Vanguard Managed Solutions

Vanguard Applications Ware
IP and LAN Feature Protocols

Internetwork Packet Exchange

Notice

Restricted Rights Notification for U.S. Government Users

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum Òrestricted rightsÓ in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

Restricted Rights Legend

Use, duplication, or disclosure by the Government
is subject to restrictions as set forth in
subparagraph (c)(1)(ii) of the
Rights in Technical Data and Computer Software
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

Notice

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

Proprietary Material

Part No. T0100-07, Revision H
Publication Code DS
First Printing April 1997

Manual is current for Release 6.2 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to LGEN031@vanguardms.com

Overview

Introduction

This document describes the Internetwork Packet Exchange (IPX) Protocol option for Vanguard products.

In This Manual

Topic **See Page**

About the Internetwork Packet Exchange Protocol

Description

The Internetwork Packet Exchange (IPX) protocol is the network layer protocol used in Novell NetWare networks. IPX routes Netware packets between different local area networks (LANs). Vanguard products can serve as IPX routers to interconnect PC workstations with any Novell server in a LAN/WAN internetwork.

Novell Netware

Novell NetWare is one of the most popular PC LAN operating systems. NetWare is based on the concept of file servers, which contain files that can be accessed using PC workstations anywhere on the internetwork. When a workstation logs into a server PC, directories on the server PC are mapped into the network such as “Y:” or “Z:” on the workstation.

Interconnecting Netware LANs

NetWare supports operation on a LAN internetwork—a connected set of LANs. Workstations on any LAN are able to log into a server on any other LAN. Each LAN is assigned an IPX Network Number and every NetWare packet has an IPX header that contains the source and destination Network Number.

All differently numbered NetWare LANs must be interconnected an IPX router. When a router receives a packet addressed to a LAN other than the one where it originated, it forwards the packet onto another LAN for the next hop to its destination.

When a Novell file server is attached to more than one LAN, it always serves as an IPX router between those LANs. When connecting LANs over a Wide Area Network (WAN), however, a separate multiprotocol bridge/router, such as a Vanguard product, is usually used.

Typical LAN/WAN Interconnection

Figure 1 shows a typical configuration for a LAN/WAN IPX interconnection.

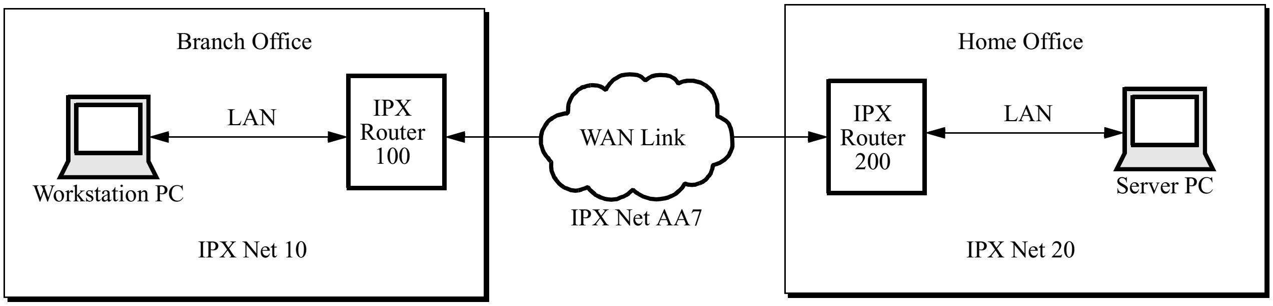


Figure 1. Typical LAN/WAN Interconnection

In a WAN IPX interconnection, each local LAN is assigned a different IPX network number. As shown in Figure 1, the LAN connecting all workstations in a branch office to the Vanguard IPX router is assigned IPX Network Number 10. The LAN connecting the file servers in the home office is assigned the Network Number 20. The WAN link between IPX routers is assigned IPX Network Number AA7.

■ **Note**

IPX Network Numbers are 32-bit numbers that are always represented in hexadecimal format. For IPX routing purposes, all connections into an IPX router are considered to be a LAN, and so even the WAN link must be assigned an IPX LAN Network Number.

Interfaces

Routers use the term “interface” to mean the connection of a router to a single LAN or WAN link. Routers route packets from one interface to another. In Vanguard routers, interface number 1 is reserved for the locally attached LAN and interface 5 and above are reserved for the WAN links.

Vanguard supports mixed LAN interfaces, meaning you can configure a mix of one Ethernet LAN interface and one Token Ring LAN interface in the same node.

LCONs

In Vanguard routers, WAN links are logical entities called LAN Connections or LCONs. Each LCON is assigned a small integer LCON number as its index in the LAN Connection Table. An LCON of a type that supports routing, such as the ROUT or BROUT type, is configured to attach to a particular interface number of the Vanguard router. The Mnemonic Table and Route Selection Table then define how LCONs are established on the virtual circuits of the physical X.25 or Frame Relay ports of the router. LCONs are considered to originate and accept data calls on the WAN network. For X.25 calls, they are considered to be subaddress 94 of the node’s X.25 address.

Example of Internal Data Flow

Figure 2 shows an example of internal data flow.

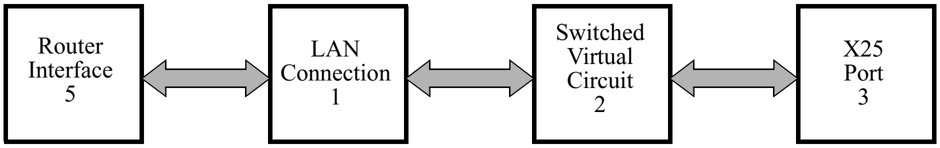


Figure 2. Example of Internal Data Flow

What You Need to Know About IPX

You should have a good working knowledge of:

- IPX addressing schemes
- Routing Information Protocol (RIP)
- Service Advertising Protocol (SAP)

Addressing

Introduction

IPX provides the addressing for packet delivery. Addressing includes the addresses assigned to each network segment. IPX uses host numbers, network numbers, and socket numbers to provide unique addresses for network devices such as servers and printers.

IPX Addressing

This table describes these numbers and describes how they are used in the network:

Number Type	***Description***
Network	The network number provides a unique address for each IPX network. It is a 32-bit hexadecimal number used for all routers and file servers on the network. Routers use this number to send packets to their final destination.
Node	This 48-bit number provides a unique hardware address for each node in the network. It identifies the Network Interface Card (NIC).
Socket	The 16-bit socket number is used for binding a packet to an application service. It identifies each process that communicates using IPX. Socket numbers are used for routing packets to specific processes within a node.

Format for IPX Frame

The basic format for an IPX frame consists of a MAC header, IPX header, data field, and MAC Frame Check Sequence (FCS).

The IPX header contains the destination network, node, and socket addresses to which the packet is addressed. It also contains the source network, node, and socket so that the packet recipient knows where to respond. The basic function of an IPX router is to forward IPX packets to the proper destination network.

■ **Note**

IP and IPX network numbers are different, but the router interface numbers are the same.

IPX Header Fields

This table describes the IPX header fields:

Field	Bytes	Description
Checksum	2	Checksum ignored. Always 0xFFFF
Packet Length	2	Includes IPX header and data
Transport Control	1	Starts at 0, incremented by routers, discarded at 16
Packet Type	1	0x00 Unknown/other 0x01 Routing Information Protocol 0x04 Service Advertising Protocol 0x05 Sequenced Packet Control 0x11 Netware Core Protocol 0x14 NetBios Propagated Packet
Destination Network	4	Identifies the unique destination from a number of interconnected networks
Destination Node	6	The 6-byte MAC address on the numbered IPX network
Destination Socket	2	0x451 Netware Core Protocol (NCP) 0x452 Service Advertising Protocol (SAP) 0x453 Route Information Protocol (RIP) 0x455 Novell Netbios 0x4000+ Dynamic 0x8000+ Assigned by Novell
Source Network	4	Identifies the unique source network from a number of interconnected networks
Source Node	6	The 6-byte MAC address on the numbered IPX network
Source Socket	2	See Destination Socket in this list

RIP

For detailed information on RIP, refer to the IP Routing option guide.

■ **Note**

Both the IP and IPX network protocols use a “RIP” route discovery protocol. IP RIP and IPX RIP are different protocols, with different formats. Unless otherwise specified, this section refers to IPX RIP.

SAP

SAP is used to locate devices such as file servers and printers. File and print servers advertise their presence to the network. Routers maintain a SAP services table and periodically (every 60 seconds) re-advertise all services.

SAP Frame Format

This table shows the SAP frame format:

Field	Bytes
IPX Header (Packet Type 4) (Socket 0452)	30
SAP Operation	2
Service Type	2
Server Name	48
Network Number	4
Node Address	6
Socket Number	2
Hops to Server	2

SAP Fields

This table describes the SAP fields:

Field	Description
SAP Operation	1 Request 2 Response 3 Get Nearest Server Request 4 Get Nearest Server Response
Service Type	0004 File Server 0005 Job Server 0007 Print Server 0009 Archive Server

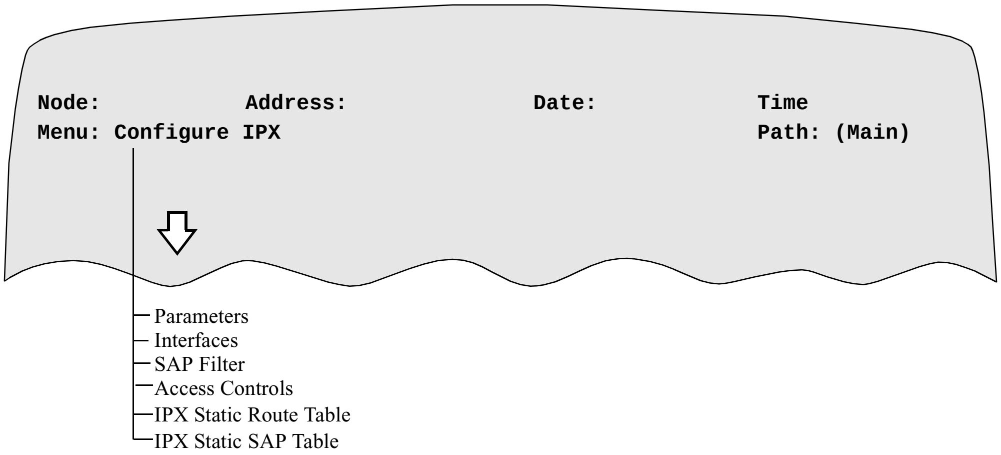
Configuration

Introduction

This section describes how to configure Vanguard products for IPX protocol operation.

Configure IPX Menu

Figure 3 shows the records and tables you need to configure before you can run IPX on a Vanguard in your network. The parameters for these records and tables are described in the following sections.



```
Node:            Address:                Date:             Time
Menu: Configure IPX                                        Path: (Main)
```

Figure 3. Configure Menu

Booting IPX Parameters and Tables

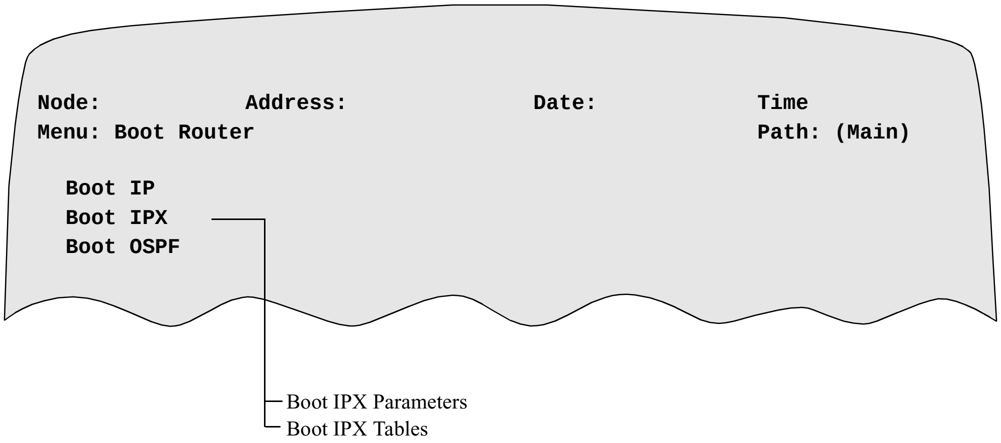
Introduction

After configuring many different IPX parameters, it may be necessary to boot either the parameter or table. This section explains how to perform these functions.

Booting IPX Parameters

Follow these steps to boot IPX parameters:

Step	Action	Result
1	Select **Boot** from the CTP Main menu.	The Boot menu appears.
2	Select **Boot Router** from the Boot menu.	The Boot Router menu, shown in Figure 4, appears.
3	Select **Boot IPX Parameters** from the Boot Router menu.	The modified parameters are booted and all changes made are implemented.



```
Node:            Address:                Date:            Time
Menu: Boot Router                                         Path: (Main)

  Boot IP
  Boot IPX
  Boot OSPF
```

Figure 4. Boot Router Menu

Booting IPX Tables

The procedure to boot IPX tables is similar to the parameter boot except that you must select the Boot IPX Tables menu item.

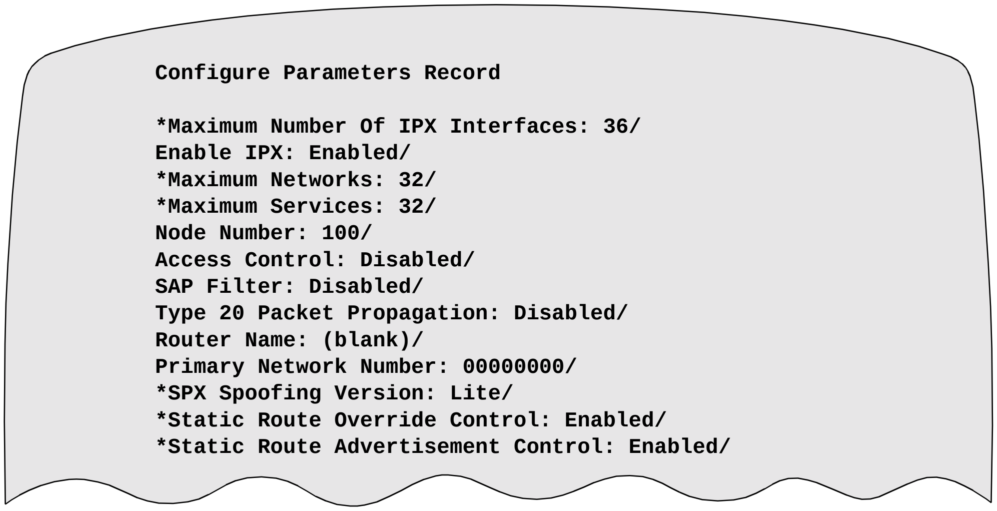
IPX Parameters

Introduction

Configuring IPX parameters lets you set up networks, services, and filters that effect the overall routing of IPX packets.

Configure Parameters Record

Figure 5 lists the parameters in the Configure Parameters Record.



```
Configure Parameters Record

*Maximum Number Of IPX Interfaces: 36/
Enable IPX: Enabled/
*Maximum Networks: 32/
*Maximum Services: 32/
Node Number: 100/
Access Control: Disabled/
SAP Filter: Disabled/
Type 20 Packet Propagation: Disabled/
Router Name: (blank)/
Primary Network Number: 00000000/
*SPX Spoofing Version: Lite/
*Static Route Override Control: Enabled/
*Static Route Advertisement Control: Enabled/
```

Figure 5. Configure Parameters Record

Parameters

These parameters make up the IPX Parameters Table Record:

■**Note**

Unless otherwise indicated, you must “Boot IPX Parameters”, for changes to these parameters to take effect. See “Booting IPX Parameters and Tables” on page 8.

■**Note**

Parameters that require a Node boot are identified with an asterisk in the parameter name.

*Maximum Number of IPX Interfaces

Range:	36 to 1000
Default:	36
Description:	Specify the maximum number of interfaces configurable for IPX. It is used to define the high range for IPX interface number.

Enable IPX

Range:	Disabled, Enabled
Default:	Disabled
Description:	Enables or disables overall routing of Internet Protocol Exchange (IPX) packets, the principal transport protocol for Novell Netware. Set this parameter to permit Novell workstations to connect to remote file and printer servers.

*Maximum Networks

Range:	1 to 4000
Default:	32
Description:	Size of the IPX RIP table. Set this parameter greater than the number of the LANs, serial links, and routers in the IPX Internetwork. IPX RIP is a different protocol than the IP RIP, and operates whenever IPX is enabled. It permits the router to identify which interface it should forward packets to for particular IPX network numbers.

*Maximum Services

Range:	1 to 4000
Default:	32
Description:	Size of the IPX SAP table. Set this parameter greater than the number of the file server, gateway/routers, and print servers in the IPX internetwork.

Node Number

Range:	1 to 12 hexadecimal digits
Default:	0
Description:	Used as the IPX source node address for all locally generated IPX packets transmitted on serial links. If this parameter is configured as zero, the MAC address of the LAN in Interface 1 is used as the default source node number. Set this parameter to a non-zero value if no LAN port is installed as Interface 1.

Access Control

Range:	Disabled, Enabled
Default:	Disabled
Description:	Globally enables or disables the IPX Access Controls feature, as configured with Access Control records (see Access Controls Menu). The Access Controls feature permits the router to explicitly include or exclude IPX packets based on their IPX destination and/or source Network/Host/Socket. When Access Controls is enabled, the packet must match an inclusive Access Controls record in order to be forwarded. The Access Controls records are searched in order. If the first matching record is inclusive, the packet is dropped. It is highly recommended that the last Access Controls Record be an inclusive “wild card” record that matches all packets.

SAP Filter

Range:	Disabled, Enabled
Default:	Disabled
Description:	Globally enables or disables the IPX SAP filter function, as configured with the SAP Filter records (see IPX SAP Filter menu). The SAP Filter prevents Novell bindery overflows by restricting the maximum number of hops to learned services. A typical SAP filter restricts Service Type 4 (Filter Service) to not more that six hops. SAP filters are not required for most Novell networks.

Default SAP Action

Range:	PASS, BLOCK
Default:	PASS
Description:	This parameter lets you specify one default action for all SAPs, such as file servers and printers, encountered by this router. This means you no longer have to configure separate entries in the SAP Filter Table for services you want to block from being advertised beyond this node. Specify the filtering action for services not configured in the SAP Filter Table. • PASS - means all services seen by the router, and not configured in the SAP Filter Table, will be installed in the SAP Table. • BLOCK - means all services seen by the router, and not configured in the SAP Filter Table, will not be installed in the SAP Table. If the SAP is configured in the router's SAP Filter Table, the decision to accept or block the SAP is determined by the hop count set in the Maximum Hop Count parameter in the SAP Filter Table. ■ **Note** This parameter appears only if the SAP filter is enabled.

Type 20 Packet Propagation

Range:	Disabled, Enabled
Default:	Disabled
Description:	Globally enables or disables type 20 packet propagation. When disabled, type 20 packets are discarded by the router. When enabled, type 20 packets are forwarded.

SPX Spoofing Version

Range:	Lite, Enhanced
Default:	Lite
Description:	• Lite - Determines when two communicating nodes begin exchanging keep alive packets, and starts spoofing them. The Lite spoofing version does not track the status of active sessions. It does quick processing and occupies minimum memory. Lite spoofing has the disadvantage of not reflecting the state of a node if it is inactive on one end of a communicating pair. For example, if the client side of an SPX session is out of service, the server node should be reset. However, it will not be reset due to the spoofing. If the server node is not reset, it will be unable to make a new connection with the client. • Enhanced - Overcomes the shortcoming described above. This option requires memory configuration to store SPX session state information such that inactivity at the remote end of a communicating pair is detected, and spoofing of the inactive node stops. A reset can be performed allowing a new connection to be made.

Static Route Override Control

Range:	Disable, Enable
Default:	Enable
Description:	Disables overwriting of static routes with RIP routes. If you enable this parameter, dynamically learned, better cost routes do not overwrite static routes in the Routing Table.

Static Route Advertisement Control

Range:	Disable, Enable
Default:	Enable
Description:	Enables or disables static route advertisement over the whole network. When this parameter is enabled, static routes are advertised to the network. When it is disabled, static routes are not advertised, so other routers cannot learn these routes.

Router Name

Range:	1 to 47 alphanumeric characters
Default:	Blank
Description:	Specifies a readable name that is used to identify the router for network management purposes. ■ **Note** This parameter is used by IPXWAN. Any changes to this parameter means that IPXWAN must renegotiate the IPX Network Number and the node number. IPXWAN renegotiation can be started by booting the LAN Connections on which IPXWAN is enabled.

Primary Network Number

Range:	00000000 to FFFFFFFF
Default:	00000000
Description:	Identifies the router within a unique IPX network number. This number must be unique within the IPX internetwork; that is, it must not match any other IPX network number attached to the router or any other router in the internetwork. This must be defined for IPXWAN. ■ **Note** This parameter is used by IPXWAN. Any changes to this parameter means that IPXWAN must renegotiate the IPX Network Number and the node number. IPXWAN renegotiation can be started by booting the LAN Connections on which IPXWAN is enabled.

Static Route IPX

What Is Static Route IPX?

The Static Route IPX feature enables IPX to work efficiently over dialed links. This feature minimizes and eliminates RIP and SAP overhead traffic on switched or permanent WAN connections, thereby conserving bandwidth for other uses. RIP and SAP messages can be turned off for On Demand SVC WAN links, allowing calls to be disconnected when there is no other user data to transmit.

Route discovery protocols periodically broadcast packets every 30 or 60 seconds. Unless the RIP and SAP broadcasts are "turned off," On Demand SVCs will never idle out. On Demand SVCs establish an X.25 call only when there is user data to send and subsequently terminate that call when there is no data for a configured interval. Unless disabled, regular RIP/SAP messages keep the connection active even when there is no user data.

For IP, Vanguard Applications Ware already supports the concept of "static routing." You can add static entries to the IP routing table, and can disable IP RIP broadcasts altogether.

■ **Note**

Both the IP and IPX network protocols use a "RIP" route discovery protocol. IP RIP and IPX RIP are different protocols, with different formats. Unless otherwise specified, this section refers to IPX RIP.

Static Route IPX Features

Several options for minimizing RIP and SAP overhead include:

- Static configuration of RIP and SAP tables on a per interface basis
- Configurable RIP and SAP Interval
- "Delta" update optionally disabled
- Keep Alive Spoofing
- Serialization spoofing

■ **Note**

RIP, SAP, and Keep Alive and Serialization Spoofing, are described beginning on page 75.

Using Delta Update and the Update Interval Increase

If you do not want to statically configure RIP and SAP, you can turn on Delta update and also set a desirable update interval (for example, one week). This provides an up-to-date database at a small dial line cost premium.

What Are Delta Updates?

Under normal RIP/SAP operation, any changes to the RIP or SAP table cause a "Delta update" packet to be sent, with only the changed route (or service). In large networks, these Delta updates are frequent, and can keep a dialed connection repeatedly active. The Send RIP/SAP Delta Updates parameter lets you disable this feature. In this case, only the full RIP/SAP updates as specified by the RIP/SAP update interval would be sent.

What Is the Update Interval Increase?

The RIP and SAP update interval can be set to a maximum of 10080 minutes (one week), meaning that an update can be set to occur just once a week. 1440 minutes (one day) is recommended for dial connections. The default is one minute, which is appropriate for permanent WAN connections.

Advantages to Static Route IPX

Configuring Static Route IPX operation is recommended if you:

- Use switched services, predominantly.
- Pay for WAN bandwidth on a per packet basis.

Configuration Considerations

Consider the following when configuring Static Route IPX.

- You must configure both the RIP and SAP tables in the router node.
- You should enable RIP and SAP on Interface Number 1 (LAN Interface) and leave the update frequency set to the default of one minute. You should either configure the WAN statically or increase the RIP/SAP time for the WAN.
- If not statically configured, then on a per interface basis, you must configure Delta updates and set Keep Alive updates to ON or OFF.
- RIP and SAP update frequency must be configured to the same value for all servers and routers on a network.
- Every Static Route has a cost associated with it. If RIP learns of a lower cost path to the same destination IPX address, it uses that path. However, if a lower cost path exists to the same destination router and a dial port is the primary route to that destination, the dial port will be used.

Recommended IPX Routing Configuration Values

This matrix provides recommended values when statically configuring IPX routing:

Parameter	*Permanent Link*	*Dial Link*
RIP Update Interval	LAN - 1 Minute	N/A
	WAN - 5 Minutes	WAN - 1440 Minutes (1 Day)
SAP Update Interval	LAN - 1 Minute	N/A
	WAN - 5 Minutes	WAN - 1440 Minutes (1 Day)
Advertise Delay	LAN - 1 tick	LAN - 1 tick
	T1 - 6 ticks	T1 - 6 ticks
	56K - 78 ticks	56K - 78 ticks
IPX RIP/SAP Split Horizon	PT_to_PT LCON - ENABLED	PT_to_PT LCON - ENABLED
	Group LCON - DISABLED	Group LCON - DISABLED
Enable RIP Delta	ENABLED	DISABLED
Enable SAP Delta	ENABLED	DISABLED
IPX Session Keep Alive Spoofing	ENABLED	DISABLED

Other Static Route IPX Features

Introduction

Release 5.1M, and greater, software enhances the IPX Static Routing feature to determine how static routing information is maintained when dynamically learned routes are available. Static Routing features include:

- IPX Static Route Relearning
- IPX Static Route Override Control
- IPX Static Route Advertisement Control

What Is IPX Static Route Relearning?

When a link associated with a static route fails, it is replaced with a dynamically learned route advertised from a neighboring router. When the failed link comes back up, it is not replaced in the routing table, even though it is a lower cost path. Static Route Relearning maintains the static route via the following options:

Case 1

You can enable or disable the Static Route Override parameter (refer to the Configure Parameters Record on page 9). This parameter allows you to disable static route overrides such that no learned entry can ever replace it, regardless of whether the link associated with this static route is up or down. Therefore, the above problem cannot occur. If you enable the override parameter, then cases 2 and 3 below handle these situations.

Case 2

When the link associated with the static route goes down, it is not replaced by any new path since one does not exist. When this link comes back up, it can be relearned as a static route in the routing table.

Case 3

When the link associated with the static route goes down, the entry in the routing table is replaced by a dynamically learned one. When the dynamically learned route ages out and is marked as unreachable, you can replace it with this static route in the routing table.

Case 4

If the dynamic route is learned on a different network interface, then when the failed link associated with the static route comes back up, you can check whether it is a better cost route and replace the dynamic route in the routing table.

Case 5

If static route overrides are disabled and an interface comes up, the direct route associated with the interface does not replace the static route even though the direct route may offer better cost. If the static route is using some other interface, the static routes associated with that interface are not updated even if it is active.

IPX Static Route Override Control

This feature allows you to configure whether static routes remain in the routing table or whether they are overwritten by learned (better cost) IPX RIP routes. (Refer to the Configure Parameters Record on page 9.)

IPX Static Route Advertisement Control

When broadcasting information from the routing table, this feature lets you configure whether or not static routes are included in advertisements. If you disable the parameter, information about any of the static route entries in the routing table are not advertised during routing information broadcasts. (Refer to the Configure Parameters Record on page 9.)

Parallel SVCs (Bandwidth on Demand)

Introduction

Parallel SVCs for IPX traffic are supported with Release 5.0 and greater software. The Parallel SVC feature, also known as Bandwidth on Demand, is identical to that described for IP traffic in the *IP Routing Manual* (Part Number T0100-03) with one exception.

Parallel SVC support for IPX can change the sequence in which the packets arrive at the end application. Parallel SVC support for IPX on the Vanguard routers does not include support for sequencing packets. The parallel SVC feature on the node, assumes that the IPX applications are capable of handling out of sequence packets.

What Is Bandwidth on Demand?

Bandwidth on Demand (BoD) refers to the ability to activate additional incremental wide area bandwidth for IPX traffic, on a packet-by-packet basis, when congestion thresholds are exceeded on the primary SVC. This incremental bandwidth can be:

- Additional X.25 SVCs on the same or a different physical port.
- An external dial modem, ISDN-terminal adapter, or Switched-56 device connected to a different physical port.

How Bandwidth on Demand Works

When a configured threshold of congestion is reached on a primary SVC, a Bandwidth on Demand, or parallel SVC can be activated. Vanguard nodes queue up and transmit packets over the parallel SVC, until congestion ceases on the primary link. Once congestion on the primary link ceases, packets queued to the parallel SVC are redirected to the primary SVC.

If parallel SVCs stay idle for longer than the configured idle time, they are terminated.

Example

Figure 6 shows a Bandwidth on Demand connection assisting the primary link. Note that On Demand links can be ISDN B channel, as shown in the figure.

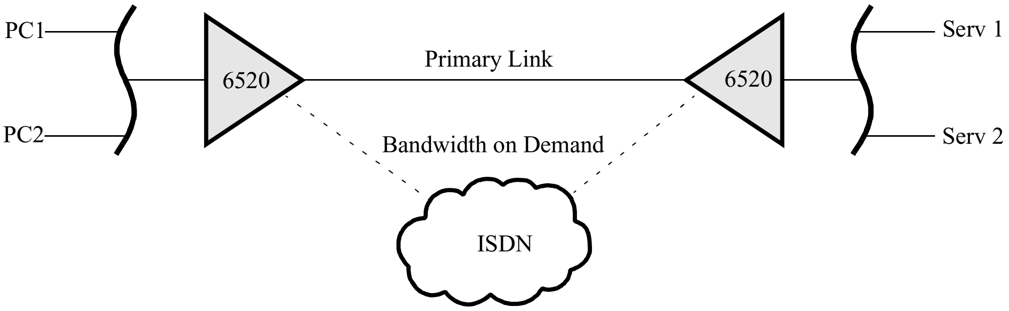


Figure 6. Bandwidth on Demand Connection

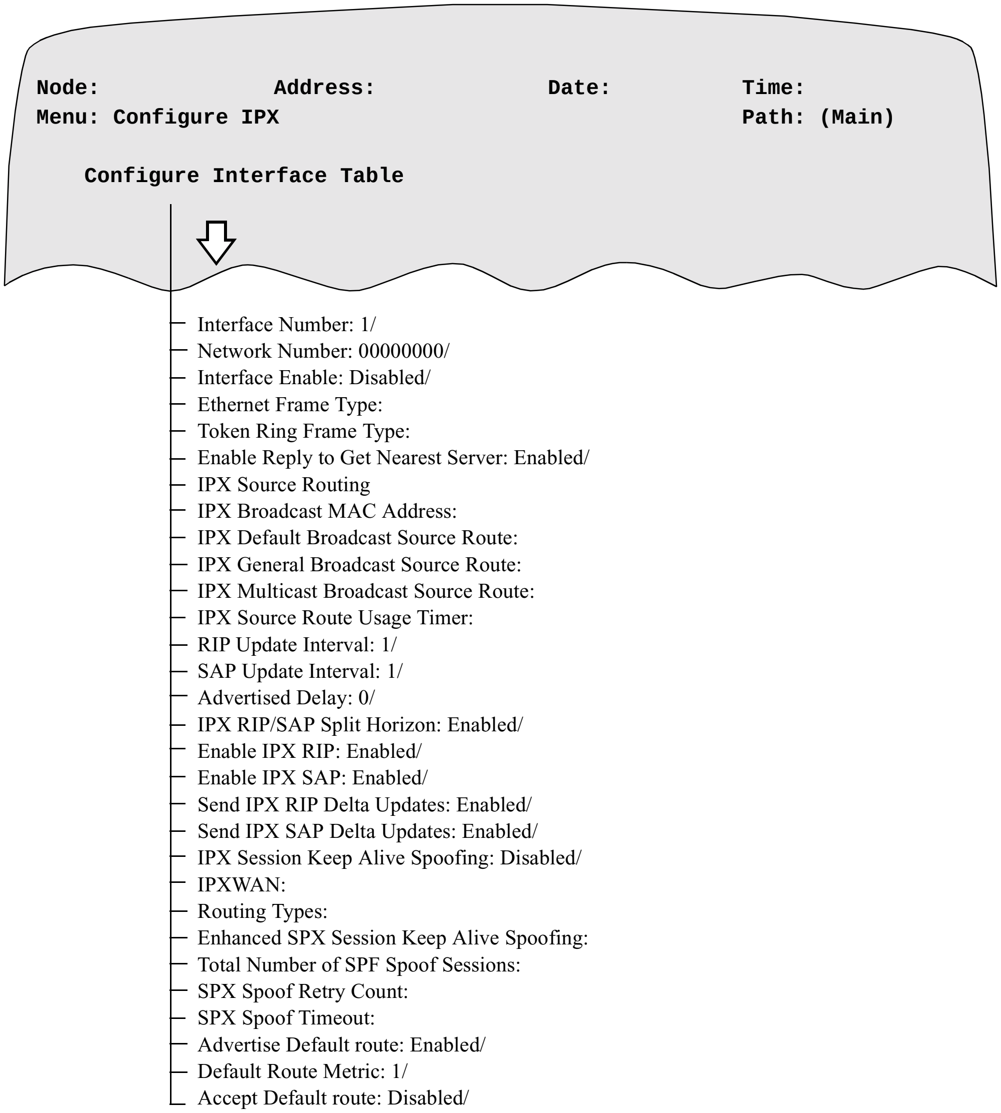
IPX Interfaces

Introduction

For IPX, each interface can have only one IPX network number. For all Router protocols (IP and IPX), a network number can be assigned to only one interface.

Interface Configuration Table Record

Figure 7 shows the Interface Configuration Table record.



```
Node:                Address:              Date:          Time:
Menu: Configure IPX                                       Path: (Main)

    Configure Interface Table
```

Interface Number: 1/
Network Number: 00000000/
Interface Enable: Disabled/
Ethernet Frame Type:
Token Ring Frame Type:
Enable Reply to Get Nearest Server: Enabled/
IPX Source Routing
IPX Broadcast MAC Address:
IPX Default Broadcast Source Route:
IPX General Broadcast Source Route:
IPX Multicast Broadcast Source Route:
IPX Source Route Usage Timer:
RIP Update Interval: 1/
SAP Update Interval: 1/
Advertised Delay: 0/
IPX RIP/SAP Split Horizon: Enabled/
Enable IPX RIP: Enabled/
Enable IPX SAP: Enabled/
Send IPX RIP Delta Updates: Enabled/
Send IPX SAP Delta Updates: Enabled/
IPX Session Keep Alive Spoofing: Disabled/
IPXWAN:
Routing Types:
Enhanced SPX Session Keep Alive Spoofing:
Total Number of SPF Spoof Sessions:
SPX Spoof Retry Count:
SPX Spoof Timeout:
Advertise Default route: Enabled/
Default Route Metric: 1/
Accept Default route: Disabled/

Figure 7. Interface Configuration Table Record

Parameters

These parameters make up the IPX Interfaces Configuration Table Record:

■ **Note**
Unless otherwise indicated, you must "Boot IPX Tables" for changes to these parameters to take effect. See "Booting IPX Parameters and Tables" on page 8.

Entry Number

Range:	1 to 1024
Default:	1
Description:	Used to reference this table record.
Boot Type:	A Table or Node Record boot is required.

Interface Number

Range:	1, 5 to 36
Default:	5
Description:	Each interface must be assigned an Interface Number. Interface Number 1 must be assigned to the LAN port. Interface Numbers 5 through 36 are reserved for LAN connections, which are virtual circuit links over WAN networks such as X.25 or Frame Relay to other routers. The Interface Number must match the interface number configured for the LAN connection. The router "network number" reported in log messages is considered to be one less than the Interface Number. For example, Interface 1 is Network 0.

Network Number

Range:	00000000 to FFFFFFFF
Default:	00000000
Description:	A 4-byte Novell network number assigned to the network attached to the corresponding interface. Every Novell LAN and serial link must be assigned a unique network number. IPX network numbers are entered with up to 8 hexadecimal digits, such as 0000 030A or just 30A. ■ **Note** All changes to the routing table result in the generation of a "Delta" updates. These are sent out on all interfaces on which updates are enabled for RIP.

Interface Enable

Range:	Enabled, Disabled
Default:	Disabled
Description:	Enables or disables IPX routing on the particular interface corresponding to this entry. An interface is the connection of the router to a network such as a LAN or a WAN virtual circuit. For IPX routing, the Enable IPX parameter must be enabled in addition to this parameter for all active interfaces.

Ethernet Frame Type

Range:	802.3, II, 802.2, SNAP
Default:	802.2
Description:	Selects the frame type for IPX if the interface is an Ethernet LAN. All Novell servers, workstations, and routers on a particular Ethernet network must be configured with the same IPX frame type. This parameter is displayed only for Ethernet LAN interfaces.The router recognizes and transmits only packets with the configured frame type. • The 802.3 setting corresponds to Novell's ETHERNET_802.3 packet format, which was the original default for Novell networks. • The II setting corresponds to Novell's ETHERNET_II frame type, which is the default for Novell 3.12 and later. • The 802.2 setting corresponds to Novell's ETHERNET_802.2 frame type. • The SNAP setting corresponds to Novell's ETHERNET_SNAP frame type.

Token Ring Frame Type

Range:	802.2, SNAP
Default:	802.2
Description:	Selects the frame type with which IPX frames are encapsulated on a token ring network. The router recognizes and transmits packets with only the configured frame type. This parameter is displayed only for a Token Ring LAN interface. • The 802.2 setting corresponds to Novell's TOKEN-RING frame type, and is Novell's default for token ring networks. With this frame type, IPX packets are encapsulated with an IEEE 802.2 header using DSAP 0xE0. • The SNAP setting is for Novell's TOKEN-RING_SNAP frame type. With this frame type, IPX packets are encapsulated with the SNAP header defined in RFC 1042 using the IPX protocol number 0x8137.

Enable Reply to Get Nearest Server

Range:	Enable, Disable
Default:	Enable
Description:	Enables the router to reply to a SAP Get Nearest Server request from the workstation. It is required for the workstation to be able to log into a remote server, and so is usually enabled. A router configured as a parallel “hot standby” may need to disable this parameter to prevent workstations from using a higher-cost backup link. ■ **Note** When you disable this parameter, the router does not respond to Get Nearest Server or General Server requests.

IPX Source Routing

Range:	Enabled, Disabled
Default:	Disabled
Description:	Enables or disables source route operation on the token ring. This parameter is displayed only for a Token Ring LAN interface. When source routing is enabled, all IPX packets transmitted contain a Routing Information Field (RIF) allowing them to be forwarded with IBM source route bridges. All of the bridged rings are considered to be on the same IPX Network number. Enabling source routing corresponds to including the Novell ROUTE module in a workstation or server configuration.

IPX Broadcast MAC Address

Range:	Broadcast, Functional
Default:	Broadcast
Description:	Destination MAC address for transmitted IPX broadcasts on an unbridged token ring. This parameter is displayed only for a Token Ring LAN interface. “B” or “F” may be entered as abbreviations. The destination MAC address values are: • Broadcast: FFFFFFFFFFFF • Functional: C00000800000 When IPX Source Routing is enabled, this parameter is ignored, and all IPX broadcasts are transmitted using the Broadcast (all FFs) MAC address.

IPX General Broadcast Source Route

Range:	SRB, ARB
Default:	SRB
Description:	General Broadcast source route field to use when the router transmits an IPX broadcast frame. Recent standards recommend Source Route Broadcast (SRB), but older IBM source route bridges may only be able to forward All Routes Broadcast (ARB) frames. This corresponds to Novell's “GBR” parameter in the ROUTE module. This parameter is displayed only for a Token Ring LAN interface.

RIP Update Interval

Range:	1 to 10080 (1 week)
Default:	1
Description:	Indicates in minutes the interval between periodic RIP updates. Novell routes are allowed to be replaced if no routing updates are received within two times the value of the update interval. Novell routes are marked as unreachable (16 hops) if no routing updates are received within three times the value of the update interval. Novell routes are removed from the routing table if no routing updates are received within four times the value of the update interval.

SAP Update Interval

Range:	1 to 10080 (1 week)
Default:	1
Description:	Indicates in minutes the interval between periodic SAP updates. SAP entries are allowed to be replaced if no routing updates are heard within two times the value of the update interval. SAP entries are marked as unreachable (16 hops) if no SAP updates are received within three times the value of the update interval. SAP entries are removed from the routing table if no SAP updates are received within four times the value of the update interval.

Advertised Delay

Range:	0 to 65535
Default:	0
Description:	Specify the advertised number of IBM PC “ticks” (18ths of a second) to transmit a maximum size frame on the interface. If this parameter is 0, the router automatically calculates the advertised link delay value. You may want to manually configure larger delay values for interfaces that experience unusually large packet transmission delays due to very large packet sizes (over 1500 bytes) or unusually slow links (less than 19.2 kbps). LAN interfaces to bridged networks may need to be manually configured to a delay such as 5 ticks.

IPX RIP/SAP Split Horizon*

Range:	Enabled, Disabled
Default:	Enabled
Description:	Enables or disables the IPX RIP/SAP Split Horizon. Split Horizon prevents routes or services from being advertised over the same interface they were learned on. This helps reduce the formation of routing loops. You may not want to enable Split Horizon when the interface is tied to a LAN connection group, which emulates a broadcast WAN network. In such cases, Split Horizon should be disabled.

Enable IPX RIP

Range:	Enabled, Disabled
Default:	Enabled
Description:	When enabled, the router sends and receives IPX Routing Interface protocols per Novell standards. When disabled, the router neither generates nor accepts RIP updates on interfaces. Disabled IPX RIP operation may be appropriate for dial-on-demand switched WAN links. ■ **Note** Initial RIP queries are not sent when RIP is enabled. RIP updates are sent out at regular update intervals.

Enable IPX SAP

Range:	Enabled, Disabled
Default:	Enabled
Description:	When enabled, the router sends and receives IPX Service Advertising Protocols per Novell standards. When disabled, the router neither generates nor accepts SAP updates on interfaces. Disabled IPX SAP operation may be appropriate for dial-on-demand switched WAN links. ■ **Note** Initial SAP queries are not sent when SAP is enabled. SAP updates are sent out at regular update intervals.

Send IPX RIP Delta Updates

Range:	Enabled, Disabled
Default:	Enabled
Description:	Controls whether changes to the Routing Table cause “Delta” RIP packets to be sent immediately on this interface when the change is detected. You may want this for permanently connected WAN circuits and for LAN interfaces. For dialed WAN circuits, however, these Delta updates force a new call to be dialed if the circuit is not currently active. If you have large networks, you may want to disable this feature on dialed interfaces to reduce the number of calls.

Send IPX SAP Delta Updates

Range:	Enabled, Disabled
Default:	Enabled
Description:	Controls whether changes to the SAP Services Table cause “Delta” SAP packets to be sent immediately on this interface when the change is detected. You may want this for permanently connected WAN circuits and for LAN interfaces. For dialed WAN circuits, however, these Delta updates force a new call to be dialed if the circuit is not currently active. If you have large networks, you may want to disable this feature on dialed interfaces to reduce the number of calls.

IPX Session Keep Alive Spoofing

Range:	Enabled, Disabled
Default:	Disabled
Description:	Controls whether the router spoofs Client responses to Server Keep Alive requests received on this interface and destined for On Demand (dial) connections not currently active. Remote workstations can maintain their Server login connectivity even after the On Demand connection has gone down. Enable Keep Alive Spoofing for Dial-on-Demand switched WAN links. This should be enabled only on a LAN Interface.

IPXWAN

Range:	Enabled. Disabled
Default:	Disabled
Description:	Enables or disables the IPX WAN on the interface. When Enabled, the IPX WAN protocol operates on the link as defined in RFC-1634. ■ **Note** This parameter is only displayed when the node is connected to a WAN interface.

Routing Types

Range:	0 to 4
Default:	0
Description:	Specifies the list of protocol types that would be included in the Timer request packets for negotiation. • 0; Numbered RIP/SAP • 1; Netware Link State Protocol • 2 ; Unnumbered RIP/SAP • 3; On Demand Static Routing • 4; Workstation Connectivity ■ **Note** Options 1, 3, and 4 are not supported by Vanguard Applications Ware Release 5.2. ■ **Note** The parameter can be a combination of the above (for example, 1,0,2). The order of specification also determines the preference.

Enhanced SPX Spoofing

Range:	Enable, Disable
Default:	Disable
Description:	Spoofs SPX Keep Alive packets for all registered SPX connections on the network interface, with the ability to detect an inactive SPX session and perform a reset. This allows new connections to be established without delay, while ensuring spoofing is not performed for a node that is not operational.

Total Number of SPX Spoof Sessions

Range:	10 to 65535
Default:	10
Description:	Represents the number of SPX sessions for which spoofing is supported. The router discards all SPX session related information that it had before the parameter was changed. This information is recreated after a Table boot is performed.

SPX Spoof Timeout

Range:	3 seconds to 3000 seconds
Default:	30 seconds
Description:	Specifies a communicating entity as being active if Keep Alive packets are received periodically and within the time interval specified here.

SPX Spoof Retry Count

Range:	3 to 50
Default:	10
Description:	Specifies the number of timeouts allowed before a communicating entity is described as non-operational.

Advertise Default Route

Range:	Enable, Disable
Default:	Disable
Description:	Enables and disable the default route on this interface.

Default Route Metric

Range:	Enable, Disable
Default:	Disable
Description:	Enables and disables accepting the default route on this interface.

Accept Default Route

Range:	1 to 16
Default:	1
Description:	Specifies metric for default route on this interface.

IPX Service Advertising Protocol (SAP) Filters

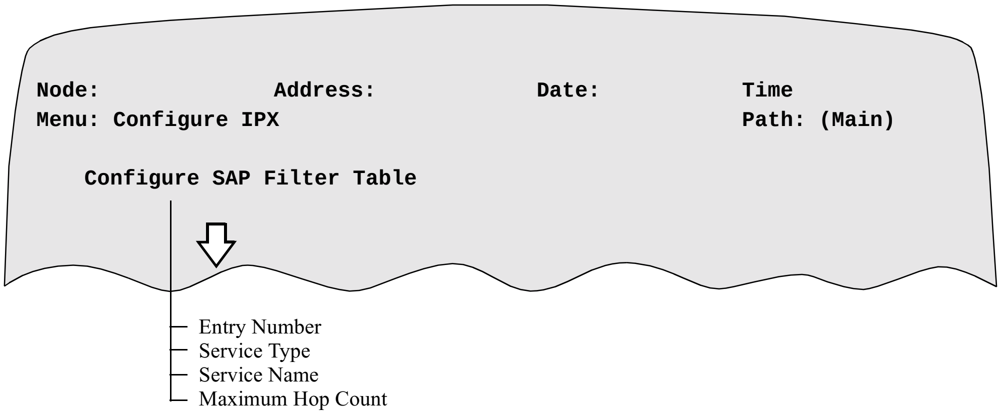
Introduction

Every Vanguard router maintains a SAP services table to locate NetWare services such as printers and file servers. The router and periodically (typically every 60 seconds) re-advertises these services. The SAP Filter Table restricts what is loaded into a SAP table.

You can also configure a default action to block or pass all services encountered by this router node. See the Default SAP Action parameter in the “IPX Interfaces” section on page 20 for details.

Configure SAP Filter Table Record

Figure 8 shows the Configure SAP Filter Table record.



```
Node:               Address:               Date:            Time
Menu: Configure IPX                                         Path: (Main)

    Configure SAP Filter Table
```

Figure 8. Configure SAP Filter Table Record

Parameters

These parameters make up the IPX SAP Filter Configuration Table Record:

■ **Note**

Unless otherwise indicated, you must “Boot IPX Tables” for changes to these parameters to take effect. See “Booting IPX Parameters and Tables” on page 8.

Entry Number

Range:	1 to 255
Default:	1
Description:	Entry number used to reference this record.
Boot Type:	A Table or Node boot is required.

Service Type

Range:	0 to FFFF
Default:	0000
Description:	A hexadecimal number that you must enter as a SAP Service Type code. The most common code is 4 for a file server. Other codes include 3 for Print Queue and 5 for Job Server. The SAP Filter prevents Novell bindery overflows by restricting the maximum number of hops to a learned server. A typical SAP Filter is used to restrict server type 4 (File Server) to no more than 6 hops. SAP Filters are not required for most Novell networks.

Service Name

Range:	0 to 47 alphanumeric characters. (Use the space bar to blank the field.)
Default:	(blank)
Description:	This field is usually left blank, in which case the SAP Filter record applies to all servers of the type in the Service Type field. If the field is not blank, it must match exactly the name of a particular server, and the filter record applies only to that server.

Maximum Hop Count

Range:	0 to 15
Default:	1
Description:	Specify the maximum number of hops (in decimal) that a service may be away in order for the router to include the service in its SAP Table. Each traversed LAN or serial LAN connection counts as one hop. IPX automatically considers any service with a hop count value of 15 or more as unreachable. By specifying a hop count smaller than 15, distant services can be disabled from automatic inclusion in the SAP table, thereby avoiding network bindery overflows. This feature is needed only on extremely large Novell internetworks.

IPX Access Controls

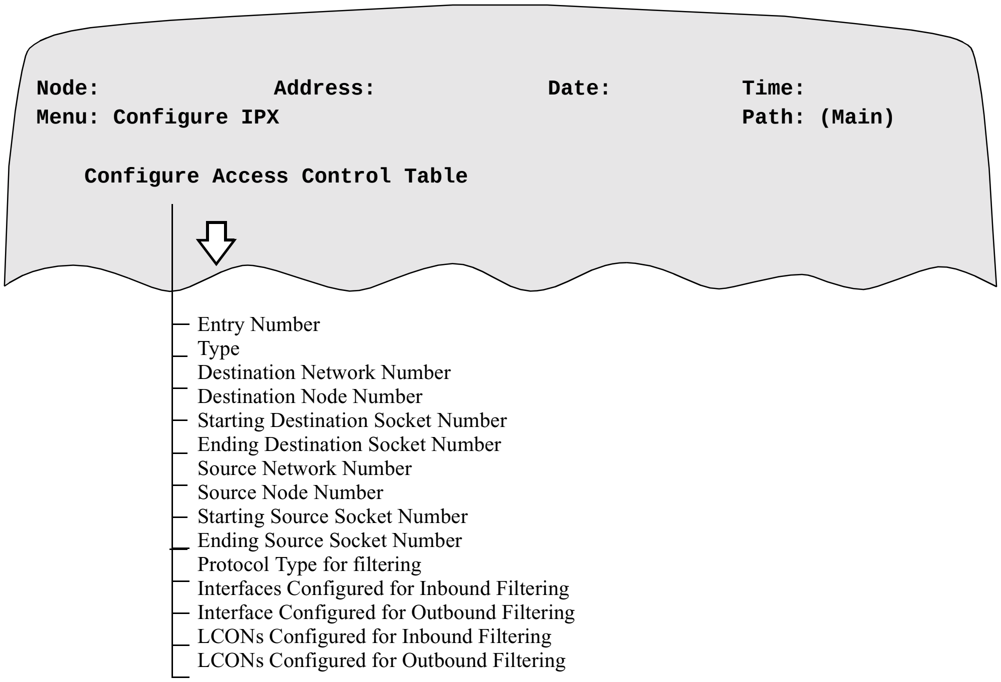
Introduction

The IPX Access Controls feature lets the router explicitly include or exclude IPX packets based on their IPX destination and/or source Network/Host/Socket. When Access Controls are enabled, the packet must match an inclusive Access Controls record in order to be forwarded.

Release 5.1M and greater software also allows you to filter packets on a protocol type, interface (as opposed to node), and LCON basis. In addition, you can also define whether filtering occurs on inbound or outbound traffic.

Configure Access Control Table Record

Figure 9 shows the Configure Access Control Table record.



```
Node:               Address:             Date:          Time:
Menu: Configure IPX                                     Path: (Main)

   Configure Access Control Table
```

Entry Number
Type
Destination Network Number
Destination Node Number
Starting Destination Socket Number
Ending Destination Socket Number
Source Network Number
Source Node Number
Starting Source Socket Number
Ending Source Socket Number
Protocol Type for filtering
Interfaces Configured for Inbound Filtering
Interface Configured for Outbound Filtering
LCONs Configured for Inbound Filtering
LCONs Configured for Outbound Filtering

Figure 9. Configure Access Control Table Record

Parameters

These parameters make up the IPX Access Control Configuration Table Record:

■ **Note**

Unless otherwise indicated, you must “Boot IPX Tables”, for changes to these parameters to take effect. See “Booting IPX Parameters and Tables” on page 8.

■ **Note**

Parameters that require a Node boot are identified with an asterisk in the parameter name.

Entry Number

Range:	1 to 255
Default:	1
Description:	Used to reference this Access Control Record.
Boot Type:	A Table and Node Record boot is required.

Type

Range:	Exclude, Include
Default:	Include
Description:	Each entry in this table defines an Access Control Record that describes a pattern an IPX packet must match. The Exclude/ Include type field of the record controls whether a packet matching the pattern is excluded (dropped) or included (forwarded). A packet must match all fields of the Access Control Record in order to be considered to match the record. If the Access Control feature is used, it is highly recommended that the last entry in the table be a "wild card" pattern matching all packets with an Include type. Refer to the Access Control parameter in the section "IPX Parameters," earlier in this document, to globally enable or disable the Access Control features.

Destination Network Number

Range:	00000000 to FFFFFFFF hexadecimal
Default:	00000000
Description:	The IPX Destination Network Number is a maximum 4-byte value entered in hexadecimal notation. A value of 00000000 is a "wild card" value that matches any destination network number.

Destination Node Number

Range:	1 to 12 hexadecimal digits
Default:	0
Description:	This value represents the IPX Destination Node Number. If nonzero, a packet must have a destination address that matches this value in order to match the Access Control record. A value of zero is a "wild card" value that matches all packets.

Starting Destination Socket Number

Range:	0000 to FFFF hexadecimal
Default:	0000
Description:	The beginning of a range of IPX socket numbers to which the packet's destination socket number is compared. IPX socket numbers are entered in hexadecimal notation. Common IPX socket numbers include: • 0451; Netware Core Protocol (NCP) • 0452; Service Advertising Protocol (SAP) • 0453; Routing Information Protocol (RIP) • 0455; Novell NETBIOS Process • 0456; Diagnostic Process A value of 0000 is a "wild card" value that matches any packet's destination socket number.

Ending Destination Socket Number

Range:	0000 to FFFF
Default:	FFFF
Description:	The end of a range of IPX socket numbers to which the packet's destination socket number is compared. IPX socket numbers are entered in hexadecimal notation. A value of FFFF is a "wild card" value that matches any packet's destination socket number.

Source Network Number

Range:	00000000 to FFFFFFFF
Default:	00000000
Description:	The IPX Source Network Number. Enter this maximum 4-byte value in hexadecimal notation. A value of 00000000 is a "wild card" value that matches any source network number.

Source Node Number

Range:	1 to 12 hexadecimal digits
Default:	0
Description:	This is the IPX Source Node Number. If non-zero, a packet must have a source address that matches this value in order to match the Access Control record. A value of zero is a "wild card" value that matches all packets.

Starting Source Socket Number

Range:	0000 to FFFF
Default:	0000
Description:	The beginning of a range of IPX socket numbers to which the packet's source socket number is compared. IPX socket numbers are entered in hexadecimal notation. Common IPX socket numbers include: • 0451; Netware Core Protocol (NCP) • 0452; Service Advertising Protocol (SAP) • 0453; Routing Information Protocol (RIP) • 0455; Novell NETBIOS Process • 0456; Diagnostic Process A value of 0000 is a "wild card" value matching any packet's source socket number.

Ending Source Socket Number

Range:	0000 to FFFF
Default:	FFFF
Description:	The end of a range of IPX socket numbers to which the packet's destination socket number is compared. IPX socket numbers are entered in hexadecimal notation. A value of FFFF is a "wild card" value that matches any packet's socket number.

Protocol Type for Filtering

Range:	0 to 255, ALL
Default:	ALL
Description:	The IPX protocol type with which the packet's protocol type is compared. Common IPX protocol types include: • 5: sequenced Packet Exchange (SPX) • 17: Netware Core Protocol (NCP) • 20: NetBIOS Type 20 If configured as ALL, this parameter is not considered for filtering.

Interfaces Configured for Inbound Filtering

Range:	1 to 254, ALL, NONE
Default:	ALL
Description:	Specifies a list of interfaces on which received packets are filtered. You can configure this parameter as a list. The number of ranges in the list is limited to 8. For example: 1, 5, 7 - 10 If you specify NONE, the action is not applied on any LCON. If you specify ALL (default), all interfaces are selected.

Interfaces Configured for Outbound Filtering

Range:	1 to 254, ALL, NONE
Default:	ALL
Description:	A list of interfaces on which received packets are filtered. You can configure this parameter as a list. The number of ranges in the list is limited to 8. Ex: 1, 5, 7-10 If you specify NONE, the action is not applied on any LCON. If you specify ALL (default), all interfaces are selected.

LCONs Configured for Inbound Filtering

Range:	1 to 2000, NONE, ALL
Default:	ALL
Description:	A list of LAN connections on which received packets are filtered. You can configure this parameter as a list. The number of ranges in the list is limited to 8. This is primarily intended for Grouped LCON usage. Since a single interface can comprise multiple LCONs, LCON-based filtering is considered useful. For example: 1, 5, 7- 10 If you specify NONE, the action is not applied on any LCON. If ALL is specified, all LCONs are selected.

LCONs Configured for Outbound Filtering

Range:	1 to 2000, NONE, ALL
Default:	ALL
Description:	A list of LAN connections on which routed packets are filtered. The filter is applied to packets routed on these connections. You can configure this parameter as a list. The number of ranges in the list is limited to 8. This is primarily intended for Grouped LCON usage. Since a single interface can comprise multiple LCONs, LCON-based filtering is considered useful. For example: 1, 5, 7 - 10 If you specify NONE, the action is not applied on any LCON. If ALL is specified, all LCONs are selected.

Considerations for Filtering

Configuration Considerations

Consider the following when configuring filtering:

- Whenever an entry or flow element is matched, only the parameters other than LCONs and Interfaces are considered for matching.
- If an entry or flow element has matched, and if the LCON/Interface matches the entry's LCON/Interface, then the corresponding action is taken.
- If an entry or flow element has matched, and if the LCON/Interface does NOT match the entry's LCON/Interface list, then opposite action is taken.

Interpretation of Action for Inbound and Outbound Filtering

Refer to the table below for a description of action when inbound or outbound filtering is applied to LCONs and interfaces:

Type of Action	*LCONs Configured for Inbound and Outbound Filtering*	*Interfaces Configured for Inbound and Outbound Filtering*	*Action*
Include/ Exclude	ALL	ALL	Action configured. Filtering applied on ALL LCONs and Interfaces configured.
Include/ Exclude	ALL	A set of interfaces	Filtering applied on all LCONs with the action configured. Interface set defined will be applicable for interfaces 1-4.
Include/ Exclude	ALL	NONE	Filtering applied on all LCONs with action configured. For interfaces 1-4, opposite of the configured action will be taken.

Type of Action	LCONs Configured for Inbound and Outbound Filtering	Interfaces Configured for Inbound and Outbound Filtering	Action
Include/ Exclude	None	ALL	Action configured. Filtering applied on all interfaces configured.
Include/ Exclude	None	A set of interfaces	If the packet matches the defined flow elements then filtering will be applied on the set of defined interfaces. For packets which match the flow elements but do not match the set of interface, opposite of the action configured will be taken.
Include/ Exclude	None	None	For all packets which match the flow elements configured, opposite of the action configured will be taken.
Include/ Exclude	A set of defined LCONs	None	Action is taken if the packet matches the flow elements defined and the LCON number is within the LCON set defined. For those packets which match the flow elements but do not match the LCON set, the opposite of the configured action is taken. Packets from interface 1-4 do not belong to any LCON and therefore opposite of action configured will be taken.
Include/ Exclude	A set of defined LCONs	ALL	Configured action applied for all packets.
Include/ Exclude	A set of defined LCONs	A set of interfaces	For Inbound filtering: • If the packet matches the defined flow element and its LCON is within the defined set of LCONs, the configured action is taken. • For those packets which match the flow elements but do not match defined set of LCONs, the action is taken for the set of defined interfaces. If the interface is not within the defined set, the opposite action to that configured is taken. For Outbound filtering: • Filtering is applied to the set of defined interfaces first and then to the set of defined LCONs.

■ **Note**

For inbound packets, filtering based on LCONs is applied before filtering based on interfaces. To avoid filtering based on inbound LCONs, configure the "LCONs Configured for Inbound Filtering" parameter to NONE and configure a set of valid interfaces. For outbound packets, filtering based on interface is applied before filtering based on LCONs.

Example of Filtering

Suppose the following filter entry have been defined:

- Action = Exclude
- Destination Network = 555
- Interfaces Configured for Inbound Filtering = 1-10
- Interface Configured for Outbound Filtering = NONE
- LCONs Configured for Inbound Filtering = NONE
- LCONs Configured for Outbound Filtering = NONE

■ **Note**

Default values used for parameters not specified.

Any packet with destination network number of 555 and received on one of the interfaces in the set range (1-10), will be excluded. This means that the packet will be filtered out (EXCLUDED) and not forwarded to the next hop or router.

Suppose a packet arrive on interface 11 with a destination network number 555. Although the network number matches, the interface is out of the defined range of interfaces configured for inbound filtering. Therefore, the opposite action to that configured will occur. This means that the packet will be included and forwarded to the next hop or router.

Limitations

These limitations apply to filtering:

- Statistics do not include LCONs and interfaces.
- The last entry in the table should be a wild card pattern matching all packets, with a default action.

IPX Static Route Table

Introduction

You can use an IPX Static Route Table when RIP operation is disabled. Entries are loaded into the IPX route table at startup time. Invalid entries are ignored.

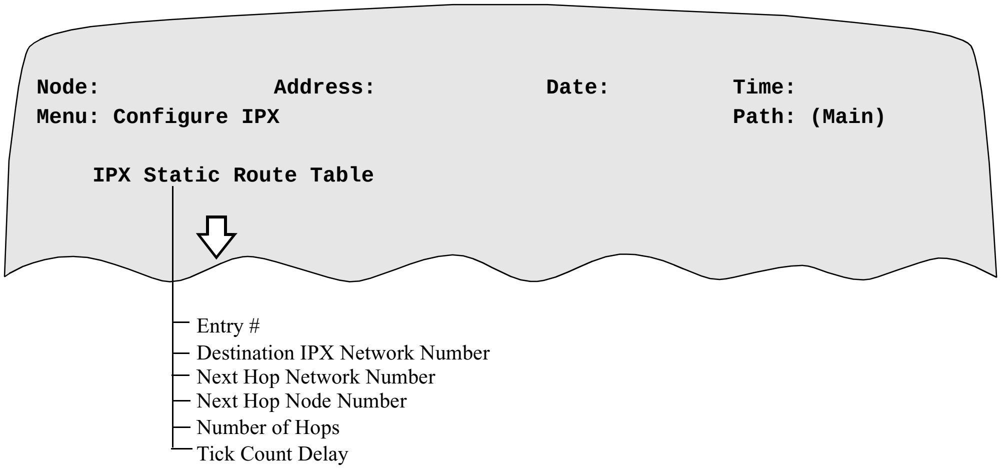
How It Works

This table shows how the IPX Static Route Table works:

<table>
<tr><th colspan="2">Action</th></tr>
<tr><td colspan="2">• At initialization, static entries are loaded into the operational RIP table with a hop count of 16 and a maximum delay.</td></tr>
<tr><th>When...</th><th>Then...</th></tr>
<tr><td>The interface for the next hop router comes up</td><td>The static table cost (hop count and delay) is entered into the table. Such routes are recorded in the operational table as RIP routes, and are aged.</td></tr>
<tr><td colspan="2">• Dynamically learned RIP routes can override static table entries, if their cost is better.</td></tr>
<tr><th>If...</th><th>Then...</th></tr>
<tr><td>A dynamically learned route ages out, or is learned to be unreachable</td><td>In this way, static routes over a dial-up link can be configured as a “backup” to the normally learned dynamic route.</td></tr>
<tr><td colspan="2">• Networks that contain a Static IPX Route Table entry are always advertised in the RIP packets sent from interfaces configured for RIP operation.</td></tr>
<tr><th>If...</th><th>Then...</th></tr>
<tr><td>The next hop network is down</td><td>The route is advertised as 16 hops, indicating an “infinite” cost.</td></tr>
</table>

IPX Static Route Table Record

Figure 10 shows the IPX Static Route Table record.



```
Node:                 Address:              Date:          Time:
Menu: Configure IPX                                        Path: (Main)

     IPX Static Route Table
```

Figure 10. IPX Static Route Table Record

Parameters

The IPX Static Route Table parameters are described in these tables:

■ **Note**
Unless otherwise indicated, you must “Boot IPX Tables” for changes to these parameters to take effect. See “Booting IPX Parameters and Tables” on page 8. When changes are made, dynamic information is not discarded except when static information overrides the dynamic information. Older static information is removed from the table. Changing the Routing Table generates RIP triggered updates.

Entry Number

Range:	1 to 65536
Default:	(blank)
Description:	Used to reference this table record.

Destination IPX Network Number

Range:	1 to 8 alphanumeric characters.
Default:	0
Description:	The IPX Static Route Table defines IPX routing table entries that are fixed in the table. It is most often used when RIP operation is disabled on the router or on certain interfaces. The route table requires a next hop in the form of an IPX Net and IPX Node number you define for every Destination IPX Network Number. If the default is entered, IPX packets that are otherwise unroutable are forwarded to the next hop defined by this record. ■ **Note** Use the space bar to blank this field.

Next Hop Network Number

Range:	00000000 to FFFFFFFF hexadecimal
Default:	00000000
Description:	Provides the network number of the router that is the next hop for packets addressed to the Destination IPX Net Number for this record. The Next Hop Network must be directly attached to the router. For a branch office, use the IPX Network Number assigned to the WAN link back to the home office.
Condition:	An entry of 0 will be rejected; you must enter a nonzero value. Also, at startup time, if an entry has a non-directly attached network, an error message is sent to the log and the record is ignored.

Next Hop Node Number

Range:	1 to 12 hexadecimal digits
Default:	0
Description:	Provides the 6-byte node number for the router that is the next hop for packets addressed to the Destination IPX Network Number of this record. For example, a branch office would set this to the Node Number assigned to the WAN link at the home office router.

Number of Hops

Range:	1 to 65535
Default:	1
Description:	Hop count associated with the destination network, as it would have been advertised by the next hop router. The hop count is the number of routers a packet must traverse in order to reach the destination IPX network.

Tick Count Delay

Range:	1 to 65535
Default:	6
Description:	The number of IBM PC clock "ticks" (measured as 1/18 second per tick) considered to be the delay to reach the destination network that would have been advertised by the next hop router. One useful formula for tick count is 10,000,000 divided by the link speed for the tick count. For instance, this gives a recommended tick count of: • Ethernet (10 Mbps) = 1 • T1 = 6 • 56K = 78

IPX Static SAP Table

Introduction

You can use the Static SAP table when SAP operation is disabled.

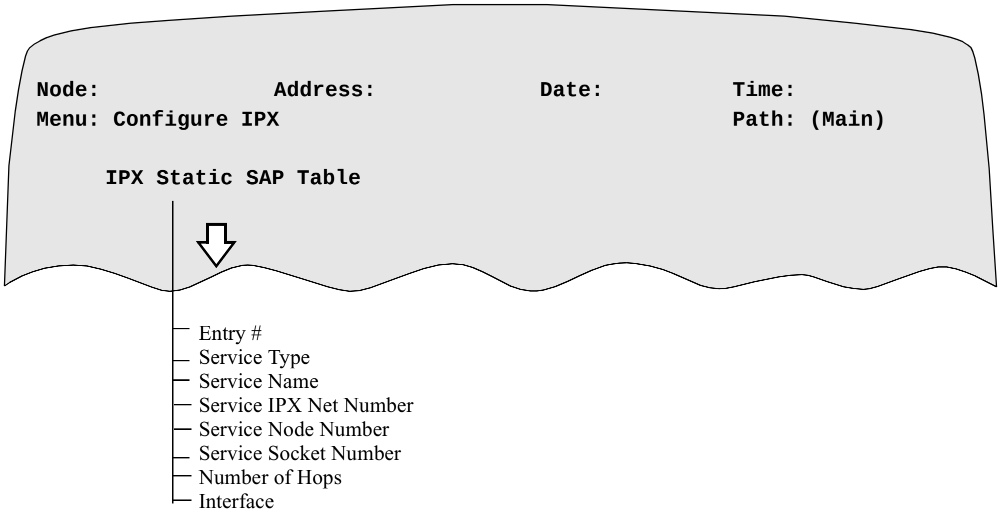
How the SAP Table Works

This table describes how the IPX static table works:

<table>
<tr><th colspan="2"><em>Action</em></th></tr>
<tr><td colspan="2">At router initialization, static SAP table entries are loaded into the operational SAP table, but with a hop count cost of 16 (the maximum cost).</td></tr>
<tr><th><em>When...</em></th><th><em>Then...</em></th></tr>
<tr><td>The Service IPX Net Number becomes “reachable” through the RIP process</td><td>The operational cost is changed to match the static configured cost.</td></tr>
<tr><td colspan="2">Static SAP table entries are always advertised in SAP messages, on those interfaces for which SAP is enabled.</td></tr>
<tr><th><em>When...</em></th><th><em>Then...</em></th></tr>
<tr><td>The Service IPX Net Number is unreachable through the routing table</td><td>The cost is advertised as 16 hops.</td></tr>
</table>

IPX Static SAP Table Record

Figure 11 shows the IPX SAP Table that you use when SAP operation is disabled.



```
Node:               Address:             Date:          Time:
Menu: Configure IPX                                     Path: (Main)

     IPX Static SAP Table
```

Figure 11. IPX Static SAP Table Record

Parameters

The IPX Static SAP Table parameters are described in these tables.

Only one static entry for a particular Type/Name combination can be entered. It is a configuration error to define two or more entries with the same Type/Name.

■ **Note**

Unless otherwise indicated, you must “Boot IPX Tables” for changes to these parameters to take effect. See “Booting IPX Parameters and Tables” on page 8. When changes are made, dynamic information is not discarded except when static information overrides the dynamic information. Older static information is removed from the table. Changing the SAP Table generates SAP triggered updates.

Entry Number

Range:	1 to 65536
Default:	(blank)
Description:	Used to reference this table record.

Service Type

Range:	0000 to FFFF hexadecimal
Default:	0000
Description:	Service Type Code for the service being defined. The most common service types are 4 for a File Server and 3 for a print queue.

Service Name

Range:	1 to 48 characters.
Default:	(blank)
Description:	Specifies the Novell Netware service name advertised for a Server, for example, “BOSTON_FILESERVER_1”. ■ **Note** All alphanumeric characters, hyphens, and underscores are valid IPX characters. The name cannot contain a period or space. The first character must be a number or letter. Use the space bar to blank the field.

Service IPX Net Number

Range:	00000000 to FFFFFFFF hexadecimal
Default:	00000000
Description:	The IPX network on which the service resides. For 3.X and later file servers, this should be the “internal network number” of the server.

Service Node Number

Range:	1 to 12 hexadecimal digits
Default:	0
Description:	A 6-byte node number that identifies the particular node on which the service is implemented. For 3.X and later File Servers, this should be the “internal node number” of the server.

Service Socket Number

Range:	0000-FFFF hexadecimal
Default:	0000
Description:	A 2-byte socket number to which server packets are addressed. For example, all File Servers (server type 0004) use socket 0451 for NetWare Core Protocol.

Number of Hops

Range:	1 to 15
Default:	1
Description:	The number of router hops required in order to reach the service.

Interface

Range:	1, 5 to 36
Default:	1
Description:	Specifies the interface through which the static entry is assumed to have been learned. The split horizon algorithm, when enabled, prevents re-advertising the service on this interface.

Reset IPX RIP, SAP, and SPX Spoofing Tables

Introduction

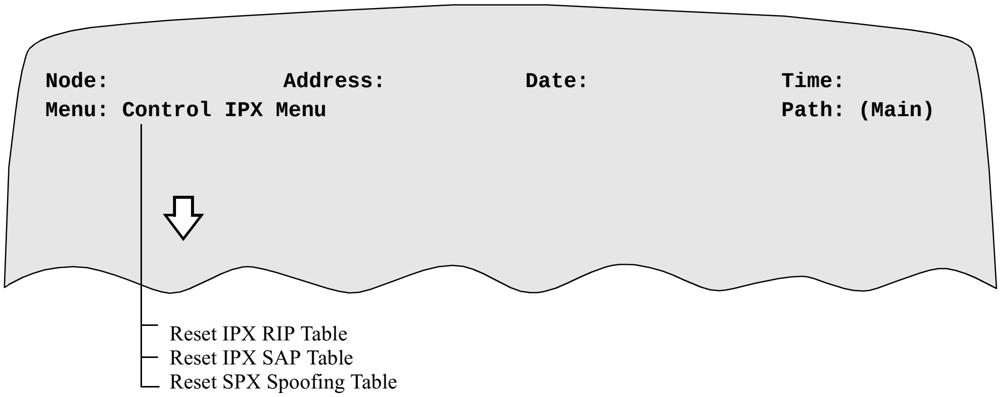
You use the Control IPX menu to reset the IPX RIP, SAP, and SPX Spoofing Tables to their default values. Figure 12 shows the Control IPX menu.

Follow these steps to access the Control IPX menu from the main CTP menu.

Step	Action	Result
1	Select **LAN Control Menu** from the CTP menu.	The LAN Control menu appears.
2	Select **Control Router**.	The Control Router menu appears.
3	Select **Control IPX**.	The Control IPX menu appears as shown in Figure 12.

Control IPX Menu

Figure 12 shows the Control IPX menu from which you access IPX Reset options.



```
Node:                Address:             Date:                Time:
Menu: Control IPX Menu                                         Path: (Main)
```

Figure 12. Control IPX Menu

Actions

These tables describe the control IPX actions that you can perform:

Action	Description
Reset IPX RIP Table	This operation clears all dynamic RIP table entries and forces a RIP general query to be sent on all networks. If a dialed link is down, it forces a call to be made. This permits a branch spoofing RIP broadcasts to synchronize itself with the Host.
Reset IPX SAP Table	This operation clears all dynamic SAP Table entries and forces a SAP general query to be sent on all networks. If a dialed link is down, it forces a call to be made. This permits a branch spoofing RIP broadcasts to synchronize itself with the Host.

Action	Description (continued)
Reset SPX Spoofing Table	This operation clears all SPX session entries registered for spoofing on the specified LAN Interface. ■ **Note** Resetting the entry discontinues the spoofing action for the applicable SPX session. However, the session can still be connected if communicating client/server pairs require it.

RIP/SAP Aging Control

Introduction

RIP/SAP allows a router to dynamically learn about all attached networks, Periodic RIP/SAP updates (typically at 60 second intervals) can cause a WAN link to come up and stay up unnecessarily (just to pass RIP/SAP traffic). Given the cost of unnecessary connection charges, this is not a desirable situation.

Vanguard products solve this problem on PPP/MLPPP links by using the RIP/SAP Aging Control feature. This lets you use RIP/SAP for a PPP/MLPPP WAN interface without incurring unnecessary connection charges.

Description

When RIP/SAP is enabled on a LAN or WAN interface, Vanguard tries to exchange routing information with all directly connected routers. Vanguard maintains the learned routing information in it's routing table. Each entry in this table is aged (an internal timer is incremented at configurable intervals). If the same routing information is received for a particular route the internal timer for that entry is reset to zero, and the route is considered as valid.

If, however, no routing information for that particular route is received within a specific period of time (3 times the RIP/SAP update period) the route is considered invalid; after 4 times the RIP/SAP update period the route is deleted from the routing table.

Features

RIP/SAP Aging Control has these features:

- RIP/SAP updates are sent out on PPP and MLPPP links only if the connection is already up.
- RIP/SAP Aging on entries learned from the directly connected link stops as soon as the link is brought down.
- Normal aging of routing table entries resumes when the connection is brought up again.
- RIP/SAP packets sent over a PPP link do not reset the Idle Disconnect timer so the connection is not kept up simply to pass RIP/SAP packets.
- The Idle Disconnect timer is reset on outgoing data only.
- There are no user configurable parameters for this feature. This feature applies to all PPP/MLPPP links, on all platforms, automatically.

Configuration Considerations

RIP/SAP Aging Control has these configuration rules:

- Set the PPP link's Idle disconnect time large enough to ensure that the connection to the remote node will stay up long enough for the node to send/receive RIP/SAP updates.
- It is recommended that the Idle disconnect time on the PPP/MLPPP link be set to a minimum of twice the configured RIP/SAP update time.
- Configure at least one static entry to the directly connected Vanguard nodes so that one can force a connection to a remote node. In this way, the remote node can, if necessary, learn the necessary routing information.

Learning Network Topology for the First Time

If a Vanguard (with PPP/MLPPP and ISDN), that is configured to call, is booted, the PPP/MLPPP will connect to its remote router.

If the connection is successful, the node can then learn about remote networks. If the ISDN link is faulty, or the remote node is not reachable (busy or down) at the time of the node boot, these calls are not established and the Network Routing topology and services are not learned. To have the Vanguard re-learn the network topology, after the network problem is resolved, try to access any statistically configured resource address of the remote node to bring up the connection.

Configuration Example

Introduction

This section describes the minimum configuration of a Vanguard LAN/WAN interconnection. The general steps are outlined in this table and are detailed in individual sections.

Step	Action
1	Configure the Node names and numbers of the nodes.
2	Configure the LAN connections and WAN links (such as X.25 or Frame Relay) between the two nodes.
3	Enable the LAN and at least one WAN interface in the Router Interface States record.
4	Enable overall IPX routing in the IPX Parameters record.
5	Configure an Interface record for the LAN interface and at least one WAN interface. Give the IPX network number assigned to the LAN or WAN link to which the interface attaches.

Step 1

Configure the Node names and numbers of the nodes as shown in this example:

	BN100	BN200
Node Record		
Node Name	BN100	BN200
Node Number	100	200
Node Address	200	200

Step 2

Configure the LAN connections and WAN links (such as X.25 or Frame Relay) between the two nodes. This example assumes a straight-through cable connecting BN100’s Port 1 to BN200’s Port 3. It defines the dialing mnemonic “BN200” on node BN100 to connect to the remote LCON facility.

	BN100	BN200
Port Record		
Port Number	1	3
Type	X.25	X.25
Clocking	External	External
Speed		56000
Routing Table		
Entry Number	1	1
Dial String	200*	20094
Destination	X25-3	LCON

(continued)	**BN100**	**BN200**
Mnemonic Table		
Entry Number	1	
Mnemonic	BN200	
Address	20094	
LAN Connection		
Entry Number	1	2
Type	ROUT	ROUT
Router Interface		
Interface Number	5	5
Autocall Mnemonic	BN200	
Connection ID	2	

Step 3

Enable the LAN and at least one WAN interface in the Interface Configuration Table record:

- Interface #1 State: Enabled
- Interface #5 State: Enabled

Step 4

Enable overall IPX routing in the Configure Parameters record.

Step 5

Configure an Interface record for the LAN interface and at least one WAN interface in the Interface Configuration Table. Give the IPX network number assigned to the LAN or WAN link to which the interface attaches.

- Entry [1]
  - Interface Number: 1
  - Network Number: 10
- Entry [2]
  - Interface Number: 5
  - Network Number: AA7

■**Note**

When you configure a Novell server, you assign it an IPX Network Number for each LAN to which it attaches. All Novell servers and IPX routers attached to the same LAN must be assigned the same Network Number. The Network Number assigned to a WAN link must be configured the same on both ends of the link.

Statistics

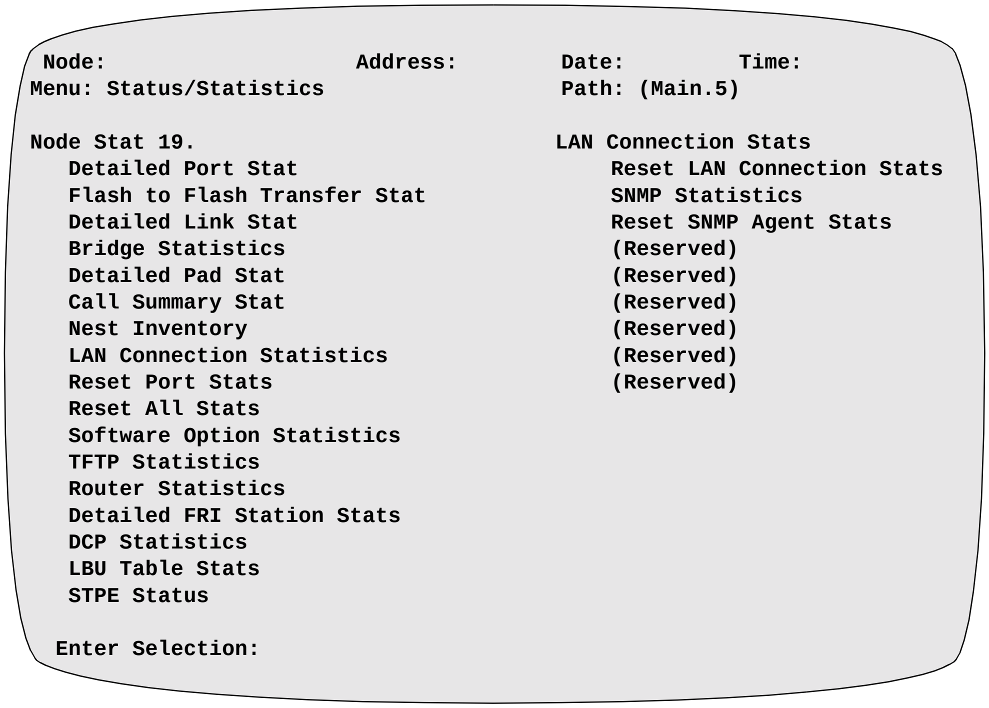
Introduction

The IPX Router Statistics section provides information about the status of IPX operations and includes statistics on IPX routing tables, access controls, filters, and event counters.

To access IPX Statistics, select Router Statistics from the Status/Statistics menu.

Status/Statistics Menu

Figure 13 shows the CTP Status/Statistics menu.

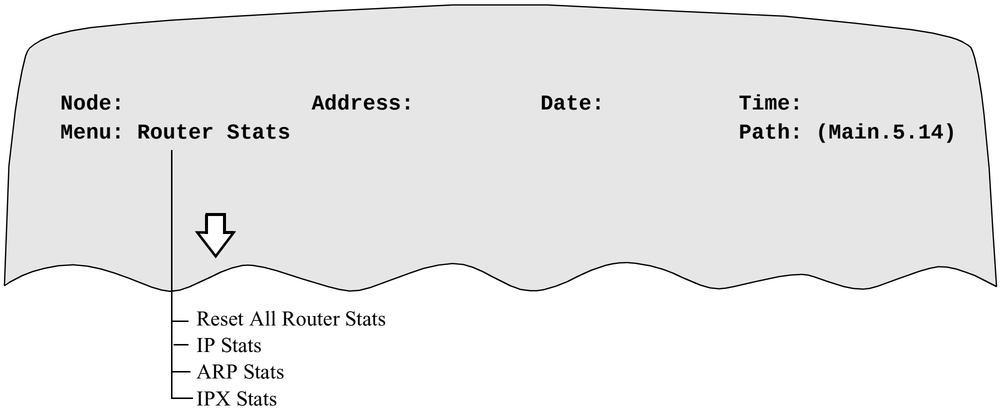


```
 Node:                    Address:        Date:         Time:
Menu: Status/Statistics                   Path: (Main.5)

Node Stat 19.                            LAN Connection Stats
   Detailed Port Stat                        Reset LAN Connection Stats
   Flash to Flash Transfer Stat              SNMP Statistics
   Detailed Link Stat                        Reset SNMP Agent Stats
   Bridge Statistics                         (Reserved)
   Detailed Pad Stat                         (Reserved)
   Call Summary Stat                         (Reserved)
   Nest Inventory                            (Reserved)
   LAN Connection Statistics                 (Reserved)
   Reset Port Stats                          (Reserved)
   Reset All Stats
   Software Option Statistics
   TFTP Statistics
   Router Statistics
   Detailed FRI Station Stats
   DCP Statistics
   LBU Table Stats
   STPE Status

  Enter Selection:
```

Figure 13. Status/Statistics Menu

Router Stats Screen

The Router Statistics menu appears as shown in Figure 14. Select **IPX Stats** to access information about the status of the IPX Protocol.

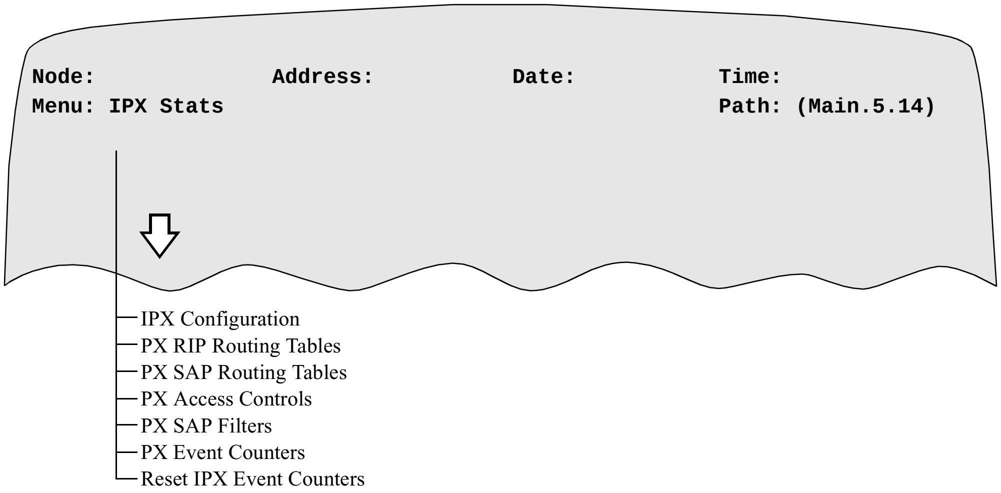


```
Node:               Address:          Date:          Time:
Menu: Router Stats                                   Path: (Main.5.14)
```

Figure 14. Router Stats Menu Screen

IPX Stats Menu

The IPX Statistics menu shown in Figure 15 allows you to access statistics for the various functions that make up the IPX protocol.

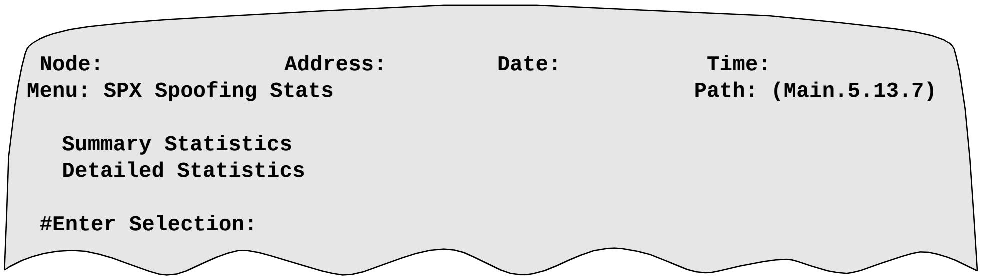


```
Node:                 Address:          Date:           Time:
Menu: IPX Stats                                         Path: (Main.5.14)
```

Figure 15. IPX Statistics Menu

SPX Spoofing Statistics Menu

The SPX Spoofing Statistics menu shown in Figure 16 allows you to access the statistics for spoofing on all Network Interfaces, as well as specific Network interface spoofing.

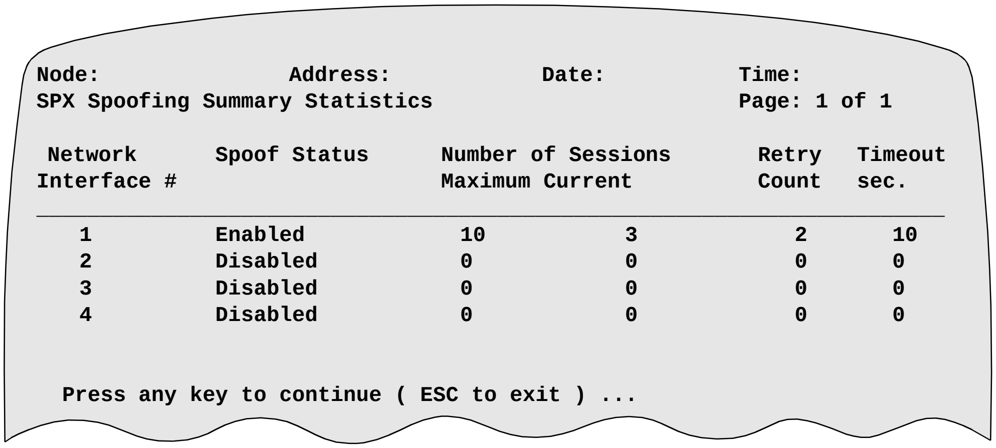


```
 Node:                Address:         Date:           Time:
Menu: SPX Spoofing Stats                              Path: (Main.5.13.7)

   Summary Statistics
   Detailed Statistics

 #Enter Selection:
```

Figure 16. SPX Spoofing Statistics Menu

Spoofing Summary Statistics Screen

The SPX Spoofing Summary Statistics screen shown in Figure 17 provides statistical information for all Network Interface spoofing.



```
Node:             Address:          Date:          Time:
SPX Spoofing Summary Statistics                    Page: 1 of 1

 Network      Spoof Status      Number of Sessions      Retry   Timeout
Interface #                     Maximum Current         Count   sec.
______________________________________________________________________
    1         Enabled            10           3           2      10
    2         Disabled           0            0           0      0
    3         Disabled           0            0           0      0
    4         Disabled           0            0           0      0


  Press any key to continue ( ESC to exit ) ...
```

Figure 17. Spoofing Summary Statistics Screen

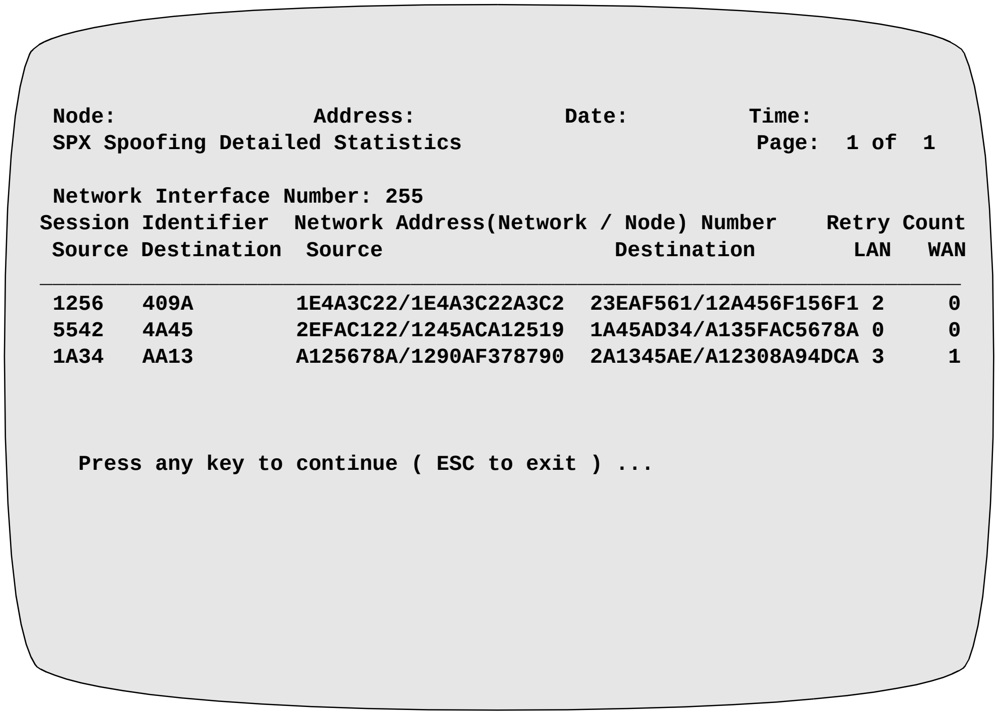
Screen Terms

This table describes the terms used in the SPX Summary Statistics screen.

Term	*Describes...*
Network Interface #	The Network Interface number to which the statistics apply.
Spoof Status	The Enabled/Disabled status of spoofing on the interface specified by the Network Interface Number.
Number of Sessions	The number of active sessions having SPX in action as well as the maximum number of possible sessions. The number of active sessions is a configurable value.
Retry Count	The number of retry attempts at SPX spoofing for the Network Interfaces listed. This is a configurable value.
Timeout sec.	The time in seconds after which the session is no longer active. This is a configurable value.

Spoofing Detailed Statistics Screen

The Detailed Statistics screen shown in Figure 18 provides statistical information on a specific Network Interface.



```
 Node:               Address:            Date:         Time:
 SPX Spoofing Detailed Statistics                       Page:  1 of  1

 Network Interface Number: 255
Session Identifier  Network Address(Network / Node) Number    Retry Count
 Source Destination  Source                 Destination        LAN   WAN
________________________________________________________________________
 1256   409A        1E4A3C22/1E4A3C22A3C2  23EAF561/12A456F156F1 2     0
 5542   4A45        2EFAC122/1245ACA12519  1A45AD34/A135FAC5678A 0     0
 1A34   AA13        A125678A/1290AF378790  2A1345AE/A12308A94DCA 3     1



   Press any key to continue ( ESC to exit ) ...
```

Figure 18. Spoofing Detailed Statistics

Screen Terms

This table describes the terms used in the Spoofing Detailed Statistics screen.

Term	Describes...
Network Interface Number	The Network Interface Number for the statistics displayed.
Session Identifier	The connection identification number generated for the packet's source and destination ends during establishment of the connection.
Network Address Number	The Network and Node number of the source and destination.
Retry Count	The number of times failure for getting SPX Keep Alive messages can be tolerated.

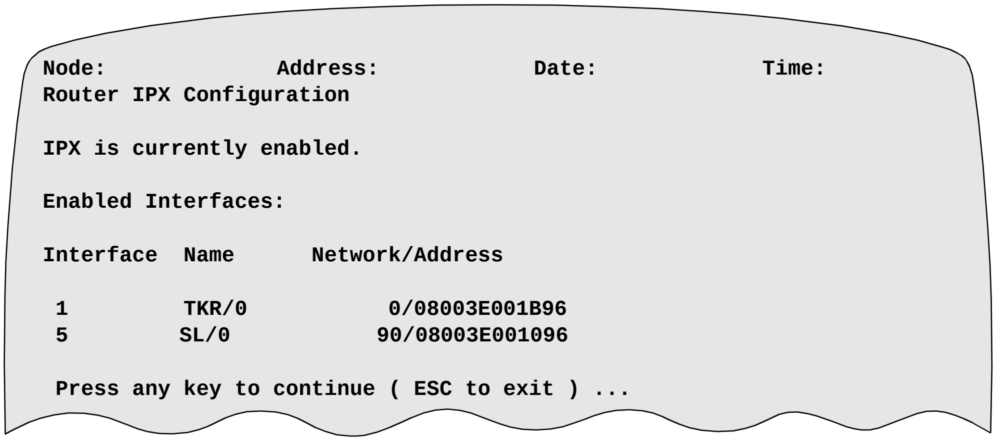
IPX Configuration Statistics

Introduction

This selection allows you to view the names and network addresses of all the interfaces that are currently enabled. A configured interface that does not appear in this table is either disabled in the Router Interface States menu or is misconfigured.

IPX Configuration Statistics Screen

Figure 19 shows a sample IPX Configuration Statistics screen. The terms used in the screens are described in the following table.



```
Node:             Address:            Date:            Time:
Router IPX Configuration

IPX is currently enabled.

Enabled Interfaces:

Interface  Name      Network/Address

 1         TKR/0           0/08003E001B96
 5         SL/0           90/08003E001096

 Press any key to continue ( ESC to exit ) ...
```

Figure 19. IPX Configuration Statistics Screen

Screen Terms

This table describes the terms used in the IPX Configuration Statistics screen shown in .

Term	*Describes...*
Interface	The interface number of an enabled and properly configured interface.
Name	The interface type such as "TKR" for token ring, "ETH" for Ethernet, or "SL" for serial line. The number after the slash is the instance number used in event messages to distinguish the particular port of the displayed type.
Network/ Address	The 4-byte IPX Network Number configured for the network attached to the interface, and the 6-byte IPX Node Number of the router on that network.

IPX RIP Routing Table Statistics

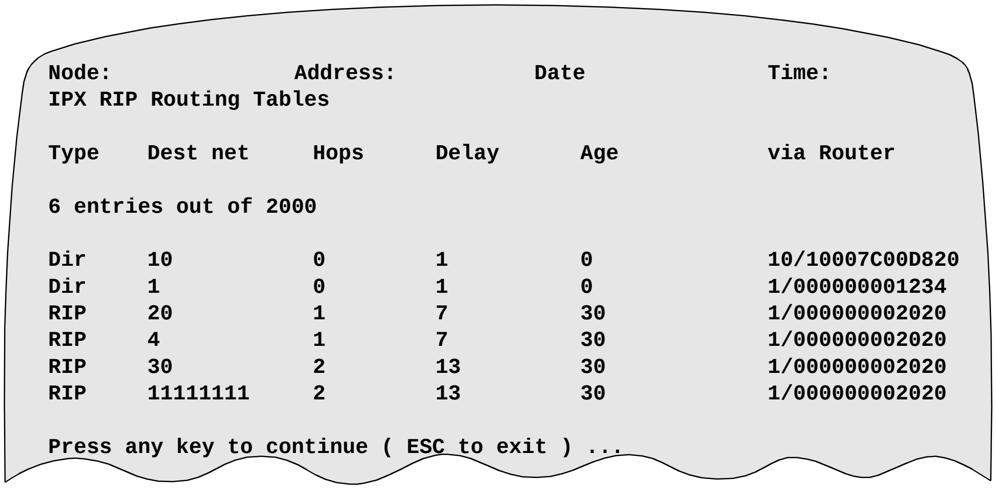
Introduction

The IPX RIP Routing Table displays the routes to all IPX Networks that have been learned by the router. Use this table to verify that the IPX network is operating properly. It should contain entries for all numbered physical LANs in the Internetwork and should contain the “internal network” numbers of 3.X and later Novell servers.

The IPX RIP table stores information on hop counts and tick count delays as received by other routers. When the router re-advertises routes, it adds one to the hop count and the Advertised Delay of the outgoing interface when it builds a RIP packet for transmission.

IPX Routing Table Statistics Screen

Figure 20 shows the IPX RIP Routing Table Statistics screen. The terms used in the screen are described in the following table.



```
Node:               Address:          Date              Time:
IPX RIP Routing Tables

Type    Dest net     Hops      Delay      Age           via Router

6 entries out of 2000

Dir     10           0         1          0             10/10007C00D820
Dir     1            0         1          0             1/000000001234
RIP     20           1         7          30            1/000000002020
RIP     4            1         7          30            1/000000002020
RIP     30           2         13         30            1/000000002020
RIP     11111111     2         13         30            1/000000002020

Press any key to continue ( ESC to exit ) ...
```

Figure 20. IPX RIP Routing Table Statistics Screen

Screen Terms

This table describes the terms used in the IPX RIP Routing Table Statistics screen shown in Figure 20 on page 58.

Term	Describes...
Type	The type of route. • Dir - indicates directly attached interface. • RIP - indicates network routes learned using IPX RIP. • Old - indicates a route that has missed two RIP update intervals and is thereby permitted to be replaced by a different next hop. • Del - indicates a deleted route that is advertised as dead (hop count 16).
Dest net	The IPX Network Number of a known route. Packets destined for networks unknown by the router are dropped.

Term	Describes... (continued)
Hops	The number of hops to the destination network as received in a RIP packet. For directly attached networks, the hop count is considered to be zero.
Delay	The number of "ticks" to the destination network as received in a RIP packet. For directly attached networks, this is the Advertised Delay configured for an interface.
Age	The number of seconds since a RIP advertisement for the route was received. If this exceeds three times the RIP update interval configured for an interface, the route is considered "down," and is advertised as such. When this exceeds four times the RIP Update Interval, the route is removed, or "garbage collected" from the table. For directly connected networks, the age is always zero.
via Router	The IPX Network Number and Node Number of the next hop to which to forward frames for the destination network using learned RIP routes. The next hop will always be on a directly attached network. For directly attached networks themselves, this column provides the configured IPX Network Number and the IPX Node Number used by the router itself.

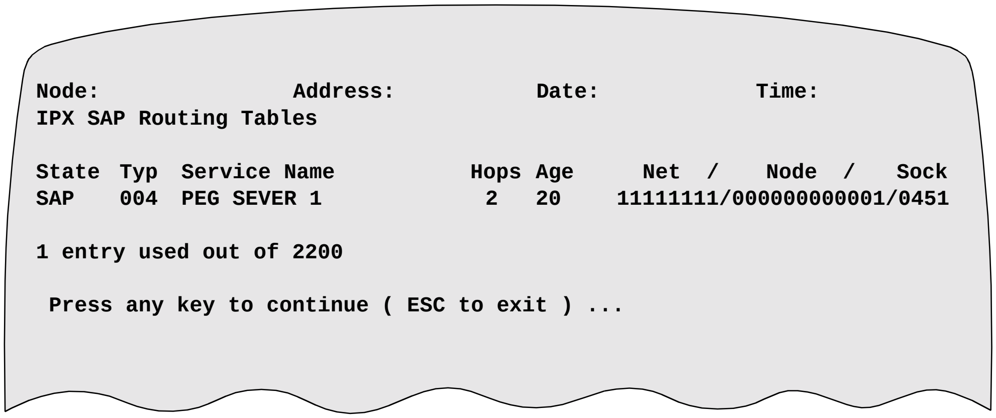
IPX SAP Routing Table Statistics

Introduction

The IPX SAP Routing Table displays all servers learned using SAP. Check this table to verify that all servers in an Internetwork are “visible” to the router. This table corresponds to the list command that would be run on a workstation.

IPX SAP Routing Statistics Screen

Figure 21 shows the IPX SAP Routing Table Statistics screen. The terms used in the screens are described in the following table.



```
Node:                Address:           Date:            Time:
IPX SAP Routing Tables

State  Typ  Service Name           Hops Age     Net  /    Node  /   Sock
SAP    004  PEG SEVER 1             2   20    11111111/000000000001/0451

1 entry used out of 2200

 Press any key to continue ( ESC to exit ) ...
```

Figure 21. IPX SAP Routing Table Statistics Screen

Screen Terms

This table describes the terms used in the IPX SAP Routing Table Statistics screen shown in Figure 21.

Term	Describes...
State	The status of SAP updates. • SAP indicates a normally learned service that has been properly updated. • Old indicates a service that has not been updated in two SAP update intervals, and is thus eligible for replacement. • Del indicates a service that has missed three SAP update intervals and is marked (and re-advertised as dead). After four update intervals with no update, a SAP service is removed from the table.
Type	The 16-bit Novell “server type” for the learned service. The most common type code is 0004 for a file server.
Service Name	The service name advertised in SAP for the service.
Hops	The number of router hops away from the service, as received in the SAP packet which advertised the service.
Age	The number of seconds since the last SAP update of the service.

Term	***Describes...*** *(continued)*
Net/Node/ Sock	The IPX Network Number, Node Number, and Socket Number advertised for the service. A service which is advertised on a network that is not reachable by the Routing Table will be rejected. All numbers are in hexadecimal.

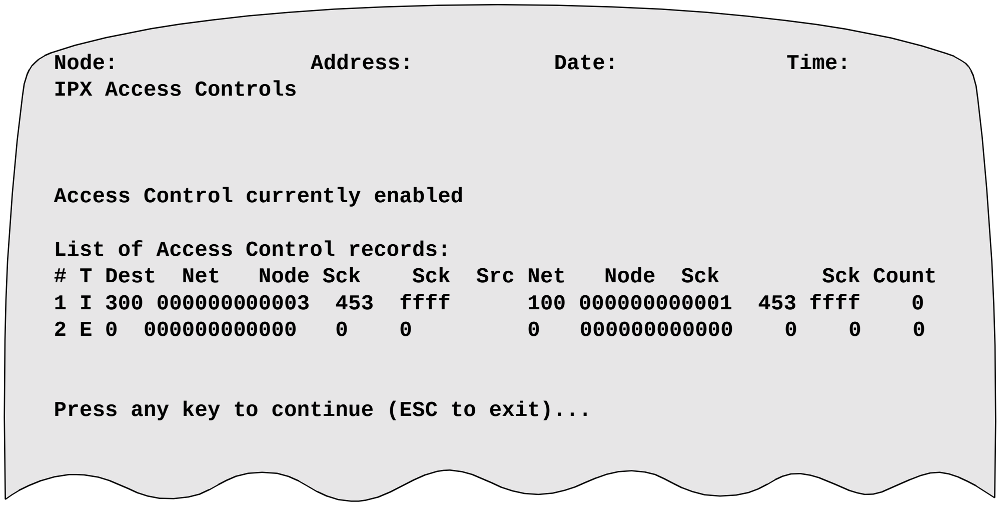
IPX Access Controls Statistics

Introduction

Each line in the IPX Access Controls Statistics screen corresponds to an entry in the IPX Access Controls Table.

IPX Access Controls Statistics Screen

Figure 22 shows the IPX Access Controls Statistics screen. The terms used in the screens are described in the following table.



```
Node:               Address:           Date:             Time:
IPX Access Controls



Access Control currently enabled

List of Access Control records:
# T Dest  Net   Node Sck    Sck  Src Net   Node  Sck        Sck Count
1 I 300 000000000003  453  ffff      100 000000000001  453 ffff    0
2 E 0  000000000000   0    0         0   000000000000    0    0    0


Press any key to continue (ESC to exit)...
```

Figure 22. IPX Access Controls Statistics Screen

Screen Terms

This table describes the terms used in the IPX Access Controls Statistics screen shown in Figure 22.

Term	*Describes...*
#	The entry number of access control record.
T	The type of the record: “I” for inclusive and “E” for exclusive. Type “I” records, if matching a packet, cause it to be included and thus forwarded. Type “E” records, if matching a packet, cause it to be excluded and thus filtered. The first matching record governs the action taken, and if no record matches, the packet is excluded.
Dest Net	If nonzero, selects an IPX destination network number that a packet must match.
Dest Node	If nonzero, selects an IPX destination node number that a packet must match.
Sck	The starting and ending destination IPX socket numbers (inclusive) that a packet must match. 0 to FFFF matches all packets.
Src Net	If nonzero, selects an IPX source network number that a packet must match.

Term	***Describes...*** *(continued)*
Src Node	If nonzero, selects an IPX source node number that a packet must match.
Sck	The starting and ending source IPX socket numbers (inclusive) that a packet must match. 0 to FFFF matches all packets.
Count	The number of received packets discarded due to access controls. Access controls apply only to received packets; they cannot be used to filter internally generated transmissions of the router (such as RIP or SAP transmissions).

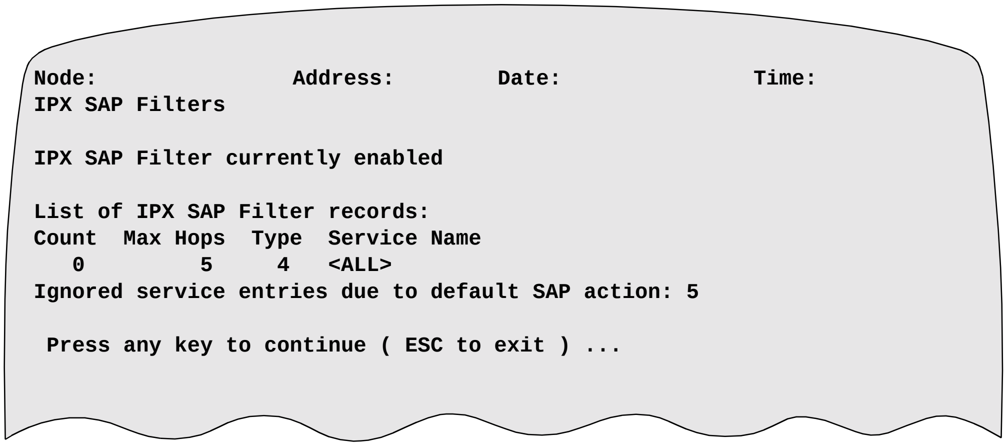
IPX SAP Filter Statistics

Introduction

The IPX SAP Filter Statistics screen displays the configured IPX SAP filters.

IPX SAP Filter Statistics Screen

Figure 23 shows the IPX SAP Filter Statistics screen. The terms used in the screens are described in the following table.



```
Node:                Address:        Date:               Time:
IPX SAP Filters

IPX SAP Filter currently enabled

List of IPX SAP Filter records:
Count  Max Hops  Type  Service Name
   0         5     4   <ALL>
Ignored service entries due to default SAP action: 5

 Press any key to continue ( ESC to exit ) ...
```

Figure 23. IPX SAP Filter Statistics Screen

Screen Terms

This table describes the terms used in the IPX SAP Filter Statistics screen shown in Figure 23.

Term	Describes...
IPX SAP Filter Currently...	The Enabled/Disabled state of SAP Filtering. This field shows: • Enabled when the SAP filtering action is enabled, even though the IPX SAP filter list may be empty. • Disabled when the SAP action is disabled.
Count	The number of SAP packets ignored due to restrictions of a SAP filter record.
Max Hops	The configured maximum number of hops away a service can be in order to be accepted in the SAP table.
Type	The 16-bit Novell type code for the SAP service.
Service Name	The character string name (48 characters maximum) for the server.
Ignored service entries...	A count of how many services were blocked due to the SAP Default Action parameter being configured as BLOCK, since the node was last reset or powered up. This count may include services being broadcast repeatedly.

IPX Event Counters Statistics

Introduction

Vanguard products collect statistics as a count of certain events. These events are organized in terms of the routing protocol under which they occur. The IPX Event Counters Statistics screen shows the events for the IPX protocol.

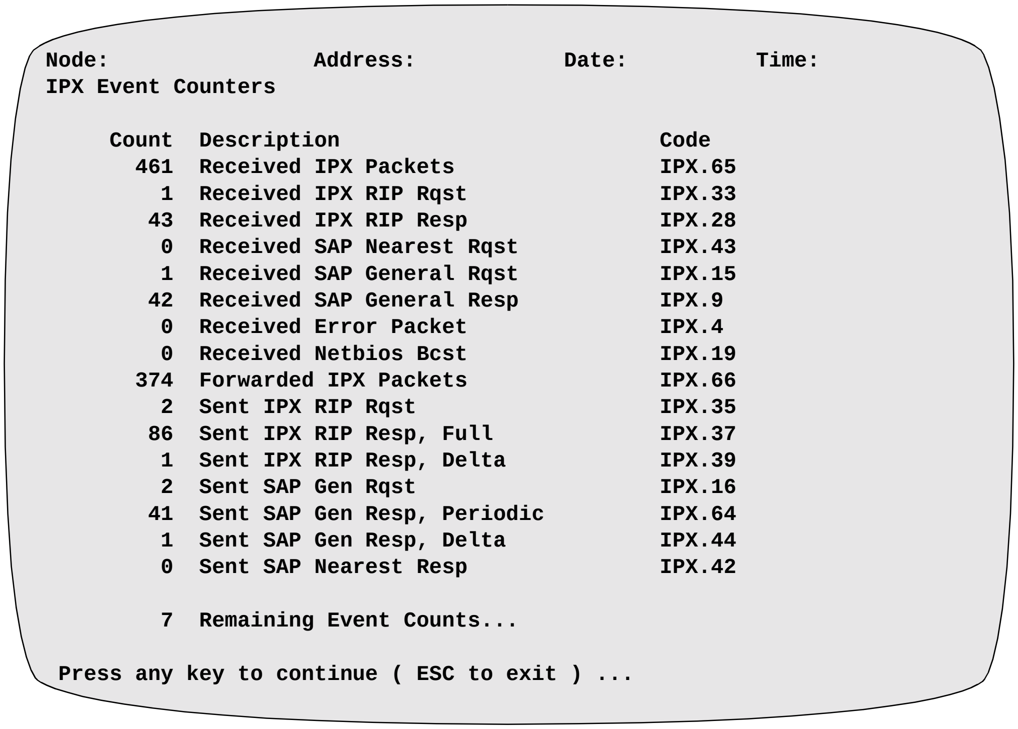
IPX Event Counters Statistics

The IPX Event Counters Statistics are shown in two parts:

- A first screen that shows common packet processing counts
- A second (and perhaps third) screen that shows unusual and error event counts

IPX Event Counters Statistics Screen

Figure 24 shows an example of the first screen. The terms used in the screens are described in the following table.



```
Node:                Address:           Date:          Time:
IPX Event Counters

     Count  Description                          Code
       461  Received IPX Packets                 IPX.65
         1  Received IPX RIP Rqst                IPX.33
        43  Received IPX RIP Resp                IPX.28
         0  Received SAP Nearest Rqst            IPX.43
         1  Received SAP General Rqst            IPX.15
        42  Received SAP General Resp            IPX.9
         0  Received Error Packet                IPX.4
         0  Received Netbios Bcst                IPX.19
       374  Forwarded IPX Packets                IPX.66
         2  Sent IPX RIP Rqst                    IPX.35
        86  Sent IPX RIP Resp, Full              IPX.37
         1  Sent IPX RIP Resp, Delta             IPX.39
         2  Sent SAP Gen Rqst                    IPX.16
        41  Sent SAP Gen Resp, Periodic          IPX.64
         1  Sent SAP Gen Resp, Delta             IPX.44
         0  Sent SAP Nearest Resp                IPX.42

         7  Remaining Event Counts...

 Press any key to continue ( ESC to exit ) ...
```

Figure 24. IPX Event Counters Statistics Screen

Screen Terms

This table describe the terms used in the IPX Event Counters Statistics screen shown in Figure 24 on page 65.

Term	Describes...
Count	A count of the number of events that have occurred.
Description	A brief description of the event. The upper half of the first screen shows all received packets; the lower half counts all transmitted packets.
Code	A short code that identifies the protocol and event number for that protocol. Router error events that are logged on the CTP screen or the Alarm Log are identified by these event codes.
Remaining Event Counts	The total number of error and unusual events that are displayed on the second and later screens.

Reset IPX Event Counters

Description

In a properly configured system, any IPX packet that is received that is not RIP or SAP should be forwarded. This can be verified in the Event Counters screen. Any packets that are discarded cause event counts to be displayed on the second and later screens. On the first screen, the same counts always appear. On the second and later screens, only non-zero event counts are displayed.

A common use of the Event Counts screen is to press Control-R repeatedly during router operation. This repeatedly updates the first screen of packet event counts. If the Received and Forwarded IPX counts increase, the router is operating properly. The Remaining Event Counts line can be used to verify that errors are not increasing.

You can reset the Events Counters screen. Resetting this screen sets all IPX event counts back to zero. It is frequently used to clear the counts before conducting a test operation such as a Novell login attempt. The screen requires that you press ENTER to confirm that event counts are to be cleared.

Select Number 7 to reset the IPX Event Counter.

Spoofing of SPX Keep Alive Frames

Introduction

Sequenced Packet Exchange (SPX) Keep Alive Spoofing ensures that there are no unnecessary SPX polls transmitted across the wide area in an IPX environment using Netware for SAA or Netbios emulation. This feature is especially useful in a switched environment. Dialup charges continue to occur if polls are being transmitted just to check whether the link is available and ready to receive data.

SPX Background

SPX adds the Transport Layer function to the IPX packet within the Novell architecture. It provides a connection-oriented guaranteed delivery system between two workstations.

How Keep Alive Frames Work

This table describes SPX Keep Alive frames.

<table>
<tr><th>Step</th><th colspan="2">Stage</th></tr>
<tr><td>1</td><td colspan="2">Any application using the SPX protocol opens a connection between the two endpoints.</td></tr>
<tr><td rowspan="4">2</td><td colspan="2">After a connection has been established, both sides periodically generate SPX packets of the type 0x80 (System Control packet) every seven seconds.</td></tr>
<tr><th>If...</th><th>Then...</th></tr>
<tr><td>An endpoint does not receive a System Control packet</td><td>The endpoint generates an SPX packet of the type 0xC0.
This packet is retransmitted three times and the connection is terminated.</td></tr>
<tr><td>The remote end responds with a System Control packet before the retry count is exceeded</td><td>The connection is not terminated and the two ends return to periodically generating SPX System Control packets.</td></tr>
</table>

Why Spoofing Is Necessary

The periodic generation of the SPX System Control packets causes an on demand Switched Virtual Circuit (SVC) to stay up indefinitely. To overcome this problem, the response to SPX packets, which are generated as Keep Alive messages, can be spoofed by the router itself so that these messages do not cause the on demand link to come up.

This feature ensures that the routers spoof responses to SPX Keep Alive packets when the Dial on Demand link goes down. These SPX Keep Alive packets do not keep the Dial on Demand link up.

Before Spoofing Example

Figure 25 shows the network before spoofing.

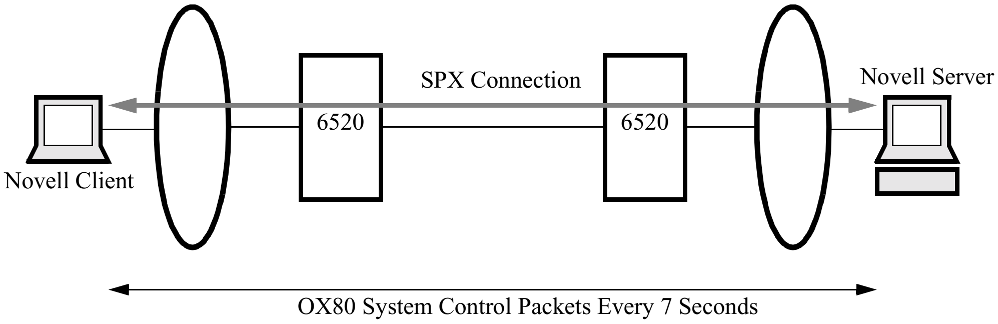


Figure 25. Network With No Spoofing

After Spoofing Example

Figure 26 shows the network after the spoofing connection. Although the figure shows a Token Ring network, spoofing is supported on Ethernet as well.

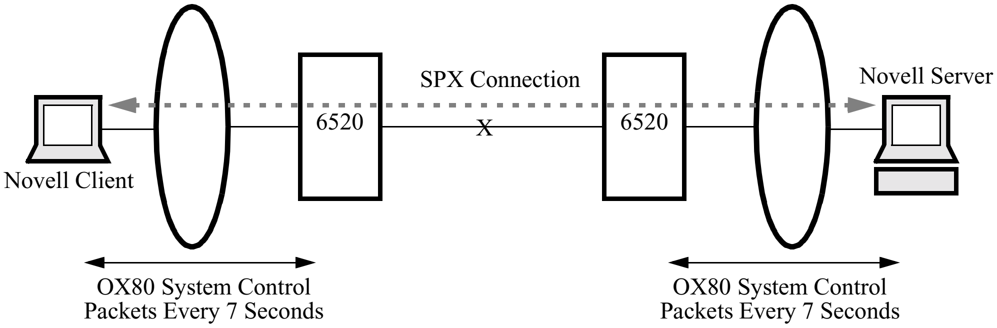

SPX Connection
Novell Server
6520
X
6520
Novell Client
OX80 System Control Packets Every 7 Seconds
OX80 System Control Packets Every 7 Seconds

Figure 26. Network With Spoofing

Lite Keep Alive Spoofing

Lite Keep Alive spoofing determines when two communicating nodes begin exchanging keep alive packets, and starts spoofing them. The Lite spoofing version does not track the session's activity status. It does quick processing and occupies minimum memory. Lite spoofing has the disadvantage of not reflecting the state of a node if it is inactive on one end of a communicating pair.

For example, if the client side of an SPX session is out of service, the server node should be reset, however, it is not reset due to the spoofing. If the server node is not reset, it will be unable to make a new connection with the client.

Enhanced Keep Alive Spoofing

Enhanced Keep Alive Spoofing overcomes the shortcoming described above. This option requires memory configuration to store SPX session state information such that inactivity at the remote end of a communicating pair is detected, and spoofing of the inactive node stops. A reset can be performed allowing a new connection to be made. SPX connections can be reset earlier, which prevents unnecessary retries, thereby saving response time and data transfer cost.

SPX Spoofing Features

SPX Spoofing has these functional features. The features, unless otherwise stated are applicable on a per LAN interface basis.

- Configurable enable or disable of SPX spoofing.
- Continually maintained listing of currently active SPX sessions. The number of such entries that can be maintained is configurable. This provides for user control of memory optimization. At any time, you can decrease the maintained number of SPX entries, for interfaces expected to have fewer active sessions.
- Configurable timeout trigger interval whereby Keep Alive packets are sent to local communicating entities that have SPX sessions established. The sessions are recorded by the spoofing functionality. Receiving a response to a Keep Alive message within the time limit determines if the machine remains functional.
- Configurable number of retries following the timeout trigger.
- User reset of SPX session entries maintained for spoofing. You can also reset all entries for an interface experiencing a network failure.

Limitation

When using Lite SPX, the server has no way of knowing if the client shuts down (powers off) without performing a normal SPX session shutdown. The router on the server end is still spoofing responses for the client. When a client tries to log in again, there is a lockout.

Enabling SPX Spoofing

Introduction

Perform these tasks to enable SPX spoofing:

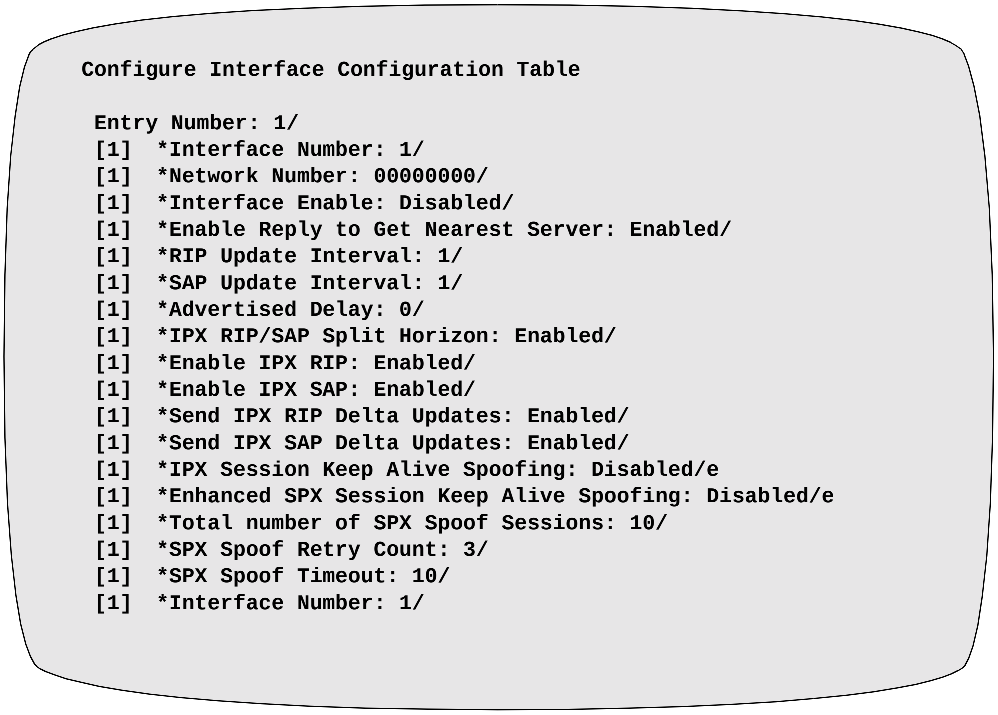
- Set the SPX Spoofing parameters available from the IPX Interface Configuration Table. These include:
  - IPX Session Keep Alive Spoofing
  - Enhanced SPX Session Keep Alive Spoofing
  - Total Number of SPX Spoof Sessions
  - SPX Spoof Retry Count
  - SPX Spoof Timeout
- Set the SPX Spoofing Version parameter, available from the Configure IPX Parameters Record.
- Specify the Idle Timeout for the Dial on Demand link, available from the Configure LAN Connections Table

IPX Interface Configuration Table

Figure 27 shows the IPX Interface Configuration Table in which you can find most of the Keep Alive Spoofing parameters.

■Note

RIP, SAP, and Serialization spoofing, also configurable from this menu, are discussed beginning on page 75.



```
Configure Interface Configuration Table

 Entry Number: 1/
 [1]  *Interface Number: 1/
 [1]  *Network Number: 00000000/
 [1]  *Interface Enable: Disabled/
 [1]  *Enable Reply to Get Nearest Server: Enabled/
 [1]  *RIP Update Interval: 1/
 [1]  *SAP Update Interval: 1/
 [1]  *Advertised Delay: 0/
 [1]  *IPX RIP/SAP Split Horizon: Enabled/
 [1]  *Enable IPX RIP: Enabled/
 [1]  *Enable IPX SAP: Enabled/
 [1]  *Send IPX RIP Delta Updates: Enabled/
 [1]  *Send IPX SAP Delta Updates: Enabled/
 [1]  *IPX Session Keep Alive Spoofing: Disabled/e
 [1]  *Enhanced SPX Session Keep Alive Spoofing: Disabled/e
 [1]  *Total number of SPX Spoof Sessions: 10/
 [1]  *SPX Spoof Retry Count: 3/
 [1]  *SPX Spoof Timeout: 10/
 [1]  *Interface Number: 1/
```

Figure 27. IPX Interface Configuration Table

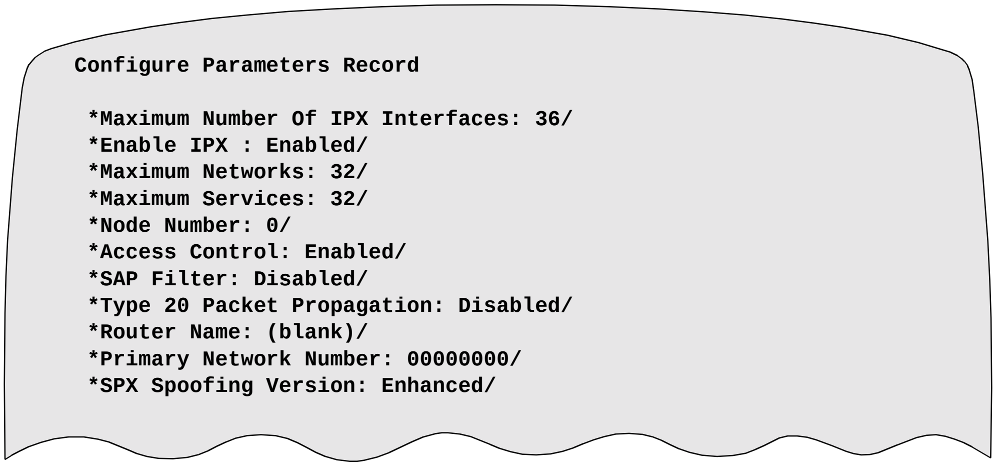
Setting the Parameters

You must configure these parameters to enable SPX Keep Alive Spoofing. Detailed descriptions of these parameters appear beginning on page 68.

- IPX Session Keep Alive Spoofing - Controls whether the router spoofs responses to keep alive packets (received from servers on this interface) that are destined for dial-up router connections not currently active. When you enable this parameter, remote dial-up workstations can keep their server login sessions active even though the connection has hung up.
- Enhanced SPX Keep Alive Spoofing parameter - Spoofs SPX Keep Alive packets for all registered SPX connections on the network interface, while tracking the activity state of the communicating pair in order to halt spoofing of a non-operational node.
- Total Number of SPX Spoofing Sessions - Represents the number of SPX sessions for which spoofing is supported.
- SPX Spoof Retry Count - Specifies a communicating entity as being active if Keep Alive packets are received periodically and within the time interval specified here.
- SPX Spoof Timeout - Specifies the number of timeouts allowed before a communicating entity is described as non-operational.

IPX Parameters Record Spoofing Parameters

Figure 28 shows the IPX Parameters Record in which you set the SPX Spoofing Version parameter.



```
Configure Parameters Record

 *Maximum Number Of IPX Interfaces: 36/
 *Enable IPX : Enabled/
 *Maximum Networks: 32/
 *Maximum Services: 32/
 *Node Number: 0/
 *Access Control: Enabled/
 *SAP Filter: Disabled/
 *Type 20 Packet Propagation: Disabled/
 *Router Name: (blank)/
 *Primary Network Number: 00000000/
 *SPX Spoofing Version: Enhanced/
```

Figure 28. Configure IPX Parameters Record

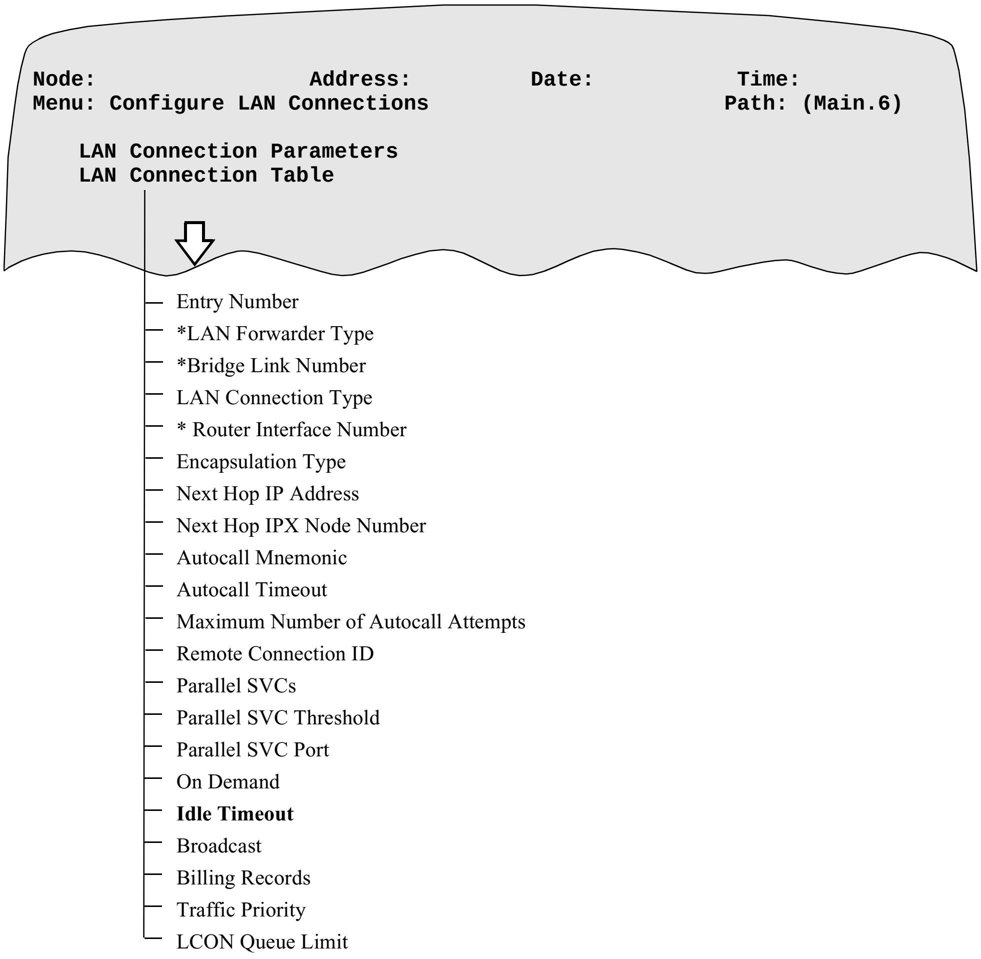
Setting the SPX Spoofing Version Parameter

The SPX Spoofing Version parameter controls whether Lite or Enhanced SPX spoofing occurs. You must configure this parameter to enable SPX Keep Alive Spoofing. Detailed descriptions of SPX parameters appear beginning on page 68.

- Lite SPX spoofing - Does not store session state information, performing quick processing and occupying minimal memory. It does not reflect the state of a machine that is inactive on a remote node and does not reset an SPX session of a non-operational node.
- Enhanced SPX spoofing - Does store session state information, and discontinues spoofing of an inactive node. This allows earlier reset and faster reconnection than possible with Lite spoofing.

Idle Timeout Parameter

You also need to specify the idle timeout for the Dial on Demand link. Figure 29 shows the Configure LAN Connections menu and the LAN Connection Table in which you can find the Idle Timeout parameter.



```
Node:                    Address:        Date:          Time:
Menu: Configure LAN Connections                        Path: (Main.6)

     LAN Connection Parameters
     LAN Connection Table
```

Figure 29. Configure LAN Connections Menu

Setting the Idle Timeout Parameter

This parameter specifies the amount of time in seconds the circuit remains connected without passing any data before being brought down. Setting this parameter to zero (0) keeps the circuit up indefinitely.

Set the value for the Idle Timeout parameter greater than 60 to 90 seconds so that some Keep Alive packets are exchanged.

RIP, SAP, and Serialization Spoofing

Introduction

This section describes RIP, SAP, and Serialization spoofing, configurable from the IPX Interface Configuration Table shown in Figure 27 on page 71.

Spoofing RIP and SAP Updates

Spoofing RIP/SAP means continuing to send RIP and SAP updates on the LAN at one-minute intervals, but not sending such updates on the WAN at one-minute intervals.

Per Interface

You can perform static configuration of RIP and SAP tables on a per interface basis. Most of the time, remote branch access to a few services, and routes to those services, should suffice. In this case, the SAP table can be configured for the service availability and RIP can be configured for the route information. No advertisements will go out on this interface.

The ability to spoof responses to a Server's Keep Alive messages is configurable on a per-interface basis, using the Server-side interface. In practice, this just means Interface 1 (the LAN Interface). You should configure spoofing for the LAN interfaces only.

With Dialed Connections

With dialed connections, response to these queries are "spoofed" when the dialed link is disabled. This prevents you from having to log in every time the dial link is established.

What Is Serialization Spoofing?

Serialization spoofing is a copy licensing protection feature that operates regardless of the Keep Alive Spoofing parameter value. Netware 4.X servers periodically transmit a "serialization" packet to every Server they have learned about. This packet is transmitted directly to the other Server's internal IPX network address approximately every 66 seconds.

The Serialization Spoofing feature discards all packets addressed to a dialed network upon call termination. It forwards these packets if the call is connected for other reasons. A new IPX event count is incremented for every serialization packet discarded. (If the packet is forwarded, it is counted in the normal IPX Forwarded Packet count.)

The sole criterion for a serialization packet is the IPX packet destination. There is no separate "enable" parameter for the serialization spoofing feature.

Index