

The general **`config ethernet <ports> ipx rip`** command is applicable only for IPX brouter ports and includes the following options.

| **`config ethernet <ports> ipx rip`** followed by: | |
|---|---|
| `info` | Displays the ethernet IPX RIP interface policy characteristics (Figure 62). |
| `in-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a RIP packet is received.<br>• *<IPX-network-number>* the name of the IPX interface to which the policy is applied.<br>• *<policy-name>* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| `out-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a RIP packet is received.<br>• *<IPX-network-number>* the IPX address of the IPX interface to which the policy is applied.<br>• *<policy-name>* the IPX address of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 62 displays sample output using the **`config ethernet <ports> ipx rip info`** command.

**Figure 62** config ethernet <ports> ipx rip info command sample output

```
BW140:6/config/vlan/57/ipx/rip# in-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/rip# out-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/rip# info

                    IPX-network-number: 0x12341234
                                 in-policy: 1
                                out-policy: 1
```

## Configuring a SAP in/out policy command

To create a SAP in/out policy on an ethernet interface (IPX brouter ports only), use the following command:

```
config ethernet <ports> ipx sap
```

To create a SAP in/out policy on an ethernet interface:

The general **`config ethernet <ports> ipx sap`** command includes the following options.

| **`config ethernet <ports> ipx sap`** followed by: | |
|---|---|
| `info` | Displays the ethernet IPX SAP interface policy characteristics (Figure 63). |
| `in-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a SAP packet is received.<br>• *`<IPX-network-number>`* the name of the IPX interface to which the policy is applied.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| `out-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a SAP packet is received.<br>• *`<IPX-network-number>`* the IPX address of the IPX interface to which the policy is applied.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 63 displays sample output using the **`config ethernet <ports> ipx sap info`** command.

**Figure 63** config ethernet <ports> ipx sap info command sample output

```
BW140:6/config/ethernet/57/ipx/sap# in-policy 0x12341234 1
BW140:6/config/ethernet/57/ipx/sap# out-policy 0x12341234 1
BW140:6/config/ethernet/57/ipx/sap# info

                  IPX-network-number: 0x12341234
                                      in-policy: 1
                                     out-policy: 1
```

## Configuring a RIP in/out policy on an IPX interface command

To create a RIP in/out policy on an IPX interface, use the following command:

```
config ipx rip interface <IPX-network-number>
```

The general **`config ipx rip interface`** command includes the following options.

| **`config ipx rip interface <IPX-network-number>`** followed by: | |
|---|---|
| `info` | Displays the ethernet IPX RIP policy interface characteristics (Figure 64). |
| `in-policy` *`<policy-name>`* | The name of the policy applied when a RIP packet is received.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| `out-policy` *`<policy-name>`* | The name of the policy applied when a RIP packet is received.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 64 displays sample output using the **`config ipx rip interface <IPX-network-number> info`** command.

**Figure 64** config ipx rip interface <IPX-network-number> info command sample output

```
BW140:6/config/ipx/rip/interface/12:34:12:34# in-policy 1
BW140:6/config/ipx/rip/interface/12:34:12:34# out-policy 1
BW140:6/config/ipx/rip/interface/12:34:12:34# info

                            in-policy: 1
                           out-policy: 1
```

## Configuring a SAP in/out policy on an IPX Interface command

To create a SAP in/out policy on an IPX interface, use the following command:

```
config ipx sap interface <IPX-network-number>
```

To create a SAP in/out policy on an IPX interface:

The general **`config ipx sap interface`** command includes the following options.

| **`config ipx sap interface <IPX-network-number>`** followed by: | |
|---|---|
| `info` | Displays the ethernet IPX SAP interface policy characteristics (Figure 65). |
| `in-policy` *`<policy-name>`* | The name of the policy applied when a SAP packet is received.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| `out-policy` *`<policy-name>`* | The name of the policy applied when a SAP packet is received.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 65 displays sample output using the **config ipx sap interface <IPX-network-number> info** command.

**Figure 65** config ipx sap interface <IPX-network-number> info command sample output.

```
BW140:6/config/ipx/sap/interface/12:34:12:34# in-policy 1
BW140:6/config/ipx/sap/interface/12:34:12:34# out-policy 1
BW140:6/config/ipx/sap/interface/12:34:12:34# info

                              in-policy: 1
                             out-policy: 1
```

## Configuring a RIP in/out policy on a VLAN interface command

To create a RIP in/out policy on a VLAN interface, use the following command:

```
config vlan <vid> ipx rip
```

To create a RIP in/out policy on a VLAN interface:

The general **config vlan <vid> ipx rip** command includes the following options.

| **config vlan <vid> ipx rip** followed by: | |
|---|---|
| info | Displays the vlan IPX RIP interface policy characteristics (Figure 66). |

| **config vlan <vid> ipx rip**<br>followed by: | |
|---|---|
| in-policy<br><*IPX-network-number*><br><*policy-name*> | The name of the policy applied when a RIP packet is received.<br>• <*IPX-network-number*> the IPX address of the IPX interface to which the policy is applied.<br>• <*policy-name*> the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| out-policy<br><*IPX-network-number*><br><*policy-name*> | The name of the policy applied when a RIP packet is received.<br>• <*IPX-network-number*> the IPX address of the IPX interface to which the policy is applied.<br>• <*policy-name*> the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 66 displays sample output using the **config vlan <vid> ipx rip info** command.

**Figure 66** config vlan <vid> ipx rip info command sample output.

```
BW140:6/config/vlan/57/ipx/rip# in-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/rip# out-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/rip# info

                  IPX-network-number: 0x12341234
                                in-policy: 1
                               out-policy: 1
```

## Configuring a SAP in/out policy on a VLAN interface command

To create a SAP in/out policy on a VLAN interface, use the following command:

```
config vlan <vid> ipx sap
```

The general **`config vlan <vid> ipx sap`** command includes the following options.

| **`config vlan <vid> ipx sap`** followed by: | |
|---|---|
| `info` | Displays the vlan IPX SAP interface policy characteristics (Figure 67). |
| `in-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a SAP packet is received.<br>• *`<IPX-network-number>`* the IPX address of the IPX interface to which the policy is applied.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |
| `out-policy` `<IPX-network-number>` `<policy-name>` | The name of the policy applied when a SAP packet is received.<br>• *`<IPX-network-number>`* the IPX address of the IPX interface to which the policy is applied.<br>• *`<policy-name>`* the name of the policy group to be applied to the interface. A blank policy-name will erase a previously entered name. |

Figure 67 displays sample output using the **`config vlan <vid> ipx sap info`** command.

**Figure 67** config vlan <vid> ipx sap info command sample output.

```
BW140:6/config/vlan/57/ipx/sap# in-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/sap# out-policy 0x12341234 1
BW140:6/config/vlan/57/ipx/sap# info

                    IPX-network-number: 0x12341234
                                     in-policy: 1
                                    out-policy: 1
```

## Configuring ipx netlist commands

The network list table contains a set of IPX network addresses that can be used by both RIP and SAP policies. Each entry in the table represents either a single IPX network address or a range of IPX network addresses. Each set of IPX network addresses is represented by a unique Id and name. There is a 1-to-1 relationship between the network list Id and name.

The Network List Table is used when doing a match on the *match-netlist* field in the route policy table.

Use the config ipx netlist commands to create and define IPX network addresses that will be used to represent networks to which policies will be applied.

To create a network address, use the following command:

```
config ipx netlist <netlistname>
```

The general **config ipx netlist** command includes the following options.

| **config ipx netlist <netlistname>** followed by: | |
|---|---|
| info | Displays the current network list characteristics (Figure 68). |
| add-network <*IPX network-number*> [*to <value>*] | Creates a new entry in the network list.<br>• <*IPX network-number*> is the network address value.<br>• *to <value>* use if a network range is to be specified. This is an optional parameter. If not entered, the entry refers to a single network. |
| delete | Deletes an entire network list. |
| name <*netlistname*> | This is used to rename the network list.<br><*netlistname*> is the network list name. It is a character string from 0 to 15 bytes. |
| remove-network <*IPX network-number*> [*to <value>*] | Used to remove an entry from the network list.<br>If there is only one entry in the network list, removing this entry will delete the entire network list.<br>• <*IPX network-number*> is the network address value.<br>• *to <value>* use if a network range is to be specified. Used to delete a range of network addresses. |

## Configuring ipx netlist add-network command

The **config ipx netlist add-network** command creates a new entry in the network lists.

The command uses the syntax:

```
config ipx netlist <netlistname> add-network <IPX-network-number>
[to <value>]
```

Figure 68 shows the **config ipx netlist add-network and info** command outputs.

**Figure 68** config ipx netlist add-network and info command outputs

```
Passport-8600:  config ipx netlist sc-01 add-network 0x100 to
0x200
Passport-8600: config ipx netlist sc-01 info

                 add-network : (0x00000100 to 0x00000200)
                      delete : N/A
                        name : sc-01
                          Id : 1
              remove-network : N/A
```

## Configuring an IPX route-policy command

A policy table contains a set of policy groups that can be used by both RIP and SAP protocols. Each policy group <listname> is identified with a unique name that can contain a group of policies with different MATCH & SET parameters. Each policy within a group is identified with a unique sequence number. Different policy groups can have same sequence number, whereas within a group the sequence number must be unique.

To create a route policy table, use the following command:

```
config ipx route-policy <policy-name> seq <seqnum>
```

The general **`config ipx route-policy`** command includes the following options.

| **`config ipx route-policy <policy-name> seq <seqnum>`** followed by: | |
|---|---|
| `info` | Displays the route policy characteristics (Figure 69). |
| `action<permit\|deny>` | Allows you to modify how the RIP/SAP packet is processed. The route/service is announced or accepted only if the action is set to *permit*. The route/service is ignored if the value is set to *deny*.<br>The default value is *`permit`*. |
| `create` | Creates a new route policy. |
| `delete` | Deletes a route policy from the table. |
| `Enable` | Allows you enabled (true) a route policy. |
| `Disable` | Allows you to disabled (false) a route policy. If disabled, the route policy should not be used. The default value is disable (false). |
| `match-netlist <list-name/id> [clear]` | Allows you to modify the number(s) of the networks to which this policy should be applied. The network list name or Id is used to refer to the range of networks in the Network List Table. If not set or if the Network List Table entry is empty, then this policy is applied to all packets. You can set a maximum of 4 network list for a policy.<br>• *`<list-name/id>`* this is the network list name or Id from the Network List Table.<br>• *`[clear]`* when used, this optional parameter will erase what is entered in the *`<list-name/id>`* parameter. |

| **config ipx route-policy <policy-name> seq <seqnum>** followed by: | |
|---|---|
| `info` | Displays the route policy characteristics (Figure 69). |
| `match-routesource <Route Source> [clear]` | Allows you to modify the route source of the packet. Use this field only for announce policies. This field is not used by accept policies. The default value is none, that is, the route source field is not checked.<br>Accepted *<Route Source>* values are:<br>• direct<br>• nlsp<br>• rip<br>• static<br>• any<br>• *[clear]* when used, this optional parameter will erase what is entered in the *<Route Source>* parameter. |
| `match-servlist <list-name/id> [clear]` | Allows you to modify the service types and service names to which this policy is to be applied. The service list name or Id is used to represent the service type and service name. If not set, or if the Service List Table entry is empty, then this policy is applied to all service types and service names. You can set a maximum of 4 service lists for a policy.<br>Note: This field is valid only for SAP policies.<br>• *<list-name/id>* this is the service list name or Id in the Service List Table.<br>• *[clear]* when used, this optional parameter will erase what is entered in the *<list-name/id>* parameter. |

| **config ipx route-policy <policy-name> seq <seqnum>** followed by: | |
|---|---|
| info | Displays the route policy characteristics (Figure 69). |
| set-hops <*hops_count*> | Use this field to set the number of hops in announce policies. The hop count of the matching RIP/SAP route is updated with this value. If the value is 0, then the hop count is not modified. This field is applicable for announce policies only. Enter a hop value with the range of 0 to 16. The default value is 0.<br>• <*hops_count*> the number of hops. |
| set-ticks <*tick_value*> | Value used as ticks in RIP announce policies. For RIP announce policies, the ticks of the route is updated with this value. If the value is 0, then ticks of the route is not modified. This field is applicable only for RIP announce policy. Enter a tick value with the range of 0 to 2147483647. The default value is 0. |

Figure 69 shows sample **config ipx route-policy** commands and output.

**Figure 69** Sample config ipx route-policy commands and output

```
Passport-8600: config ipx route-policy policy-AA seq 1
create



Passport-8600: config ipx route-policy policy-AA seq 1
match-netlist sc-aa

Passport-8600: config ipx route-policy policy-AA seq 1
match-routesource static

Passport-8600: config ipx route-policy policy-AA seq 1
match-servlist servlist-1

Passport-8600: config ipx route-policy policy-AA seq 1
set-hops 5

Passport-8600: config ipx route-policy policy-AA seq 1
set-ticks 2



Passport-8600: config ipx route-policy policy-AA seq 1
enable

Passport-8600: config ipx route-policy policy-AA seq 1
info



                                    id : 1
                                   seq : 1
                                  name : policy-AA
                                enable : Enable
                                action : Permit
                     match-routesource : static
```

## Configuring ipx servlist command

The service list table contains IPX network service name information that can be used by both RIP and SAP policies. Each entry in the list represents a service type and a service name. Each set of IPX services is represented by a unique Id and name. There is a 1-to-1 relationship between the service list Id and name.

The Service List is used when doing a match on the *match-servlist* field in the route policy table.

Use the config ipx servlist commands to create and define IPX services that will be used to represent services to which policies will be applied.

To create a service list, use the following command:

```
config ipx servlist <servlistname>
```

The general **config ipx servlist** command includes the following options.

| **config ipx servlist <servlistname>** followed by: | |
|---|---|
| info | Displays the current service list characteristics (Figure 70). |
| add-service <*service-type*> [<*servicename*>] | Creates a new entry in the service list.<br>• <*service-type*> is the service type value. If set to 0xFFFF, all service types are matched. Enter the value in decimal format. For example a decimal 100 is equal to hex 0x0100.<br>• <*servicename*> is the service name. If not entered, an asterisk is taken as default value. This is matched to any service name. Also, an asterisk can be used to match wildcard characters. This is supported only at the end of the service name. For example: Printer* will be matched to Printer1, Printer2, Printer*n*. Service Name matching is case-sensitive. |
| delete | Deletes an entire entry from the service list. |

| **config ipx servlist <servlistname>** followed by: | |
|---|---|
| info | Displays the current service list characteristics (Figure 70). |
| name servlist-name | This is used to rename the service list. |
| remove-service <*servtype*> [<*servname*>] | Used to remove a service type entry from the service list.<br>If there is only one entry in the service list, removing this entry will delete the entire service list.<br>• <*servtype*> is the service type value.<br>• <*servname*> is the service name. If not entered, '*' is taken as default value. This is matched to any service name. Also, '*' can be used to match wildcard characters. This is supported only at the end of the service name. For example: Printer* will be matched to Printer1, Printer2, Printer*n*. Service Name matching is case-sensitive. |

## Configuring ipx servlist add-service command

The **config ipx servlist add-service** command creates a new entry in the service list.

The command uses the syntax:

```
config ipx servlist <servlistname> add-service <service-type>
[<service-name>]
```

Figure 70 shows the **config ipx servlist add-service and info** command outputs.

**Figure 70** config ipx servlist add-service and info command outputs

```
Passport-8600: config ipx servlist servlist-1 add-service 3
PrintSrv-1

Passport-8600: config ipx servlist servlist-1 add-service 4
FileSrv-1

Passport-8600: config ipx servlist servlist-1 info

                add-service : (0x00000003, PrintSrv-1),
                              (0x00000004, FileSrv-1)
                     delete : N/A
                       name : servlist-1
                         Id : 1
             remove-service : N/A
```

# Show ipx commands

These commands display the configuration of IPX on the switch.

This section includes the following commands:

| Commands | Page |
|---|---|
| Show ipx list-policy command | 136 |
| Show ipx network-list command | 137 |
| Show ipx route-policy info command | 138 |
| Show ipx service-list command | 141 |
| Show vlan info rip command | 142 |

## Show ipx list-policy command

The show ipx list-policy command displays information about list policies for an interface.

The command uses the syntax:

```
show ipx list-policy [interface <value>]
```

Figure 71 displays sample output for the `show ipx list-policy [interface <value>]` CLI command.

**Figure 71** show ipx list-policy command sample output

```
Passport-8010# show ipx list-policy

RIP OUT POLICY
    === === ======
                    Interface    Policy Name
                    ---------      ------ ----
                    0x00000009     r1

RIP IN POLICY
   === === ======
                    Interface    Policy Name
                    ---------      ------ ----
                    0x00000009     r1
                    0x00000010     r2

SAP OUT POLICY
    === === ======
                    Interface    Policy Name
                    ---------      ------ ----
                    0x00000009     r1

SAP IN POLICY
    === === ======
                    Interface    Policy Name
                    ---------    ------ ----
                    0x00000009     r1
                  0x00000010   r2
```

## Show ipx network-list command

The **show ipx network-list** command displays information about network list.

The command uses the syntax:

```
show ipx network-list [listid] [network <value>]
```

Figure 72 shows sample command output.

**Figure 72** show ipx network-list command output

```
Passport 8010:6# show ipx network-list

                add-network : (0x00000012 to 0x00000015),
                              (0x00000016 to 0x00000020)
                     delete : N/A
                       name : n1
                         Id : 1
             remove-network : N/A

                add-network : (0x00000018 to 0x00000018),
                              (0x00000020 to 0x00000022),
                              (0x00000099 to 0x00000999)
                     delete : N/A
                       name : n2
                         Id : 2
             remove-network : N/A

                add-network : (0x00000018 to 0x00000018)
                     delete : N/A
                       name : n3
                         Id : 3
             remove-network : N/A
```

## Show ipx route-policy info command

The **`show ipx route-policy info`** command displays information about a route policy.

The command uses the syntax:

```
show ipx route-policy info [id  <value>] [seqnum <value>]
```

Figure 73 displays sample output for the `show ipx route-policy info` CLI command. To display sample output for a specific ipx route id and sequence number, use the parameters [id <value>] [seqnum <value>].

**Figure 73** show ipx route-policy info command sample output

```
Passport-8010# show ipx route-policy info

================================================================================
                                          Route Policy
================================================================================
             Name = r1, Id = 1, Seq=1
--------------------------------------------------------------------------------
                               enable : Enable
                               action : Permit
                        match-netlist :
                        match-servlist :
                    match-routesource : rip|direct
                             set-hops : 5
                            set-ticks : 0
--------------------------------------------------------------------------------
             Name = r1, Id = 1, Seq=2
--------------------------------------------------------------------------------
                               enable : Disable
                               action : Permit
                        match-netlist :
                        match-servlist :
                    match-routesource : N/A
                             set-hops : 0
                            set-ticks : 0
--------------------------------------------------------------------------------
             Name = r2, Id = 2, Seq=1
--------------------------------------------------------------------------------
                               enable : Disable
                               action : Permit
                        match-netlist :
                        match-servlist :
                    match-routesource : N/A
                             set-hops : 0
                            set-ticks : 0
--------------------------------------------------------------------------------
```

Table 24 describes the show ipx route-policy info command fields.

**Table 24** show ipx route-policy info command fields

| Field | Description |
|---|---|
| Name | The network list name. |
| Id | A unique identifier assigned when creating a netlist. |
| Seq | A sequential sequence number assigned by the system. |
| enable | Displays the status of the route policy. Default is disable. |
| action | Display how the RIP/SAP packet is processed. The route/service is announced or accepted only if the action is set to *permit*. The route/service is ignored if the value is set to *deny*.The default value is *permit*. |
| match-netlist | Display the number(s) of the networks to which this policy should be applied. The network list name or Id is used to refer to the range of networks in the Network List Table. If not set or if the Network List Table entry is empty, then this policy is applied to all packets. You can set a maximum of 4 network list for a policy. |
| match-servlist | Display the service types and service names to which this policy is to be applied. The service list name or Id is used to represent the service type and service name. If not set, or if the Service List Table entry is empty, then this policy is applied to all service types and service names. You can set a maximum of 4 service lists for a policy. |
| match-routesource | Displays the route source of the packet. Use this field only for announce policies. This field is not used by accept policies. The default value is none, that is, the route source field is not checked.<br>Accepted values are:<br>direct<br>nlsp<br>rip<br>static<br>any |

**Table 24** show ipx route-policy info command fields (continued)

| Field | Description |
|---|---|
| set-hops | Display the number of hops in announce policies. The hop count of the matching RIP/SAP route is updated with this value. If the value is 0, then the hop count is not modified. This field is applicable for announce policies only. Enter a hop value with the range of 0 to 16. The default value is 0. |
| set-ticks | Value used as ticks in RIP announce policies. For RIP announce policies, the ticks of the route is updated with this value. If the value is 0, then ticks of the route is not modified. This field is applicable only for RIP announce policy. Enter a tick value with the range of 0 to 2147483647. The default value is 0. |

## Show ipx service-list command

The **`show ipx service-list`** command displays information about network list.

The command uses the syntax:

```
show ipx service-list [listid] [service-type <value>]
[service-name <value>]
```

Figure 75 shows sample command output.

**Figure 74** show ipx service-list command output

```
Passport-8010:6# show ipx service-list
                 add-service : (0x00000004, ftp),
                               (0x00000008, server),
                               (0x00000012, print)
                      delete : N/A
                        name : sc1-servlist
                          Id : 1
              remove-service : N/A
```

## Show vlan info rip command

The **show vlan info rip <vid>** command displays information about network list.

The command uses the syntax:

```
show vlan info rip <vid>
```

Figure 75 shows sample command output.

**Figure 75** show ipx service-list command output

```
Passport-8010:6# show ipx service-list
                 add-service : (0x00000004, ftp),
                               (0x00000008, server),
                               (0x00000012, print)
                      delete : N/A
                        name : sc1-servlist
                          Id : 1
              remove-service : N/A
```

# Trace ipx commands

The trace utility is used to trace the interactions of packets for a protocol or protocol feature. It displays high level information typically used for debugging and problem solving.

This section includes the following commands:



## Trace ipx policy rip in-policy command

The **`trace ipx policy rip in-policy`** command controls trace support for RIP in-policy routes.

The command uses the syntax:

```
trace ipx policy rip in-policy
```

The general **trace ipx policy rip in-policy** command includes the following options.

| **trace ipx policy rip in-policy** followed by: | |
|---|---|
| info | This command displays the trace status of all interfaces to which a RIP in-policy is assigned. |
| add <IPX-network-number> | This command activates trace support for an IPX interface. All RIP routes dropped by the interface due to the in-policy are displayed on the console. If no RIP in-policy is assigned, an error message is displayed.<br>• *<IPX-network-number>* the IPX address of the IPX interface to which the trace is applied. |
| delete <IPX-network-number> | This command removes the trace support from the interface.<br>• *<IPX-network-number>* the IPX address of the IPX interface from which the trace is deleted. |

## Trace ipx policy rip out-policy command

The **trace ipx policy rip in-policy** command controls trace support for RIP out-policy routes.

The command uses the syntax:

```
trace ipx policy rip out-policy
```

The general **`trace ipx policy rip out-policy`** command includes the following options.

| **`trace ipx policy rip out-policy`** followed by: | |
|---|---|
| `info` | This command displays the trace status of all interfaces to which a RIP out-policy is assigned. |
| `add` `<IPX-network-number>` | This command activates trace support for an IPX interface. All RIP routes dropped by the interface due to the out-policy are displayed on the console. If no RIP out-policy is assigned, an error message is displayed.<br>*`<IPX-network-number>`* the IPX address of the IPX interface to which the trace is applied. |
| `delete` `<IPX-network-number>` | This command removes the trace support from the interface.<br>*`<IPX-network-number>`* the IPX address of the IPX interface from which the trace is deleted. |

## Trace ipx policy sap in-policy command

The **`trace ipx policy sap in-policy`** command controls trace support for SAP in-policy routes.

The command uses the syntax:

```
trace ipx policy sap in-policy
```

The general **`trace ipx policy sap in-policy`** command includes the following options.

| **`trace ipx policy sap in-policy`** followed by: | |
|---|---|
| `info` | This command displays the trace status of all interfaces to which a SAP in-policy is assigned. |
| `add` `<IPX-network-number>` | This command activates trace support for an IPX interface. All SAP routes dropped by the interface due to the in-policy are displayed on the console. If no SAP in-policy is assigned, an error message is displayed.<br>• *`<IPX-network-number>`* the ipx address of the IPX interface to which the trace is applied. |
| `delete` `<IPX-network-number>` | This command removes the trace support from the interface.<br>*`<IPX-network-number>`* the IPX address of the IPX interface from which the trace is deleted. |

## Trace ipx policy sap out-policy command

The **`trace ipx policy sap out-policy`** command controls trace support for SAP out-policy routes.

The command uses the syntax:

```
trace ipx policy sap out-policy
```

The general **`trace ipx policy sap out-policy`** command includes the following options.

| **`trace ipx policy sap out-policy`** followed by: | |
|---|---|
| `info` | This command displays the trace status of all interfaces to which a SAP out-policy is assigned. |
| `add` `<IPX-network-number>` | This command activates trace support for an IPX interface. All SAP routes dropped by the interface due to the out-policy are displayed on the console. If no SAP out-policy is assigned, an error message is displayed.<br>*`<IPX-network-number>`* the ipx address of the IPX interface to which the trace is applied. |
| `delete` `<IPX-network-number>` | This command removes the trace support from the interface.<br>*`<IPX-network-number>`* the ipx address of the IPX interface from which the trace is deleted. |

# Index

## N



## O



## P



## R



## S

## T



## U



## V



## X