CHAPTER 21

Novell IPX Commands

Novell Internet Packet Exchange (IPX) is derived from the Xerox Network Systems (XNS) Internet Datagram Protocol (IDP). One major difference between IPX and XNS is that they do not always use the same Ethernet encapsulation format. A second difference is that IPX uses Novell's proprietary Service Advertisement Protocol (SAP) to advertise special network services.

Our implementation of Novell's IPX protocol has been certified as providing full IPX router functionality.

Note One or more of the commands that previously appeared this chapter have been replaced by new commands. See the *Router Products Command Reference* publication for command information. The old commands continue to perform their normal function in the current release, but support for them will cease in future releases.

Use the commands in this chapter to configure and monitor Novell IPX networks. For IPX configuration information and examples, refer to the "Configuring Novell IPX" chapter in the *Router Products Configuration Guide*.

Note For all commands that previously had the keyword **novell**, this keyword has been changed to **ipx**. However, you can still use the keyword **novell** in all commands.

access-list (extended)

To define an extended Novell IPX access list, use the extended version of the **access-list** global configuration command. To remove an extended access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*]

no access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*]

Syntax Description

access-list-number — Number of the access list. This is a decimal number from 900 to 999.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

protocol — Number of an IPX protocol type, in decimal. This also is sometimes referred to as the packet type. Table 21-1 in the "Usage Guidelines" section lists some IPX protocol numbers.

source-network — (Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeroes in the network number; for example, for the network number 000000AA, you can enter AA.

source-node — (Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-network-mask — (Optional) Mask to be applied to *source-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.

The mask must immediately be followed by a period, which must in turn immediately be followed by *source-node-mask*.

source-node-mask — (Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

source-socket

Socket number from which the packet is being sent, in hexadecimal. Table 21-2 in the “Usage Guidelines” section lists some IPX socket numbers.

destination-network

(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.

destination-node

(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-network-mask

(Optional) Mask to be applied to *destination-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.

The mask must immediately be followed by a period, which must in turn immediately be followed by *destination-node-mask*.

destination-node-mask

(Optional) Mask to be applied to *destination-node*. This is a

48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-socket

(Optional) Socket number to which the packet is being sent, in hexadecimal. Table 21-2 in the “Usage Guidelines” section lists some IPX socket numbers.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

Extended IPX access lists filter on protocol type. All other parameters are optional.

If a network mask is used, all other fields are required.

Use the **ipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface. The access list filters all outgoing packets on the interface.

Note For some versions of NetWare, the protocol type field is not a reliable indicator of the type of packet encapsulated by the IPX header. In these cases, use the source and destination socket fields to make this determination. For additional information, contact Novell.

Table 21-1 lists some IPX protocol numbers. Table 21-2 lists some IPX socket numbers. For additional information about IPX protocol numbers and socket numbers, contact Novell.

Table 21-1 Some IPX Protocol Numbers

IPX Protocol Number (Decimal)	Protocol (Packet Type)
–1	Wildcard; matches any packet type in 900 lists.
0	Could be any protocol; refer to the socket number to determine the packet type
1	Routing Information Protocol (RIP)
4	Service Advertisement Protocol (SAP)
5	Sequenced Packet Exchange (SPX)
17	NetWare Core Protocol (NCP)
20	IPX NetBIOS

Table 21-2 Some IPX Socket Numbers

IPX Socket Number (Hexadecimal)	Socket
0	All sockets, wild card used to match all sockets
451	NetWare Core Protocol (NCP) process
452	Service Advertisement Protocol (SAP) process
453	Routing Information Protocol (RIP) process
455	Novell NetBIOS process
456	Novell diagnostic packet
457	Novell serialization socket
4000-7FFF	Dynamic sockets; used by workstations for interaction with file servers and other network servers
8000-FFFF	Sockets as assigned by Novell, Inc.

To delete an extended access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific protocol, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *protocol*

Examples

The following example denies access to all RIP packets (protocol number 1) from socket 453 (RIP process socket) on source network 1 that are destined for socket 453 on network 2. It permits all other traffic.

```
access-list 900 deny 1 453 2 453
access-list 900 permit -1 –1 0 –1 0
```

The following example permits type 2 packets from any socket on network 10 to access any sockets on any nodes on networks 1000 through 100F. It denies all other traffic (with an implicit deny all):

Note This type is chosen only as an example. The actual type to use depends on the specific application.

```
access-list 910 permit 2 10.0000.0C00.0000 0000.0000.FFFF 0
  1000.0000.0000.0000 F.FFFF.FFFF.FFFF 0
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (standard)
ipx access-group
ipx input-network-filter
ipx output-network-filter
ipx router-filter
priority-list protocol †

access-list (SAP filtering)

To define an access list for filtering Service Advertisement Protocol (SAP) requests, use the SAP filtering form of the **access-list** global configuration command. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask*.*node-mask*]
[*service-type* [*server-name*]]
no access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask*.*node-mask*]
[*service-type* [*server-name*]]

Syntax Description

access-list-number	Number of the SAP access list. This is a decimal number from 1000 to 1099.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.
node	(Optional) Node on *network*. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.*node-mask*	(Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. Table 21-3 in the “Usage Guidelines” section lists examples of service types.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the **access-list** command. Do not use the *network.node* address of the particular interface board.

Table 21-3 lists some sample IPX SAP types. For more information about SAP types, contact Novell.

Table 21-3 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
1	User
2	User group
3	Print server queue
4	File server
5	Job server
7	Print server
9	Archive server
A	Queue for job servers
21	NAS SNA gateway
2D	Time Synchronization VAP
2E	Dynamic SAP
47	Advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES—NetWare for VMS
98	NetWare access server
9A	Named Pipes server
9E	Portable NetWare—UNIX
102	RCONSOLE
111	Test server
166	NetWare management (Novell's Network Management Station [NMS])
26A	NetWare management (NMS console)

To delete a SAP access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *network*

Example

The following access list blocks all access to a file server (service type 4) on the directly attached network by resources on other Novell networks, but allows access to all other available services on the interface:

```
access-list 1001 deny -1 4
access-list 1001 permit -1
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ipx input-sap-filter
ipx output-gns-filter
ipx output-sap-filter
ipx router-sap-filter
priority-list protocol †

access-list (standard)

To define a standard IPX access list, use the standard version of the **access-list** global configuration command. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source-network*[**.***source-node* [*source-node-mask*]] [*destination-network*[**.***destination-node* [*destination-node-mask*]]]

no access-list *access-list-number* {**deny** | **permit**} *source-network*[**.***source-node* [*source-node-mask*]] *[destination-network*[**.***destination-node* [*destination-node-mask*]]]

Syntax Description

access-list-number

Number of the access list. This is a decimal number from 800 to 899.

deny

Denies access if the conditions are matched.

permit

Permits access if the conditions are matched.

source-network

Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.

source-node

(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-node-mask

(Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-network

(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.

destination-node

(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-node-mask

(Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

Standard IPX access lists filter on the source network. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface. The access list filters all outgoing packets on the interface.

To delete a standard access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *source-network*

Examples

The following example denies access to traffic from all IPX networks (–1) to destination network 2:

```
access-list 800 deny -1 2
```

The following example denies access to all traffic from IPX address 1.0000.0c00.1111:

```
access-list 800 deny 1.0000.0c00.1111
```

The following example denies access from all nodes on network 1 that have a source address beginning with 0000.0c:

```
access-list 800 deny 1.0000.0c00.0000 0000.00ff.ffff
```

The following example denies access from source address 1111.1111.1111 on network 1 to destination address 2222.2222.2222 on network 2:

```
access-list 800 deny 1.1111.1111.1111 0000.0000.0000 2.2222.2222.2222 0000.0000.0000
```

or

```
access-list 800 deny 1.1111.1111.1111 2.2222.2222.2222
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (extended)
ipx access-group
ipx input-network-filter
ipx output-network-filter
ipx router-filter
priority-list protocol †

area-address

To define a set of network numbers to be part of the current NLSP area, use the **area-address** router configuration command. To remove a set of network numbers from the current NLSP area, use the **no** form of this command.

area-address *address mask*
no area-address *address mask*

Syntax Description

address	Network number prefix. This is a 32-bit hexadecimal number.
mask	Mask that defines the length of the network number prefix. This is a 32-bit hexadecimal number.

Default

No area address is defined by default.

Command Mode

Router configuration

Usage Guidelines

You must configure at least one area address before NLSP will operate.

The **area-address** command defines a prefix that includes all networks that are in the area. This prefix allows a single route to an area address to substitute for a longer list of networks.

All networks on which NLSP is enabled must fall under the area address prefix. This configuration is for future compatibility: when Level 2 NLSP becomes available, the only route advertised for the area will be the area address prefix (the prefix represents all networks within the area).

All routers in an NLSP area must be configured with a common area address, or they will form separate areas. You can configure up to three area addresses on the router.

The area address must have zero bits in all bit positions where the mask has zero bits. The mask must consist of only left-justified contiguous one bits.

Examples

The following example defines an area address that includes networks AAAABBC0 through AAAABBDF:

```
area-address AAAABBC0 FFFFFFE0
```

The following example defines an area address that includes all networks:

```
area-address 0 0
```

Related Command

ipx router nlsp

clear ipx accounting

To delete all entries in the accounting database when IPX accounting is enabled, use the **clear ipx accounting** EXEC command.

clear ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Clears the checkpointed database.

Command Mode

EXEC

Usage Guidelines

Specifying the **clear ipx accounting** command with no keywords deletes all entries in the active database.

You can also delete all entries in the checkpointed database by issuing the **clear ipx accounting** command twice in succession.

Example

The following example clears all entries in the active database:

```
clear ipx accounting
```

Related Commands

ipx accounting
ipx accounting-list
ipx accounting-threshold
ipx accounting-transits
show ipx accounting

clear ipx cache

To delete entries from the IPX fast-switching cache, use the **clear ipx cache** EXEC command.

clear ipx cache

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The **clear ipx cache** command clears entries used for fast switching, autonomous switching, and SSE fast switching.

Example

The following example deletes all entries from the IPX fast-switching cache:

```
clear ipx cache
```

Related Commands

ipx route-cache
show ipx cache

clear ipx nlsp neighbors

To delete all NLSP adjacencies from the router’s adjacency database, use the **clear ipx nlsp neighbors** EXEC command.

clear ipx nlsp neighbors

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Deleting all entries from the adjacency database forces all routers in the area to perform the shortest path first (SPF) calculation.

Example

The following example deletes all NLSP adjacencies from the router’s adjacency database:

```
clear ipx nlsp neighbors
```

Related Commands

ipx router nlsp
spf-interval

clear ipx route

To delete routes from the IPX routing table, use the **clear ipx route** EXEC command.

clear ipx route {*network* | **default** | *****}

Syntax Description

network	Number of the network whose routing table entry you want to delete. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.
default	Deletes the default route from the routing table.
*****	Deletes all routes in the routing table.

Command Mode

EXEC

Usage Guidelines

After you use the **clear ipx route** command, RIP/SAP general requests are issued on all IPX interfaces.

Example

The following example clears the entry for network 3 from the IPX routing table:

```
clear ipx route 3
```

Related Command

show ipx route

clear ipx sse

To have the Cisco 7000 series route processor recompute the entries in the IPX SSE fast-switching cache, use the **clear ipx sse** EXEC command.

clear ipx sse

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Recomputing the entries in the RP’s SSE fast-switching cache also updates the SSP’s fast-switching cache.

Example

The following example recomputes the entries in the IPX SSE fast-switching cache:

```
clear ipx sse
```

Related Command

ipx route-cache

clear sse

To reinitialize the route processor on the Cisco 7000 series, use the **clear sse** EXEC command.

clear sse

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

EXEC

Usage Guidelines

The silicon switching engine (SSE) is on the Silicon Switch Processor (SSP) board in the Cisco 7000 series.

Example

The following example causes the route processor to be reinitialized:

```
clear sse
```

distribute-list in

To filter networks received in updates, use the **distribute-list in** router configuration command. To change or cancel the filter, use the **no** form of this command.

distribute-list *access-list-number* **in** [*interface-name*]
no distribute-list *access-list-number* **in** [*interface-name*]

Syntax Description

access-list-number — Standard IPX access list number in the range 800 to 899. The list explicitly specifies which networks are to be received and which are to be suppressed.

in — Applies the access list to incoming routing updates.

interface-name — (Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

Default

Disabled

Command Mode

Router configuration

Example

The following example causes only two networks—network 2 and network 3—to be accepted by an Enhanced IGRP routing process:

```
access-list 800 permit 2
access-list 800 permit 3
access-list 800 deny -1
!
ipx router eigrp 100
network 3
distribute-list 800 in
```

Related Commands

access-list (standard)
distribute-list out
redistribute

distribute-list out

To suppress networks from being advertised in updates, use the **distribute-list out** router configuration command. To cancel this function, use the **no** form of this command.

distribute-list *access-list-number* **out** [*interface-name* | *routing-process*]
no distribute-list *access-list-number* **out** [*interface-name* | *routing-process*]

Syntax Description

access-list-number	Standard IPX access list number in the range 800 to 899. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates.
routing-process	(Optional) Name of a particular routing process (**rip** or **eigrp** *autonomous-system-number*).

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list out** command. This causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list out** command without a process name argument is applied. Addresses not specified in the **distribute-list out** command are not advertised in outgoing routing updates.

Example

The following example causes only one network—network 3—to be advertised by an Enhanced IGRP routing process:

```
access-list 800 permit 3
access-list 800 deny -1
!
ipx router eigrp 100
network 3
distribute-list 800 out
```

Related Commands

access-list (standard)
distribute-list in
redistribute

ipx access-group

To apply a generic output filter to an interface, use **ipx access-group** interface configuration command. To remove the access list, use the **no** form of this command.

ipx access-group *access-list-number*
no ipx access-group *access-list-number*

Syntax Description

access-list-number — Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, *access-list-number* is a decimal number from 900 to 999.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

Generic filters control which packets are sent out an interface based on the packet's source and destination addresses, IPX protocol type, and source and destination socket numbers. You use the standard **access-list** and extended **access-list** commands to specify the filtering conditions.

You can apply only one generic filter to an interface.

Example

In the following example, access list 801 is applied to Ethernet interface 1:

```
interface ethernet 1
ipx access-group 801
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list (extended)
access-list (standard)
priority-list protocol †

ipx accounting

To enable IPX accounting, use the **ipx accounting** interface configuration command. To disable IPX accounting, use the **no** form of this command.

ipx accounting
no ipx accounting

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

IPX accounting allows you to collect information about IPX packets and the number of bytes that are switched through the router. You collect information based on the source and destination IPX address. Accounting tracks only IPX traffic that is passing out of the router; it does not track traffic generated by or terminating at the router.

IPX accounting statistics will be accurate even if IPX fast switching is enabled or if IPX access lists are being used. However, IPX accounting does not keep statistics if autonomous switching is enabled.

The router software maintains two accounting databases, an active database and a checkpointed database.

Example

The following example enables IPX accounting on Ethernet interface 0:

```
interface ethernet 0
ipx accounting
```

Related Commands

clear ipx accounting
ipx accounting-list
ipx accounting-threshold
ipx accounting-transits
show ipx accounting

ipx accounting-list

To filter the networks for which IPX accounting information is kept, use the **ipx accounting-list** global configuration command. To remove the filter, use the **no** form of this command.

ipx accounting-list *number mask*
no ipx accounting-list *number mask*

Syntax Description

number	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA you can enter AA.
mask	Network mask.

Default

No filters are predefined.

Command Mode

Global configuration

Usage Guidelines

The source and destination addresses of each IPX packet are logically ANDed with the mask and compared with the network number. If there is a match, accounting information about the IPX packet is entered into the accounting database. If there is no match, the IPX packet is considered to be a transit packet and may be counted, depending on the setting of the **ipx accounting-transits** global configuration command.

Example

The following example adds all networks with IPX network numbers beginning with 1 to the list of networks for which accounting information is kept:

```
ipx accounting-list 1 0000.0000.0000
```

Related Commands

clear ipx accounting
ipx accounting
ipx accounting-threshold
ipx accounting-transits
show ipx accounting

ipx accounting-threshold

To set the maximum number of accounting database entries, use the **ipx accounting-threshold** global configuration command. To restore the default, use the **no** form of this command.

ipx accounting-threshold *threshold*
no ipx accounting-threshold *threshold*

Syntax Description

threshold	Maximum number of entries (source and destination address pairs) that the router can accumulate.

Default

512 entries

Command Mode

Global configuration

Usage Guidelines

The accounting threshold defines the maximum number of entries (source and destination address pairs) that the router accumulates. The threshold is designed to prevent IPX accounting from consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. To determine whether overflows have occurred, use the **show ipx accounting** EXEC command.

Example

The following example sets the IPX accounting database threshold to 500 entries:

```
ipx accounting-threshold 500
```

Related Commands

clear ipx accounting
ipx accounting
ipx accounting-list
ipx accounting-transits
show ipx accounting

ipx accounting-transits

To set the maximum number of transit entries that will be stored in the IPX accounting database, use the **ipx accounting-transits** global configuration command. To disable this function, use the **no** form of this command.

ipx accounting-transits *count*
no ipx accounting-transits

Syntax Description

count	Number of transit entries that will be stored in the IPX accounting database.

Default

0 entries

Command Mode

Global configuration

Usage Guidelines

Transit entries are those that do not match any of the filters specified by **ipx accounting-list** global configuration commands. If you have not defined any filters, no transit entries are possible.

To maintain accurate accounting totals, the router software maintains two accounting databases: an active database and a checkpointed database.

Example

The following example specifies a maximum of 100 transit records to be stored in the IPX accounting database:

```
ipx accounting-transits 100
```

Related Commands

clear ipx accounting
clear ipx accounting
ipx accounting-list
ipx accounting-threshold
show ipx accounting

ipx advertise-default-route-only

To advertise only the default route via the specified network, use the **ipx advertise-default-route-only** interface configuration command. To advertise all known routes out the interface, use the **no** form of this command.

ipx advertise-default-route-only *network*
no ipx advertise-default-route-only *network*

Syntax Description

network	Number of the network via which to advertise the default route.

Default

Disabled; that is, all known routes are advertised out the interface.

Command Mode

Interface configuration

Usage Guidelines

If you specify the **ipx advertise-default-route-only** command, only the default route, if known, will be advertised out the interface; no other networks will be advertised. If you have a large number of routes in the routing table, for example, on the order of 1000 routes, none of them will be advertised out the interface. However, if the default route is known, it will be advertised. Nodes on the interface can still reach any of the 1000 networks via the default route.

Specifying the **ipx advertise-default-route-only** command results in a significant reduction in CPU processing overhead when there are many routes and many interfaces. It also reduces the load on downstream routers.

Note Services are not considered to be reachable via the default route. They are not added to the service table unless an explicit route to the server's network is known. Therefore, do not specify the **ipx advertise-default-route-only** command if you want services advertised via this interface.

Note Not all routers recognize and support the default route. Use this command with caution if you are not sure if all routers in your network support the default route.

Example

The following example enables the advertising of the default route only:

```
interface ethernet 1
ipx network 1234
ipx advertise-default-route-only 1234
```

Related Command

ipx default-route

ipx backup-server-query-interval

To change the time between successive queries of each Enhanced IGRP neighbor's backup server table, use the **ipx backup-server-query-interval** global configuration command. To restore the default time, use the **no** form of this command.

ipx backup-server-query-interval *interval*
no ipx backup-server-query-interval

Syntax Description

interval	Minimum time, in seconds, between successive queries of each Enhanced IGRP neighbor's backup server table. The default is 15 seconds.

Default

15 seconds

Command Mode

Global configuration

Usage Guidelines

A lower interval may use more CPU resources, but may cause lost server information to be retrieved from other servers' tables sooner.

Example

The following example changes the server query time to 5 seconds:

```
ipx backup-server-query-interval 5
```

ipx bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced IGRP on an interface, use the **ipx bandwidth-percent eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ipx bandwidth-percent eigrp *as-number percent*
no ipx bandwidth-percent eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that Enhanced IGRP may use.

Default

50 percent

Command Mode

Interface configuration

Usage Guidelines

Enhanced IGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured; this may be useful if the bandwidth is set artificially low for other reasons.

Example

The following example allows Enhanced IGRP to use up to 75 percent (42 kbps) of a 56 kbps serial link in autonomous system 209.

```
interface serial 0
bandwidth 56
ipx bandwidth-percent eigrp 209 75
```

Related Commands

bandwidth
ipx router

ipx default-output-rip-delay

To set the default interpacket delay for RIP updates sent on all interfaces, use the **ipx default-output-rip-delay** global configuration command. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-rip-delay *delay*
no ipx default-output-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet RIP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between routing update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Global configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. The **ipx default-output-rip-delay** command sets a default interpacket delay for all interfaces.

The system uses the delay specified by the **ipx default-output-rip-delay** command for periodic and triggered routing updates when no delay is set for periodic and triggered routing updates on an interface. When you set a delay for triggered routing updates, the system uses the delay specified by the **ipx default-output-rip-delay** command for only the periodic routing updates sent on all interfaces.

To set a delay for triggered routing updates, see the **ipx triggered-rip-delay** or **ipx default-triggered-rip-delay** commands.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example sets a default interpacket delay of 55 ms for RIP updates sent on all interfaces:

```
ipx default-output-rip-delay 55
```

Related Command

ipx default-triggered-rip-delay
ipx output-rip-delay
ipx triggered-rip-delay

ipx default-output-sap-delay

To set a default interpacket delay for SAP updates sent on all interfaces, use the **ipx default-output-sap-delay** global configuration command. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-sap-delay *delay*
no ipx default-output-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Global configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. The **ipx default-output-sap-delay** command sets a default interpacket delay for all interfaces.

The system uses the delay specified by the **ipx default-output-sap-delay** command for periodic and triggered SAP updates when no delay is set for periodic and triggered updates on an interface. When you set a delay for triggered updates, the system uses the delay specified by the **ipx default-output-sap-delay** command only for the periodic SAP updates sent on all interfaces.

To set a delay for triggered updates, see the **ipx triggered-sap-delay** or **ipx default-triggered-sap-delay** commands.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these servers.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 interfaces.

Example

The following example sets a default interpacket delay of 55 ms for SAP updates sent on all interfaces:

```
ipx default-output-sap-delay 55
```

Related Command

ipx default-triggered-sap-delay
ipx output-sap-delay
ipx triggered-sap-delay

ipx default-route

To forward towards the default network, if known, all packets for which a route to the destination network is unknown, use the **ipx default-route** global configuration command. To discard all packets for which a route to the destination network is unknown, use the **no** form of this command.

ipx default-route
no ipx default-route

Syntax Description

This command has no arguments or keywords.

Default

Enabled; that is, all packets for which a route to the destination is unknown are forwarded towards the default network, which is –2 (0xFFFFFFFE).

Command Mode

Global configuration

Example

The following example disables the forwarding of packets towards the default network:

```
no ipx default-route
```

Related Command

ipx advertise-default-route-only

ipx default-triggered-rip-delay

To set the default interpacket delay for triggered RIP updates sent on all interfaces, use the **ipx default-triggered-rip-delay** global configuration command. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-rip-delay *delay*
no ipx default-triggered-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet RIP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between routing update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Global configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. A triggered routing update is one that the system sends in response to a “trigger” event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx default-triggered-rip-delay** command sets the default interpacket delay for triggered routing updates sent on all interfaces. On a single interface, you can override this global default delay for triggered routing updates using the **ipx triggered-rip-delay** interface command.

The global default delay for triggered routing updates overrides the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered routing updates.

If the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command is high, then we strongly recommend a low delay value for triggered routing updates so that updates triggered by special events are sent in a more timely manner than periodic routing updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for both periodic and triggered routing updates.

When you use the **no** form of the **ipx default-triggered-rip-delay** command, the system uses the delay set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the “Default” section.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on all interfaces:

```
ipx default-triggered-rip-delay 55
```

Related Command

ipx default-output-rip-delay
ipx output-rip-delay
ipx triggered-rip-delay

ipx default-triggered-sap-delay

To set the default interpacket delay for triggered SAP updates sent on all interfaces, use the **ipx default-triggered-sap-delay** global configuration command. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-sap-delay *delay*
no ipx default-triggered-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Global configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. A triggered SAP update is one that the system sends in response to a “trigger” event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx default-triggered-sap-delay** command sets the default interpacket delay for triggered SAP updates sent on all interfaces. On a single interface, you can override this global default delay for triggered updates using the **ipx triggered-sap-delay** interface command.

The global default delay for triggered updates overrides the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered updates.

If the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command is high, then we strongly recommend a low delay value for triggered updates so that updates triggered by special events are sent in a more timely manner than periodic updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX servers.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered SAP updates, the system uses the delay specified by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for both periodic and triggered SAP updates.

When you use the **no** form of the **ipx default-triggered-sap-delay** command, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the “Default” section.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example sets an interpacket delay of 55 ms for triggered SAP updates sent on all interfaces:

```
ipx default-triggered-sap-delay 55
```

Related Command

ipx default-output-sap-delay
ipx output-sap-delay
ipx triggered-sap-delay

ipx delay

To set the tick count, use the **ipx delay** interface configuration command. To reset the default increment in the delay field, use the **no** form of this command.

ipx delay *ticks*
no ipx delay

Syntax Description

ticks	Number of IBM clock ticks of delay to use. One clock tick is 1/18 of a second (approximately 55 milliseconds).

Default

The default delay is determined from the delay configured on the interface with the **delay** command. It is (interface delay + 333) / 334. Therefore, unless you change the delay by a value greater than 334, you will not notice a difference.

Command Mode

Interface configuration

Usage Guidelines

The **ipx delay** command sets the count used in the IPX RIP delay field, which is also known as the ticks field.

IPXWAN links determine their delay dynamically. Therefore, the **ipx delay** command has no effect.

Leaving the delay at its default value is sufficient for most interfaces.

Example

The following example changes the delay for serial interface 0 to 10 ticks:

```
interface serial 0
ipx delay 10
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

delay †
ipx maximum-paths
ipx output-network-filter
ipx output-rip-delay

ipx down

To administratively shut down an IPX network, use the **ipx down** interface configuration command. To restart the network, use the **no** form of this command.

ipx down *network*
no ipx down

Syntax Description

network	Number of the network to shut down. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

The **ipx down** command administratively shuts down the specified network. The network still exists in the configuration, but is not active. When shutting down, the network sends out update packets informing its neighbors that it is shutting down. This allows the neighboring systems to update their routing, SAP, and other tables without having to wait for routes and services learned via this network to time out.

To shut down an interface in a manner that is considerate of one's neighbor, use **ipx down** before using the **shutdown** command.

Example

The following example administratively shuts down network AA on Ethernet interface 0:

```
interface ethernet 0
ipx down AA
```

ipx gns-reply-disable

To disable the sending of replies to IPX GNS queries, use the **ipx gns-reply-disable** interface configuration command. To return to the default, use the **no** form of this command.

ipx gns-reply-disable
no ipx gns-reply-disable

Syntax Description

This command has no arguments or keywords.

Default

Replies are sent to IPX GNS queries.

Command Mode

Interface configuration

Example

The following example disables the sending of replies to GNS queries on Ethernet interface 0:

```
interface ethernet 0
ipx gns-reply-disable
```

Related Command

ipx gns-response-delay

ipx gns-response-delay

To change the delay when responding to Get Nearest Server (GNS) requests, use the **ipx gns-response-delay** global or interface configuration command. To return to the default delay, use the **no** form of this command.

ipx gns-response-delay [*milliseconds*]
no ipx gns-response-delay

Syntax Description

milliseconds	(Optional) Time, in milliseconds, that the router waits after receiving a Get Nearest Server request from an IPX client before responding with a server name to that client. The default is zero, which indicates no delay.

Default

0 (no delay)

Command Mode

Global configuration, changes the delay globally for the router.
Interface configuration, overrides the globally configured delay for an interface.

Usage Guidelines

This command can be used in two modes: global configuration or interface configuration. In both modes, the command syntax is the same. A delay in responding to Get Nearest Server requests might be imposed so that in certain topologies any local Novell IPX servers respond to the GNS requests before our router does. It is desirable to have these end-host server systems get their reply to the client before the router does, because the client typically takes the first response, not the best. In this case the best response is the one from the local server.

NetWare 2.*x* has a problem with dual-connected servers in parallel with a router. If you are using this version of NetWare, you should set a GNS delay. A value of 500 milliseconds is recommended.

In situations in which servers are always located across routers from their clients, there is no need for a delay to be imposed.

Example

The following example sets the delay in responding to GNS requests to 500 milliseconds (0.5 second):

```
ipx gns-response-delay 500
```

Related Command

ipx gns-reply-disable

ipx gns-round-robin

To rotate using a round-robin selection method through a set of eligible servers when responding to Get Nearest Server (GNS) requests, use the **ipx gns-round-robin** global configuration command. To use the most recently learned server, use the **no** form of this command.

ipx gns-round-robin
no ipx gns-round-robin

Syntax Description

The command has no arguments or keywords.

Default

The most recently learned, eligible server is used.

Command Mode

Global configuration

Usage Guidelines

In the normal server selection process, requests for service are responded to with the most recently learned, closest server. If you enable the round-robin method, the router maintains a list of the nearest servers eligible to provide specific services. It uses this list when responding to Get Nearest Server (GNS) requests. Responses to requests are distributed in a round-robin fashion across all active IPX interfaces on the router.

Eligible servers are those that satisfy the “nearest” requirement for a given request and that are not filtered either by a SAP filter or by a GNS filter.

Example

The following example responds to GNS requests using a round-robin selection method from a list of eligible nearest servers:

```
ipx gns-round-robin
```

Related Commands

ipx output-gns-filter
ipx output-sap-delay

ipx hello-interval eigrp

To configure the interval between Enhanced IGRP hello packets, use the **ipx hello-interval eigrp** interface configuration command. To restore the default interval, use the **no** form of this command.

ipx hello-interval eigrp *autonomous-system-number seconds*
no ipx hello-interval eigrp *autonomous-system-number seconds*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
seconds	Interval between hello packets, in seconds. The default interval is 5 seconds, which is one-third of the default hold time.

Default

For low-speed, NBMA networks: 60 seconds
For all other networks: 5 seconds

Command Mode

Interface configuration

Usage Guidelines

The default of 60 seconds applies only to low speed, nonbroadcast, multiaccess (NBMA) media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for purposes of Enhanced IGRP, Frame Relay and SMDS networks may or may not be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise they are considered not to be NBMA.

Example

The following example changes the hello interval to 10 seconds:

```
interface ethernet 0
ipx network 10
ipx hello-interval eigrp 4 10
```

Related Command

ipx hold-time eigrp

ipx helper-address

To forward broadcast packets (except type 20 propagation packets) to a specified server, use the **ipx helper-address** interface configuration command. To disable this function, use the **no** form of this command.

ipx helper-address *network***.***node*
no ipx helper-address *network***.***node*

Syntax Description

network	Network on which the target IPX server resides. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of –1 indicates all-nets flooding. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.
node	Node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). A node number of FFFF.FFFF.FFFF matches all servers.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Routers normally block all broadcast requests and do not forward them to other network segments. This is done to prevent the degradation of performance over the entire network. The **ipx helper-address** command allows broadcasts to be forwarded to other networks (except type 20 propagation packets). This is useful when a network segment does not have an end-host capable of servicing a particular type of broadcast request. This command lets you forward the broadcasts to a server, network, or networks that can process them. Incoming unrecognized broadcast packets that match the access list created with the **ipx helper-list** command, if it is present, are forwarded.

Note that type 20 propagation packet handling is controlled by a separate mechanism. See the discussion of the **ipx type-20-propagation** command for more information.

You can specify multiple **ipx helper-address** commands on a given interface.

Our routers support all-networks flooded broadcasts (sometimes referred to as *all-nets flooding*). These are broadcast messages that are forwarded to all networks. To configure the all-nets flooding, define the IPX helper address for an interface as follows:

```
ipx helper-address -1.FFFF.FFFF.FFFF
```

On systems configured for IPX routing, this helper address is displayed as follows (via the **show ipx interface** command):

```
FFFFFFFF.FFFF.FFFF.FFFF
```

Although our routers take care to keep broadcast traffic to a minimum, some duplication is unavoidable. When loops exist, all-nets flooding can propagate bursts of excess traffic that will eventually age out when the hop count reaches its limit (16 hops). Use all-nets flooding carefully and only when necessary. Note that you can apply additional restrictions by defining a helper list.

Example

In the following example, all-nets broadcasts on Ethernet interface 0 (except type 20 propagation packets) are forwarded to IPX server 00b4.23cd.110a on network bb:

```
interface ethernet 0
ipx helper-address bb.00b4.23cd.110a
```

Related Commands

ipx helper-list
ipx type-20-propagation

ipx helper-list

To assign an access list to an interface to control broadcast traffic (including type 20 propagation packets), use the **ipx helper-list** interface configuration command. To remove the access list from an interface, use the **no** form of this command.

ipx helper-list *access-list-number*
no ipx helper-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

Default

No access list is preassigned.

Command Mode

Interface configuration

Usage Guidelines

The **ipx helper-list** command specifies an access list to use in forwarding broadcast packets. One use of this command is to prevent client nodes from discovering services they should not use.

Because the destination address of a broadcast packet is by definition the broadcast address, this command is useful only for filtering based on the source address of the broadcast packet.

The helper list, if present, is applied to both all-nets broadcast packets and type 20 propagation packets.

The helper list on the input interface is applied to packets before they are output via either the helper address or type 20 propagation packet mechanism.

You should filter IPX broadcasts on dial-on-demand routing (DDR) and other similar interfaces, because IPX sends broadcast messages very regularly.

Example

The following example assigns access list 900 to Ethernet interface 0 to control broadcast traffic:

```
interface ethernet 0
ipx helper-list 900
```

Related Commands

access-list (extended)
access-list (standard)
ipx helper-address
ipx type-20-propagation

ipx hold-time eigrp

To specify the length of time a neighbor should consider Enhanced IGRP hello packets valid, use the **ipx hold-time eigrp** interface configuration command. To restore the default time, use the **no** form of this command.

ipx hold-time eigrp *autonomous-system-number seconds*
no ipx hold-time eigrp *autonomous-system-number seconds*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
seconds	Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is 15 seconds, which is three times the hello interval.

Default

For low-speed, NBMA networks: 180 seconds
For all other networks: 15 seconds

Command Mode

Interface configuration

Usage Guidelines

If the current value for the hold time is less than two times the interval between hello packets, the hold time will be reset to three times the hello interval.

If a router does not receive a hello packet within the specified hold time, routes through the router are considered available.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds applies only to low speed, nonbroadcast, multiaccess (NBMA) media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Example

The following example changes the hold time to 45 seconds:

```
interface ethernet 0
ipx network 10
ipx hold-time eigrp 4 45
```

Related Command

ipx hello-interval eigrp

ipx input-network-filter

To control which networks are added to the router's routing table, use the **ipx input-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

ipx input-network-filter *access-list-number*
no ipx input-network-filter *access-list-number*

Syntax Description

access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

The **ipx input-network-filter** command controls which networks are added to the routing table based on the networks learned in incoming IPX routing updates (RIP updates) on the interface.

You can issue only one **ipx input-network-filter** command on each interface.

Examples

In the following example, access list 876 controls which networks are added to the routing table when IPX routing updates are received on Ethernet interface 1. Routing updates for network 1b will be accepted. Routing updates for all other networks are implicitly denied and are not added to the routing table.

```
access-list 876 permit 1b
interface ethernet 1
ipx input-network-filter 876
```

The following example is a variation of the preceding that explicitly denies network 1a and explicitly allows updates for all other networks:

```
access-list 876 deny 1a
access-list 876 permit -1
```

Related Commands

access-list (extended)
access-list (standard)
ipx output-network-filter
ipx router-filter

ipx input-sap-filter

To control which services are added to the router's SAP table, use the **ipx input-sap-filter** interface configuration command. To remove the filter, use the **no** form of this command.

ipx input-sap-filter *access-list-number*
no ipx input-sap-filter *access-list-number*

Syntax Description

access-list-number	Number of the SAP access list. All incoming packets are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

The **ipx input-sap-filter** command filters all incoming service advertisements received by the router. This is done prior to a router's accepting information about a service.

You can issue only one **ipx input-sap-filter** command on each interface.

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the **access-list (SAP filtering)** command. Do not use the *network.node* address of the particular interface board.

Example

The following example denies service advertisements about the server at address 3c.0800.89a1.1527, but accepts information about all other services on all other networks:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
interface ethernet 0
ipx input-sap-filter 1000
```

Related Commands

access-list (SAP filtering)
ipx output-sap-filter
ipx router-sap-filter

ipx internal-network

To set an internal network number for use by NLSP and IPXWAN, use the **ipx internal-network** global configuration command. To remove an internal network number, use the **no** form of this command.

ipx internal-network *network-number*
no internal-network [*network-number*]

Syntax Description

network-number	Number of the internal network.

Default

No internal network number is set.

Command Mode

Global configuration

Usage Guidelines

An internal network number is a number assigned to the router.

You must configure an internal network number on each router on an NLSP-capable network in order for NLSP to operate.

When you set an internal network number, the router advertises the specified network out all interfaces. It accepts packets destined to that network at the address *internal-network*.0000.0000.0001.

Example

The following example assigns internal network number e001 to the local router:

```
ipx routing
ipx internal-network e001
```

Related Commands

ipx router nlsp
ipx routing

ipx ipxwan

To enable the IPXWAN protocol on a serial interface, use the **ipx ipxwan** interface configuration command. To disable the IPXWAN protocol, use the **no** form of this command.

ipx ipxwan [*local-node* {*network-number* | **unnumbered**} *local-server-name retry-interval retry-limit*]
no ipxwan

Syntax Description

local-node

(Optional) Primary network number of the router. This is an IPX network number that is unique across the entire internetwork. On NetWare 3.*x* servers, the primary network number is called the internal network number. The router with the higher number is determined to be the link master. A value of 0 causes the router to use the configured internal network number.

network-number

(Optional) IPX network number to be used for the link if this router is the one determined to be the link master. The number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 0 to FFFFFFFD. A value 0 is equivalent to specifying the keyword **unnumbered**.

You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.

unnumbered

(Optional) Specifies that no IPX network number is defined for the link. This is equivalent to specifying a value of 0 for the *network-number* argument.

local-server-name

(Optional) Name of the local router. It can be up to 47 characters long, and can contain uppercase letters, digits, underscores (_), hyphens (-), and at signs (@). On NetWare 3.*x* servers, this is the router name. For our routers, this is the name of the router as configured via the **hostname** command (that is, the name that precedes the standard prompt, which is an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode).

retry-interval

(Optional) Retry interval, in seconds. This interval defines how often the router will retry the IPXWAN start-up negotiation if a start-up failure occurs. Retries will occur until the retry limit defined by the *retry-limit* argument is reached. It can be a value from 1 through 600. The default is 20 seconds.

retry-limit

(Optional) Maximum number of times the router retries the IPXWAN start-up negotiation before taking the action defined by the **ipx ipxwan error** command. It can be a value from 1 through 100. The default is 3.

Default

IPXWAN is disabled.

If you enable IPXWAN, the default is **unnumbered**.

Command Mode

Interface configuration

Usage Guidelines

If you omit all optional arguments and keywords, the **ipx ipxwan** command defaults to **ipx ipxwan 0 unnumbered** *router-name* (which is equivalent to **ipx ipxwan 0** *local-server-name*), where *router-name* is the name of the router as configured with the **hostname** global configuration command. For this configuration, the **show ipx interface** command displays `ipx ipxwan 0 0` *`local-server-name`*.

If you enter a value of 0 for the *network-number* argument, the output of the **show running-config** EXEC command does not show the 0 but rather reports this value as “unnumbered.”

The name of each router on each side of the link must be different.

IPXWAN is a start-up end-to-end options negotiations protocol. When a link comes up, the first IPX packets sent across are IPXWAN packets negotiating the options for the link. When the IPXWAN options have been successfully determined, normal IPX traffic starts. The three options negotiated are the link IPX network number, Ethernet network number, and link delay (ticks) characteristics. The side of the link with the higher local-node number (internal network number) gives the IPX network number and delay to use for the link to the other side. Once IPXWAN finishes, no IPXWAN packets are sent unless link characteristics change or the connection fails. For example, if the IPX delay is changed from the default setting, an IPXWAN restart will be forced.

To enable the IPXWAN protocol on a serial interface, you must not have configured an IPX network number (using the **ipx network** interface configuration command) on that interface.

To control the delay on a link, use the **ipx delay** interface configuration command. If you issue this command when the serial link is already up, the state of the link will be reset and renegotiated.

Example

The following example enables IPXWAN on serial interface 0:

```
interface serial 0
encapsulation ppp
ipx ipxwan
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

encapsulation ppp †
hostname
ipx delay
ipx internal-network
ipx ipxwan error
ipx ipxwan static
ipx network
show ipx interface

ipx ipxwan error

To define how to handle IPXWAN when IPX fails to negotiate properly at link startup, use the **ipx ipxwan error** interface configuration command. To restore the default, use the **no** form of this command.

ipx ipxwan error [**reset** | **resume** | **shutdown**]
no ipxwan error [**reset** | **resume** | **shutdown**]

Syntax Description

reset	(Optional) Resets the link when negotiations fail. This is the default action.
resume	(Optional) When negotiations fail, IPXWAN ignores the failure, takes no special action, and resumes the start-up negotiation attempt.
shutdown	(Optional) Shuts down the link when negotiations fail.

Default

The link is reset.

Command Mode

Interface configuration

Usage Guidelines

Use the **ipx ipxwan error** command to define what action to take if the IPXWAN start-up negotiation fails.

Example

In the following example, the serial link will be shut down if the IPXWAN start-up negotiation fails after three attempts spaced 20 seconds apart:

```
interface serial 0
encapsulation ppp
ipx ipxwan
ipx ipxwan error shutdown
```

Related Commands

ipx ipxwan
ipx ipxwan static

ipx ipxwan static

To negotiate static routes on a link configured for IPXWAN, use the **ipx ipxwan static** interface configuration command. To disable static route negotiation, use the **no** form of this command.

ipx ipxwan static
no ipxwan static

Syntax Description

This command has no arguments or keywords.

Default

Static routing is disabled.

Command Mode

Interface configuration

Usage Guidelines

When you specify the **ipx ipxwan static** command, the interface negotiates static routing on the link. If the router at the other side of the link is not configured to negotiate for static routing, the link will not initialize.

Example

The following example enables static routing with IPXWAN:

```
interface serial 0
encapsulation ppp
ipx ipxwan
ipx ipxwan static
```

Related Commands

ipx ipxwan
ipx ipxwan error

ipx link-delay

To specify the link delay, use the **ipx link-delay** interface configuration command. To return to the default link delay, use the **no** form of this command.

ipx link-delay *microseconds*
no ipx link-delay *microseconds*

Syntax Description

microseconds	Delay, in microseconds.

Default

No link delay (delay of 0)

Command Mode

Interface configuration

Usage Guidelines

The link delay you specify replaces the default value or overrides the value measured by IPXWAN when it starts. The value is also supplied to NLSP for use in metric calculations.

Example

The following example sets the link delay to 20 microseconds:

```
ipx link-delay 20
```

Related Commands

ipx ipxwan
ipx spx-idle-time

ipx maximum-hops

To set the maximum hop count allowed for IPX packets, use the **ipx maximum-hop** global configuration command. To return to the default number of hops, use the **no** form of this command.

ipx maximum-hops *hops*
no ipx maximum-hops *hops*

Syntax Description

hops	Maximum number of hops considered to be reachable by non-RIP routing protocols. Also, maximum number of routers that an IPX packet can traverse before being dropped. It can be a value from 16 through 254. The default is 16 hops.

Default

16 hops

Command Mode

Global configuration

Usage Guidelines

Packets whose hop count is equal to or greater than that specified by the **ipx maximum-hops** command are dropped.

In periodic RIP updates, the router never advertises any network with a hop count greater than 15. However, using protocols other than RIP, the router might learn routes that are farther away than 15 hops. The **ipx maximum-hops** command defines the maximum number of hops that the router will accept as reachable, as well as the maximum number of hops that an IPX packet can traverse before it is dropped by the router. Also, the router will respond to a specific RIP request for a network that is reachable at a distance of greater than 15 hops.

Example

The following command configures the router to accept routes that are up to 64 hops away:

```
ipx maximum-hops 64
```

ipx maximum-paths

To set the maximum number of equal-cost paths the router uses when forwarding packets, use the **ipx maximum-paths** global configuration command. To restore the default value, use the **no** form of this command.

ipx maximum-paths *paths*
no ipx maximum-paths

Syntax Description

paths	Maximum number of equal-cost paths which the router will use. It can be an integer from 1 to 512. The default value is 1.

Default

1 path

Command Mode

Global configuration

Usage Guidelines

The **ipx maximum-paths** command is designed to increase throughput by allowing the router to choose among several equal-cost, parallel paths. (Note that when paths have differing costs, the router chooses lower-cost routes in preference to higher-cost routes.) IPX does load sharing on a packet-by-packet basis in round-robin fashion, regardless of whether you are using fast switching or process switching. That is, the first packet is sent along the first path, the second packet along the second path, and so on. When the final path is reached, the next packet is sent to the first path, the next to the second path, and so on.

Limiting the number of equal-cost paths can save memory on routers with limited memory or very large configurations. Additionally, in networks with a large number of multiple paths and systems with limited ability to cache out-of-sequence packets, performance might suffer when traffic is split between many paths.

Example

In the following example, the router uses up to three parallel paths:

```
ipx maximum-paths 3
```

Related Commands

ipx delay
show ipx route

ipx netbios input-access-filter

To control incoming IPX NetBIOS FindName messages, use the **ipx netbios input-access-filter** interface configuration command. To remove the filter, use the **no** form of this command.

ipx netbios input-access-filter {**host** | **bytes**} *name*
no ipx netbios input-access-filter {**host** | **bytes**} *name*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
name	Name of a NetBIOS access list.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

You can issue only one **ipx netbios input-access-filter host** and one **ipx netbios input-access-filter bytes** command on each interface.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

Example

The following example filters packets arriving on Token Ring interface 1 using the NetBIOS access list “*engineering*”:

```
netbios access-list host engineering permit eng*
netbios access-list host engineering deny manu*
interface tokenring 1
ipx netbios input-access-filter engineering
```

Related Commands

ipx netbios output-access-filter
netbios access-list
show ipx interface

ipx netbios output-access-filter

To control outgoing NetBIOS FindName messages, use the **ipx netbios output-access-filter** interface configuration command. To remove the filter, use the **no** form of this command.

ipx netbios output-access-filter {**host** | **bytes**} *name*
no ipx netbios output-access-filter {**host** | **bytes**} *name*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
name	Name of a previously defined NetBIOS access list.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

You can issue only one **ipx netbios output-access-filter host** and one **ipx netbios output-access-filter bytes** command on each interface.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

Example

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list "engineering":

```
netbios access-list bytes engineering permit 20 AA**04
interface token 1
ipx netbios output-access-filter bytes engineering
```

Related Commands

ipx netbios input-access-filter
netbios access-list
show ipx interface

ipx network

To enable IPX routing on a particular interface and to optionally select the type of encapsulation (framing), use the **ipx network** interface configuration command. To disable IPX routing, use the **no** form of this command.

ipx network {*network* | **unnumbered**} [**encapsulation** *encapsulation-type* [**secondary**]]
no ipx network {*network* | **unnumbered**} [**encapsulation** *encapsulation-type*]

Syntax Description

network

Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD.

You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA you can enter AA.

unnumbered

Specifies an unnumbered interface. For IPXWAN interfaces, the network number need not be preassigned; instead, the nodes may negotiate the network number dynamically.

encapsulation *encapsulation-type*

(Optional) Type of encapsulation (framing). It can be one of the following values:

- **arpa** (for Ethernet interfaces only)—Use Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
- **hdlc** (for serial interfaces only)—Use HDLC encapsulation.
- **novell-ether** (for Ethernet interfaces only)—Use Novell's "Ethernet_802.3" encapsulation.This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by NetWare Version 3.11.

- **sap** (for Ethernet interfaces)—Use Novell’s Ethernet_802.2 encapsulation.This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by NetWare Version 4.0.
  (for Token Ring interfaces)—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.
  (for FDDI interfaces)—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
- **snap** (for Ethernet interfaces)—Use Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header.
  (for Token Ring and FDDI interfaces)—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

secondary (Optional) Indicates an additional (secondary) network configured after the first (primary) network.

Defaults

IPX routing is disabled.

Encapsulation types:
For Ethernet: **novell-ether**
For Token Ring: **sap**
For FDDI: **snap**

Command Mode

Interface configuration

Usage Guidelines

The **ipx network** command allows you to configure more than one logical network on the same physical network (network cable segment). Each network on a given interface must have a different encapsulation type. The first network you configure on an interface is considered to be the primary network. Any additional networks are considered to be secondary networks; these must include the **secondary** keyword. You can also use this command to configure a single logical network on a physical network. NLSP does not support secondary networks. You must use subinterfaces in order to use multiple encapsulations with NLSP.

Note When enabling NLSP and configuring multiple encapsulations on the same physical LAN interface, you must use subinterfaces. You cannot use secondary networks.

You can configure an IPX network on any supported interface as long as all the networks on the same physical interface use a distinct encapsulation type. For example, you can configure up to four IPX networks on a single Ethernet cable because Ethernet supports four encapsulation types.

The interface processes only packets with the correct encapsulation and the correct network number. IPX networks using other encapsulations can be present on the physical network. The only effect on the router is that it uses some processing time to examine packets to determine whether they have the correct encapsulation.

All logical networks on an interface share the same set of configuration parameters. For example, if you change the IPX RIP update time on an interface, you change it for all networks on that interface.

When you define multiple logical networks on the same physical network, IPX treats each encapsulation as if it were a separate physical network. This means, for example, that IPX sends RIP updates and SAP updates for each logical network.

The **ipx network** command is useful when migrating from one type of encapsulation to another. If you are using it for this purpose, you should define the new encapsulation on the primary network.

To delete all networks on an interface, use the following command:

no ipx network

Deleting the primary network with the following command also deletes all networks on that interface. The argument *number* is the number of the primary network.

no ipx network *number*

To delete a secondary network on an interface, use one of the following commands. The argument *number* is the number of a secondary network.

no ipx network *number*
no ipx network *number* **encapsulation** *encapsulation-type*

Examples

The following example uses subinterfaces to create four logical networks on Ethernet interface 0. Each subinterface has a different encapsulation. Any interface configuration parameters that you specify on an individual subinterface are applied to that subinterface only.

```
ipx routing
interface ethernet 0.1
ipx network 1 encapsulation novell-ether
interface ethernet 0.2
ipx network 2 encapsulation snap
interface ethernet 0.3
ipx network 3 encapsulation arpa
interface ethernet 0.4
ipx network 4 encapsulation sap
```

The following example uses primary and secondary networks to create the same four logical networks as shown earlier in this section. Any interface configuration parameters that you specify on this interface are applied to all the logical networks. For example, if you set the routing update timer to 120 seconds, this value is used on all four networks.

```
ipx routing
interface ethernet 0
ipx network 1 encapsulation novell-ether
ipx network 2 encapsulation snap secondary
ipx network 3 encapsulation arpa secondary
ipx network 4 encapsulation sap secondary
```

Related Command

ipx routing

ipx nlsp csnp-interval

To configure the NLSP complete sequence number PDU (CSNP) interval, use the **ipx nlsp csnp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

ipx nlsp csnp-interval *seconds*
no ipx nlsp csnp-interval *seconds*

Syntax Description

seconds	Time, in seconds, between the transmission of CSNPs on multiaccess networks. This interval applies to the designated router only. The interval can be a number in the range 1 to 600. The default is 30 seconds.

Default

30 seconds

Command Mode

Interface configuration

Usage Guidelines

The **ipx nlsp csnp-interval** command applies only to the designated router for the specified interface only. This is because only designated routers send CSNP packets, which are used to synchronize the database.

CSNP does not apply to serial point-to-point interfaces. However, it does apply to WAN connections if the WAN is viewed as a multiaccess meshed network.

Example

The following example configures Ethernet interface 0 to transmit CSNPs every 10 seconds:

```
interface ethernet 0
ipx nlsp csnp-interval 10
```

Related Commands

ipx nlsp hello-interval
ipx nlsp retransmit-interval

ipx nlsp enable

To enable NLSP routing on the primary network configured on this interface or subinterface, use the **ipx nlsp enable** interface configuration command. To disable NLSP routing on the primary network configured on this interface or subinterface, use the **no** form of this command.

ipx nlsp enable
no ipx nlsp enable

Syntax Description

This command has no arguments or keywords.

Default

NLSP is disabled on all interfaces.

Command Mode

Interface configuration

Usage Guidelines

When you enable NLSP routing, the current settings for RIP and SAP compatibility modes as specified with the **ipx nlsp rip** and **ipx nlsp sap** interface configuration commands take effect automatically.

Examples

The following example enables NLSP routing on Ethernet interface 0:

```
interface ethernet 0
ipx nlsp enable
```

The following example enables NLSP routing on serial interface 0:

```
interface serial 0
ipx ipxwan 2442 unnumbered local1
ipx nlsp enable
```

Related Commands

ipx nlsp rip
ipx nlsp sap

ipx nlsp hello-interval

To configure the interval between the transmission of hello packets, use the **ipx nlsp hello-interval** interface configuration command. To restore the default value, use the **no** form of this command.

ipx nlsp hello-interval *seconds*
no nlsp hello-interval *seconds*

Syntax Description

seconds	Time, in seconds, between the transmission of hello packets on the interface. It can be a decimal integer in the range 1 to 1600. The default is 10 seconds for the designated router and 20 seconds for nondesignated routers.

Defaults

10 seconds for the designated router
20 seconds for nondesignated routers

Command Mode

Interface configuration

Usage Guidelines

The designated router sends hello packets at an interval equal to one-half the configured value.

Use this command to improve the speed at which a failed router is detected. A router is declared to be down if a hello has not been received from it for three times the hello interval (by default, 60 seconds for nondesignated routers and 30 seconds for designated routers). You can reduce this time by lowering the hello-interval setting, at the cost of increased traffic overhead.

Example

The following example configures serial interface 0 to transmit hello packets every 30 seconds:

```
interface serial 0
ipx nlsp hello-interval 30
```

Related Commands

ipx nlsp csnp-interval
ipx nlsp retransmit-interval

ipx nlsp metric

To configure the NLSP cost for an interface, use the **ipx nlsp metric** interface configuration command. To restore the default cost, use the **no** form of this command.

ipx nlsp metric *metric-number*
no nlsp metric *metric-number*

Syntax Description

metric-number	Metric value for the interface. It can be a decimal integer from 0 to 63.

Default

The default varies based on the throughput of the link connected to the interface.

Command Mode

Interface configuration

Usage Guidelines

Use the **ipx nlsp metric** command to cause NLSP to prefer some links over others. A link with a lower metric is more preferable than one with a higher metric.

Typically, it is not necessary to configure the metric; however, it may be desirable in some cases when there are wide differences in link bandwidths. For example, using the default metrics, a single 64-kbps ISDN link will be preferable to two 1544-kbps T1 links.

Example

The following example configures a metric of 10 on serial interface 0:

```
interface serial 0
ipx nlsp metric 10
```

Related Command

ipx nlsp enable

ipx nlsp priority

To configure the election priority of the specified interface for designated router election, use the **ipx nlsp priority** interface configuration command. To restore the default priority, use the **no** form of this command.

ipx nlsp priority *priority-number*
no ipx nlsp priority *priority-number*

Syntax Description

priority-number	Election priority of the designated router for the specified interface. This can be a number in the range 0 to 127. This value is unitless. The default is 44.

Default

44

Command Mode

Interface configuration

Usage Guidelines

Use the **ipx nlsp priority** command to control which router is elected designated router. The router with the highest priority number is selected as the designated router.

The designated router increases its own priority by 20 in order to keep its state as of the designated router more stable. To have a particular router be elected designated router, configure its priority to be at least 65.

Example

The following example sets the designated router election priority to 65:

```
ipx nlsp priority 65
```

ipx nlsp retransmit-interval

To configure the link-state packet (LSP) retransmission interval on WAN links, use the **ipx nlsp retransmit-interval** interface configuration command. To restore the default interval, use the **no** form of this command.

ipx nlsp retransmit-interval *seconds*
no ipx nlsp priority *seconds*

Syntax Description

seconds	LSP retransmission interval, in seconds. This can be a number in the range 1 to 30. The default is 5 seconds.

Default

5 seconds

Command Mode

Interface configuration

Usage Guidelines

Reducing the retransmission interval can improve the rate of convergence of the network in the face of lossy WAN links at the cost of potentially increasing link utilization.

Example

The following example configures the LSP retransmission interval to 2 seconds:

```
ipx nlsp retransmit-interval 2
```

Related Commands

ipx nlsp csnp-interval
ipx nlsp hello-interval

ipx nlsp rip

To configure RIP compatibility when NLSP is enabled, use the **ipx nlsp rip** interface configuration command. To restore the default, use the **no** form of this command.

ipx nlsp rip [**on** | **off** | **auto**]
no ipx nlsp rip [**on** | **off** | **auto**]

Syntax Description

on	(Optional) Always generates and sends RIP periodic traffic.
off	(Optional) Never generates and sends RIP periodic traffic.
auto	(Optional) Sends RIP periodic traffic only if another RIP router in sending periodic RIP traffic. This is the default.

Default

RIP periodic traffic is sent only if another router in sending periodic RIP traffic.

Command Mode

Interface configuration

Usage Guidelines

The **ipx nlsp rip** command is meaningful only on networks on which NLSP is enabled. (RIP and SAP are always on by default on other interfaces.) Because the default mode is **auto**, no action is normally required to fully support RIP compatibility on an NLSP network.

Example

In the following example, the interface never generates or sends RIP periodic traffic:

```
interface ethernet 0
ipx nlsp rip off
```

Related Commands

ipx nlsp enable
ipx nlsp sap

ipx nlsp sap

To configure SAP compatibility when NLSP in enabled, use the **ipx nlsp sap** interface configuration command. To restore the default, use the **no** form of this command.

ipx nlsp sap [**on** | **off** | **auto**]
no ipx nlsp sap [**on** | **off** | **auto**]

Syntax Description

on	(Optional) Always generates and sends SAP periodic traffic.
off	(Optional) Never generates and sends SAP periodic traffic.
auto	(Optional) Sends SAP periodic traffic only if another SAP router in sending periodic SAP traffic. This is the default.

Default

SAP periodic traffic is sent only if another router in sending periodic SAP traffic.

Command Mode

Interface configuration

Usage Guidelines

The **ipx nlsp sap** command is meaningful only on networks on which NLSP is enabled. Because the default mode is **auto**, no action is normally required to fully support SAP compatibility on an NLSP network.

Example

In the following example, the interface never generates or sends SAP periodic traffic:

```
interface ethernet 0
ipx nlsp sap off
```

Related Commands

ipx nlsp enable
ipx nlsp rip

ipx output-gns-filter

To control which servers are included in the Get Nearest Server (GNS) responses sent by the router, use the **ipx output-gns-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

ipx output-gns-filter *access-list-number*
no ipx output-gns-filter *access-list-number*

Syntax Description

access-list-number	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

You can issue only one **ipx output-gns-filter** command on each interface.

Example

The following example excludes the server at address 3c.0800.89a1.1527 from GNS responses sent on Ethernet interface 0, but allows all other servers:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing
interface ethernet 0
ipx output-gns-filter 1000
```

Related Commands

access-list (SAP filtering)
ipx gns-round-robin

ipx output-network-filter

To control the list of networks included in routing updates sent out an interface, use the **ipx output-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

ipx output-network-filter *access-list-number*
no ipx output-network-filter *access-list-number*

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

The **ipx output-network-filter** command controls which networks the router advertises in its IPX routing updates (RIP updates).

You can issue only one **ipx output-network-filter** command on each interface.

Example

In the following example, access list 896 controls which networks are specified in routing updates sent out the serial 1 interface. This configuration causes network 2b to be the only network advertised in Novell routing updates sent on the specified serial interface.

```
access-list 896 permit 2b
interface serial 1
ipx output-network-filter 896
```

Related Commands

access-list (extended)
access-list (standard)
ipx input-network-filter
ipx router-filter

ipx output-rip-delay

To set the interpacket delay for RIP updates sent on a single interface, use the **ipx output-rip-delay** interface configuration command. To return to the default value, use the **no** form of this command.

ipx output-rip-delay *delay*
no ipx output-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet RIP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between routing update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Interface configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. The **ipx output-rip-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-rip-delay** command for periodic and triggered routing updates when no delay is set for triggered routing updates. When you set a delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** command for only the periodic routing updates sent on the interface.

To set a delay for triggered routing updates, see the **ipx triggered-rip-delay** or **ipx default-triggered-rip-delay** commands.

You can also set a default RIP interpacket delay for all interfaces. See the **ipx default-output-rip-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example establishes a 55-ms interpacket delay on serial interface 0:

```
interface serial 0
ipx network 106A
ipx output-rip-delay 55
```

Related Command

ipx update-time
ipx default-output-rip-delay
ipx default-triggered-rip-delay
ipx triggered-rip-delay

ipx output-sap-delay

To set the interpacket delay for SAP updates sent on a single interface, use the **ipx output-sap-delay** interface configuration command. To return to the default delay value, use the **no** form of this command.

ipx output-sap-delay *delay*
no ipx output-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Interface configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. The **ipx output-sap-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-sap-delay** command for periodic and triggered SAP updates when no delay is set for triggered updates. When you set a delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** command only for the periodic updates sent on the interface.

To set a delay for triggered updates, see the **ipx triggered-sap-delay** or **ipx default-triggered-sap-delay** commands.

You can also set a default SAP interpacket delay for all interfaces. See the **ipx default-output-sap-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by the **ipx output-sap-delay** command forces the router to pace its output to the slower-processing needs of these servers.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example establishes a 55-ms delay between packets in multiple-packet SAP updates on Ethernet interface 0:

```
interface ethernet 0
ipx network 106A
ipx output-sap-delay 55
```

Related Command

ipx default-output-sap-delay
ipx default-triggered-sap-delay
ipx sap-interval
ipx triggered-sap-delay

ipx output-sap-filter

To control which services are included in Service Advertisement Protocol (SAP) updates sent by the router, use the **ipx output-network-filter** interface configuration command. To remove the filter, use the **no** form of this command.

ipx output-sap-filter *access-list-number*
no ipx output-sap-filter *access-list-number*

Syntax Description

access-list-number	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

The router applies output SAP filters prior to sending SAP packets.

You can issue only one **ipx output-sap-filter** command on each interface.

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the SAP **access-list** command. Do not use the *network.node* address of the particular interface board.

Example

The following example denies service advertisements about server 0000.0000.0001 on network aa from being send on network 4d (via Ethernet interface 1). All other services are advertised via this network. All services, included those from server aa.0000.0000.0001, are advertised via networks 3c and 2b.

```
access-list 1000 deny aa.0000.0000.0001
access-list 1000 permit -1
interface ethernet 0
ipx net 3c
interface ethernet 1
ipx network 4d
ipx output-sap-filter 1000
interface serial 0
ipx network 2b
```

Related Commands

access-list (SAP filtering)
ipx gns-round-robin
ipx input-sap-filter
ipx router-sap-filter

ipx pad-process-switched-packets

To control whether odd-length packets are padded so as to be sent as even-length packets on an interface, use the **ipx pad-process-switched-packets** interface configuration command. To disable padding, use the **no** form of this command.

ipx pad-process-switched-packets
no ipx pad-process-switched-packets

Syntax Description

This command has no arguments or keywords.

Default

Enabled on Ethernet interfaces
Disabled on Token Ring, FDDI, and serial interfaces

Command Mode

Interface configuration

Usage Guidelines

Use this command only under the guidance of a customer engineer or other service representative.

The **ipx pad-process-switched-packets** command affects process-switched packets only, so you must disable fast switching before the **ipx pad-process-switched-packets** command has any effect.

Some IPX end hosts reject Ethernet packets that are not padded. Certain topologies can result in such packets being forwarded onto a remote Ethernet network. Under specific conditions, padding on intermediate media can be used as a temporary workaround for this problem.

Example

The following command configures the router to pad odd-length packets so that they are sent as even-length packets on Ethernet interface 1.

```
interface ethernet 1
ipx pad-process-switched-packets
```

Related Command

ipx route-cache

ipx ping-default

To select the ping type that the router transmits, use the **ipx ping-default** global configuration command. To return to the default ping type, use the **no** form of this command.

ipx ping-default {**cisco** | **novell**}
no ipx ping-default {**cisco** | **novell**}

Syntax Description

cisco	Transmits Cisco pings.
novell	Transmits standard Novell pings.

Default

Cisco pings

Command Mode

Global configuration

Usage Guidelines

Standard Novell pings conform to the definition in the Novell NLSP specification.

Example

The following example enables standard Novell pings:

```
ipx ping-default novell
```

Related Command

ping (user)

ipx rip-max-packetsize

To configure the maximum packet size of RIP updates sent out the interface, use the **ipx rip-max-packetsize** interface configuration command. To restore the default packet size, use the **no** form of this command.

ipx rip-max-packetsize *bytes*
no ipx rip-max-packetsize *bytes*

Syntax Description

bytes	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each plus a 32-byte IPX RIP header.

Default

432 bytes

Command Mode

Interface configuration

Usage Guidelines

The maximum size is for the IPX packet excluding the media header.

Do not allow the maximum packet size to exceed the allowed maximum size of packets for the interface.

Example

The following example sets the maximum RIP update packet to 832 bytes:

```
ipx rip-max-packetsize 832
```

Related Command

ipx sap-max-packetsize

ipx rip-multiplier

To configure the interval at which a network's RIP entry ages out, use the **ipx rip-multiplier** interface configuration command. To restore the default interval, use the **no** form of this command.

ipx rip-multiplier *multiplier*
no ipx rip-multiplier *multiplier*

Syntax Description

multiplier	Multiplier used to calculate the interval at which to age out RIP routing table entries. This can be any positive integer. The value you specify is multiplied by the RIP update interval to determine the aging-out interval. The default is three times the RIP update interval.

Default

Three times the RIP update interval.

Command Mode

Interface configuration

Usage Guidelines

All routers on the same physical cable should use the same multiplier value.

Example

In the following example, in a configuration where RIP updates are sent once every 2 minutes, the interval at which RIP entries age out is set to 10 minutes:

```
interface ethernet 0
ipx rip-multiplier 5
```

Related Command

ipx update-interval

ipx route

To add a static route to the routing table, use the **ipx route** global configuration command. To remove a route from the routing table, use the **no** form of this command.

ipx route {*network* | **default**} {*network***.***node* | *interface*} [**floating-static**]
no ipx route

Syntax Description

network	Network to which you want to establish a static route. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.
default	Default network number as defined by the **ipx default-route** global configuration command.
*network***.***node*	Router to which to forward packets destined for the specified network. The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA. The argument *node* is the node number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
interface	Network interface to which to forward packets destined for the specified network. Interface is serial 0 or serial 0.2. Specifying an interface instead of a network node is intended for use on IPXWAN unnumbered interfaces. The specified interface can be a null interface.
floating-static	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.

Default

No static routes are predefined.

Command Mode

Global configuration

Usage Guidelines

The **ipx route** command forwards packets destined for the specified network (*network*) via the specified router (*network.node*) or an interface (*interface*) on that network regardless of whether that router is sending dynamic routing information.

Floating static routes are static routes that can be overridden by dynamically learned routes. Floating static routes allow you to switch to another path whenever routing information for a destination is lost. One application of floating static routes is to provide back-up routes in topologies where dial-on-demand routing is used.

If you configure a floating static route, the router checks to see if an entry for the route already exists in its routing table. If a dynamic route already exists, the floating static route is placed in reserve as part of a floating static route table. When the router detects that the dynamic route is no longer available, it replaces the dynamic route with the floating static route for that destination. If the route is later relearned dynamically, the dynamic route replaces the floating static route and the floating static route is again placed in reserve.

If you specify an interface instead of a network node address, the interface must be an IPXWAN unnumbered interface. For IPXWAN interfaces, the network number need not be preassigned; instead, the nodes may negotiate the network number dynamically.

Note that by default, floating static routes are not redistributed into other dynamic protocols.

Example

In the following example, the router at address 3abc.0000.0c00.1ac9 handles all traffic destined for network 5e:

```
ipx routing
ipx route 5e 3abc.0000.0c00.1ac9
```

Related Commands

ipx default-route
show ipx route

ipx route-cache

To enable IPX fast switching and autonomous switching, use the **ipx route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

ipx route-cache [**cbus** | **sse**]
no ipx route-cache [**cbus** | **sse**]

Syntax Description

cbus	(Optional) Enables IPX autonomous switching.
sse	(Optional) Enables SSE fast switching.

Defaults

Fast switching is enabled.
Autonomous switching is disabled.
SSE switching is disabled.

Command Mode

Interface configuration

Usage Guidelines

Specifying the **ipx route-cache** command with no keywords enables fast switching.

Fast switching allows higher throughput by switching packets using a cache created by previous transit packets. On ciscoBus-2 interface cards, fast switching is done between all encapsulation types. On other interface cards, fast switching is done in all cases *except* the following: transfer of packets with **sap** encapsulation from an Ethernet, a Token Ring, or an FDDI network to a standard serial line.

You might want to disable fast switching in two situations. One is if you want to save memory on the interface cards: fast-switching caches require more memory than those used for standard switching. The second situation is to avoid congestion on interface cards when a high-bandwidth interface is writing large amounts of information to a low-bandwidth interface.

Autonomous switching provides faster packet switching by allowing the ciscoBus processor to switch packets independently without having to interrupt the system processor. It is available only in Cisco 7000 systems, and in AGS+ systems with high-speed network controller ciscoBus2-only interfaces, such as the CCTL2 ciscoBus controller running microcode version 11.0 or later.

Autonomous switching is supported to and from all encapsulation types that you can use on IEEE interfaces; it is also supported to and from serial HDLC encapsulation. Table 21-4 lists the encapsulation types you can use on IEEE interfaces and shows the correspondence between the encapsulation type and the IPX frame type.

Table 21-4 Novell IPX Encapsulation Types on IEEE Interfaces

Interface Type	Encapsulation Type	IPX Frame Type
Ethernet	novell-ether (default) arpa sap snap	Ethernet_802.3 Ethernet_II Ethernet_802.2 Ethernet_Snap
Token Ring	sap (default) snap	Token-Ring Token-Ring_Snap
FDDI	snap (default) sap	Fddi_Snap Fddi_802.2

SSE fast switching uses the silicon switching engine (SSE) on the Cisco 7000 Series SSP card to perform packet switching.

Examples

The following example enables fast switching and autonomous switching on an interface:

```
interface ethernet 0
ipx route-cache cbus
```

The following example enables fast switching and SSE fast switching on an interface:

```
interface ethernet 0/1
ipx route-cache sse
```

In the following example, both fast switching and autonomous switching are turned off on an interface:

```
interface ethernet 0
no ipx route-cache
```

Assuming that Ethernet 0 has **ipx route-cache** and **ipx route-cache cbus** is enabled, the following example turns off only autonomous switching on an interface, but leaves fast switching enabled:

```
interface ethernet 0
no ipx route-cache cbus
```

Related Commands

clear ipx cache
ipx source-network-update
ipx watchdog-spoof
show ipx cache

ipx router

To specify the routing protocol to use, use the **ipx router** global configuration command. To disable a particular routing protocol on the router, use the **no** form of this command.

ipx router {**eigrp** *autonomous-system-number* | **nlsp** | **rip**}
no ipx router {**eigrp** *autonomous-system-number* | **nlsp** | **rip**}

Syntax Description

eigrp *autonomous-system-number*	Enables the Enhanced IGRP routing protocol. The argument *autonomous-system-number* is the Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
nlsp	Enables the NLSP routing protocol.
rip	Enables the RIP routing protocol. It is on by default.

Default

RIP is enabled.

Command Mode

Global configuration

Usage Guidelines

You must explicitly disable RIP by issuing the **no ipx router rip** command if you do not want to use this routing protocol.

You can configure multiple Enhanced IGRP processes on a router. To do so, assign each a different autonomous system number.

Example

The following example enables Enhanced IGRP on the router:

```
ipx router eigrp 4
```

Related Commands

network
redistribute

ipx router-filter

To control the routers from which packets are accepted, use the **ipx router-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

ipx router-filter *access-list-number*
no ipx router-filter

Syntax Description

access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

You can issue only one **ipx router-filter** command on each interface.

Example

In the following example, access list 866 controls the routers from which packets are accepted. For Ethernet interface 0, only packets from the router at 3c.0000.00c0.047d are accepted. All other packets are implicitly denied.

```
access-list 866 permit 3c.0000.00c0.047d
interface ethernet 0
ipx router-filter 866
```

Related Commands

access-list (extended)
access-list (standard)
ipx input-network-filter
ipx output-network-filter

ipx router-sap-filter

To filter Service Advertisement Point (SAP) messages received from a particular router, use the **ipx router-sap-filter** interface configuration command. To remove the filter, use the **no** form of this command.

ipx router-sap-filter *access-list-number*
no ipx router-sap-filter *access-list-number*

Syntax Description

access-list-number	Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

Default

No filters are predefined.

Command Mode

Interface configuration

Usage Guidelines

You can issue only one **ipx router-sap-filter** command on each interface.

Example

In the following example, the router will receive service advertisements only from router aa.0207.0104.0874:

```
access-list 1000 permit aa.0207.0104.0874
access-list 1000 deny -1
interface ethernet 0
ipx router-sap-filter 1000
```

Related Commands

access-list (SAP filtering)
ipx input-sap-filter
ipx output-sap-filter
ipx sap
show ipx interface

ipx routing

To enable IPX routing, use the **ipx routing** global configuration command. To disable IPX routing, use the **no** form of this command.

ipx routing [*node*]
no ipx routing

Syntax Description

node	(Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). It must not be a multicast address. If you omit *node*, the router uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (such as only serial interfaces), you must specify *node*.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

The **ipx routing** command enables the IPX Routing Information Protocol (RIP) and Service Advertisement Point (SAP) services on the router.

If you omit the argument *node* and if the MAC address later changes, the IPX node address automatically changes to the new address. However, connectivity may be lost between the time that the MAC address changes and the time that the IPX clients and servers learn the router's new address.

If you plan to use DECnet and IPX routing concurrently on the same interface, you should enable DECnet router first, then enable IPX routing without specifying the optional MAC node number. If you enable IPX before enabling DECnet routing, routing for IPX will be disrupted.

Example

The following example enables IPX routing:

```
ipx routing
```

Related Command

ipx network

ipx sap

To specify static Service Advertisement Protocol (SAP) entries, use the **ipx sap** global configuration command. To remove static SAP entries, use the **no** form of this command.

ipx sap *service-type name network***.***node socket hop-count*
no ipx sap *service-type name network***.***node socket hop-count*

Syntax Description

service-type SAP service-type number. Table 21-3 earlier in this chapter lists some IPX SAP services.

name Name of the server that provides the service.

*network***.***node* Network number and node address of the server.

The argument network is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA you can enter AA.

The argument node is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

socket Socket number for this service. Table 21-2 earlier in this chapter lists some IPX socket numbers.

hop-count Number of hops to the server.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

The **ipx sap** command allows you to add static entries into the SAP table. Each entry has a SAP service associated with it. Static SAP assignments always override any identical entries in the SAP table that are learned dynamically, regardless of hop count. The router will not announce a static SAP entry unless it has a route to that network.

Example

In the following example, the route to `JOES_SERVER` is not yet learned, so the system displays an informational message. The `JOES_SERVER` service will not be announced in the regular SAP updates until the router learns the route to it either by means of a RIP update from a neighbor or an **ipx sap** command.

```
ipx sap 107 MAILSERV 160.0000.0c01.2b72 8104 1
ipx sap 4 FILESERV 165.0000.0c01.3d1b 451 1
ipx sap 143 JOES_SERVER A1.0000.0c01.1234 8170 2
no route to A1, JOES_SERVER won't be announced until route is learned
```

Related Commands

ipx input-sap-filter
ipx output-sap-filter
ipx router-sap-filter
show ipx servers

ipx sap-incremental

To send SAP updates only when a change occurs in the SAP table, use the **ipx sap-incremental** interface configuration command. To send periodic SAP updates, use the **no** form of this command.

ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]
no ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

Syntax Description

eigrp *autonomous-system-number*	IPX Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
rsup-only	(Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

Default

Enabled on serial interfaces
Disabled on LAN media (Ethernet, Token Ring, FDDI)

Command Mode

Interface configuration

Usage Guidelines

In order to use the **ipx sap-incremental** command, you must enable Enhanced IGRP on the router. This is the case even if you want to use only RIP routing. You must do this because the incremental SAP feature requires the Enhanced IGRP reliable transport mechanisms.

With this functionality enabled, if an IPX Enhanced IGRP peer is found on the interface, SAP updates will be sent only when a change occurs in the SAP table. Periodic SAP updates are not sent. When no IPX Enhanced IGRP peer is present on the interface, periodic SAPs are always sent regardless of how this command is set.

If you configure the local router to send incremental SAP updates on an Ethernet, and if the local router has at least one IPX Enhanced IGRP neighbor and any servers, clients, or routers that do not have IPX Enhanced IGRP configured on the Ethernet interface, these devices will not receive complete SAP information from the local router.

If the incremental sending of SAP updates on an interface is configured and no IPX Enhanced IGRP peer is found, SAP updates will be sent periodically until a peer is found. Then, updates will be sent only when changes occur in the SAP table.

To take advantage of Enhanced IGRP's incremental SAP update mechanism while using the RIP routing protocol instead of the Enhanced IGRP routing protocol, specify the **rsup-only** keyword. SAP updates are then sent only when changes occur, and only changes are sent. Use this feature only when you want to use RIP routing.

Example

The following example sends SAP updates on Ethernet interface 0 only when there is a change in the SAP table:

```
interface ethernet 0
ipx sap-incremental eigrp 200
```

ipx sap-interval

To configure less frequent Service Advertisement Point (SAP) updates over slow links, use the **ipx sap-interval** interface configuration command. To return to the default value, use the **no** form of this command.

ipx sap-interval *interval*
no ipx sap-interval

Syntax Description

interval	Interval, in minutes, between SAP updates sent by the router. The default value is 1 minute. If *interval* is 0, periodic updates are never sent.

Default

1 minute

Command Mode

Interface configuration

Usage Guidelines

Setting the interval at which SAP updates are sent is most useful on limited-bandwidth, point-to-point links or on X.25 interfaces.

You should ensure that all IPX servers and routers on a given network have the same SAP interval. Otherwise, they may decide that a server is down when it is really up.

It is not possible to change the interval at which SAP updates are sent on most PC-based servers. This means that you should never change the interval for an Ethernet or Token Ring network that has servers on it.

Setting the interval to zero means that periodic SAP updates are never sent. It is recommended that you never do this. If you set the interval to zero, routers that are inaccessible for any reason when a server powers up or shuts down will miss that event, and will either fail to learn about new servers or fail to detect that the server shut down.

Example

In the following example, SAP updates are sent (and expected) on serial interface 0 every 5 minutes:

```
interface serial 0
ipx sap-interval 5
```

Related Command

ipx output-sap-delay

ipx sap-max-packetsize

To configure the maximum packet size of SAP updates sent out the interface, use the **ipx sap-max-packetsize** interface configuration command. To restore the default packet size, use the **no** form of this command.

ipx sap-max-packetsize *bytes*
no ipx sap-max-packetsize *bytes*

Syntax Description

bytes — Maximum packet size in bytes. The default is 480 bytes, which allows for seven servers (64 bytes each) plus a 32-byte IPX SAP header.

Default

480 bytes

Command Mode

Interface configuration

Usage Guidelines

The maximum size is for the IPX packet excluding the media header. For example, to allow ten servers per SAP packet, you would configure (32 + (10 x 64)), or 672 bytes for the maximum packet size.

You are responsible for guaranteeing that the maximum packet size does not exceed the allowed maximum size of packets for the interface.

Example

The following example sets the maximum SAP update packet size to 672 bytes:

```
ipx sap-max-packetsize 672
```

Related Command

ipx rip-max-packetsize

ipx sap-multiplier

To configure the interval at which a network's or server's SAP entry ages out, use the **ipx sap-multiplier** interface configuration command. To restore the default interval, use the **no** form of this command.

ipx sap-multiplier *multiplier*
no ipx sap-multiplier *multiplier*

Syntax Description

multiplier	Multiplier used to calculate the interval at which to age out SAP routing table entries. This can be any positive integer. The value you specify is multiplied by the SAP update interval to determine the aging-out interval. The default is three times the SAP update interval.

Default

Three times the SAP update interval.

Command Mode

Interface configuration

Usage Guidelines

All routers on the same physical cable should use the same multiplier value.

Example

In the following example, in a configuration where SAP updates are sent once every 1 minute, the interval at which SAP entries age out is set to 10 minutes:

```
interface ethernet 0
ipx sap-multiplier 10
```

Related Command

ipx sap-max-packetsize

ipx sap-queue-maximum

To configure the maximum length of the queue of pending input SAP GNS requests and SAP query packets, use the **ipx sap-queue-maximum** global configuration command. To return to the default value, use the **no** form of this command.

ipx sap-queue-maximum *number*
no ipx sap-interval

Syntax Description

number	Maximum length of the queue of pending SAP requests. By default, there is no limit to the number of pending SAP requests that the router stores in this queue.

Default

No maximum queue size

Command Mode

Global configuration

Usage Guidelines

The router maintains a list of SAP requests to process, including all pending Get Nearest Server (GNS) queries from clients attempting to reach servers. When the network is restarted, the router can be inundated with hundreds of requests for servers. Most of these can be repeated requests from the same clients. The **ipx sap-queue-maximum** command allows you to configure the maximum length allowed for the pending SAP requests queue. Packets received when the queue is full are dropped.

Example

The following example sets the length of the queue of pending SAP requests to 20:

```
ipx sap-queue-maximum 20
```

ipx source-network-update

To repair corrupted network numbers, use the **ipx source-network-update** interface configuration command. To disable this feature, use the **no** form of this command.

ipx source-network-update
no ipx source-network-update

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

In some early implementations of IPX client software, it was possible for the client's network number to become corrupted. The **ipx source-network-update** command repairs this number by setting the source network field of any packet on the local network that has a hop count of zero.

You must disable fast switching with the **no ipx route-cache** command before using the **ipx source-network-update** command.

This command interferes with the proper working of OS/2 Requestors. Therefore, do not use this command in a network that has OS/2 Requestors.

Do not use the **ipx source-network-update** command on interfaces on which NetWare servers are using internal network numbers.

Caution The **ipx source-network-update** command interferes with the proper working of OS/2 Requestors. Do not use this command in a network that has OS/2 Requestors.

Caution Do not use the **ipx source-network-update** command on interfaces on which NetWare (NetWare 3.1x or 4.0 or later) Servers are using internal network numbers.

Example

In the following example, corrupted network numbers on serial interface 0 are repaired:

```
interface serial 0
no ipx route-cache
ipx source-network-update
```

Related Command

ipx route-cache

ipx split-horizon eigrp

To configure split horizon, use the **ipx split-horizon eigrp** interface configuration command. To disable split horizon, use the **no** form of this command.

ipx split-horizon eigrp *autonomous-system-number*
no ipx split-horizon eigrp *autonomous-system-number*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

When split horizon is enabled, Enhanced IGRP update and query packets are not sent for destinations that have next hops on this interface. This reduces the number of Enhanced IGRP packets on the network.

Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communication among multiple routers, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and SMDS, situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.

Example

The following example disables split horizon on serial interface 0:

```
interface serial 0
no ipx split-horizon eigrp 200
```

ipx spx-idle-time

To set the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer, use the **ipx spx-idle-time** command. To disable the current delay time set by this command, use the **no** form of this command.

ipx spx-idle-time *delay-in-seconds*
no ipx spx-idle-time

Syntax Description

delay-in-seconds	The amount of time in seconds to wait before spoofing SPX keepalives after data transfer has stopped.

Default

60 seconds

Command Mode

Interface configuration

Usage Guidelines

This command sets the elapse time in seconds after which spoofing of keepalive packets occurs, following the end of data transfer; that is, after the acknowledgment and sequence numbers of the data being transferred have stopped increasing. By default, SPX keepalive packets are sent from servers to clients every 15 to 20 seconds.

If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins when SPX spoofing begins. For example, if the dialer idle time is three minutes, the elapse time before SPX spoofing begins is four minutes: three minutes of dialer idle time plus one minute of SPX spoofing idle time.

For this command to take effect, you must first use the **ipx spx-spoof** interface configuration command to enable SPX spoofing for the interface.

Example

The following example enables spoofing on serial interface 0 and sets the idle timer to 300 seconds:

```
interface serial 0
ipx spx-spoof
no ipx route-cache
ipx spx-idle-time 300
```

Related Commands

ipx spx-spoof
show ipx spx-spoof

ipx spx-spoof

To configure the router respond to a client or server's SPX keepalive packets on behalf of a remote system so that a dial-on-demand link will go idle when data has stopped being transferred, use the **ipx spx-spoof** interface configuration command. To disable spoofing, use the **no** form of this command.

ipx spx-spoof
no ipx spx-spoof

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

You can use the **ipx spx-spoof** command on any serial dialer or point-to-point interface. Fast switching and autonomous switching must be disabled on the interface; otherwise, SPX spoofing will not be permitted.

SPX keepalive packets are sent from servers to clients every 15-20 seconds after a client session has been idle for a certain period of time following the end of data transfer and after which only unsolicited acknowledgments are sent. The idle time may vary depending on parameters set by the client and server.

Due to acknowledgment packets, a session would never go idle on a DDR link. On pay-per-packet or byte networks, these keepalive packets can incur large phone connection charges for idle time on the customer. You can prevent these calls from being made by configuring the router to respond to the server's keepalive packets on a remote client's behalf. This is sometimes referred to as "spoofing the server."

You can use the **ipx spx-idle-time** command to set the elapse time in seconds after which spoofing of keepalive packets occurs, following the end of data transfer. If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins when SPX spoofing begins. For example, if the dialer idle time is 3 minutes, the elapse time before the line goes "idle-spoofing" is 4 minutes: 3 minutes of dialer idle time plus 1 minute of SPX spoofing idle time.

Example

The following example enables spoofing on serial interface 0:

```
interface serial 0
ipx spx-spoof
no ipx route-cache
```

Related Commands

ipx throughput
show ipx spx-spoof

ipx throughput

To configure the throughput, use the **ipx throughput** interface configuration command. To restore the default throughput, use the **no** form of this command.

ipx throughput *bits-per-second*
no ipx throughput *bits-per-second*

Syntax Description

bits-per-second	Throughput, in bits per second.

Default

No default throughput is defined.

Command Mode

Interface configuration

Usage Guidelines

The value you specify with the **ipx throughput** command overrides the value measured by IPXWAN when it starts. This value is also supplied to NLSP for use in its metric calculations.

Example

The following example changes the throughput to 1000000 bits per second:

```
ipx throughput 1000000
```

Related Command

ipx ipxwan

ipx triggered-rip-delay

To set the interpacket delay for triggered RIP updates sent on a single interface, use the **ipx triggered-rip-delay** interface configuration command. To return to the default delay, use the **no** form of this command.

ipx triggered-rip-delay *delay*
no ipx triggered-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet RIP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between routing update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Interface configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. A triggered routing update is one that the system sends in response to a “trigger” event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx triggered-rip-delay** command sets the interpacket delay for triggered routing updates sent on a single interface. The delay value set by this command overrides the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered routing updates sent on the interface.

If the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command is high, then we strongly recommend a low delay value for triggered routing updates so that updates triggered by special events are sent in a more timely manner than periodic routing updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for both periodic and triggered routing updates.

When you use the **no** form of the **ipx triggered-rip-delay** command, the system uses the global default delay set by the **ipx default-triggered-rip-delay** command for triggered RIP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the "Default" section.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on interface FDDI 0:

```
int FDDI 0
ipx triggered-rip-delay 55
```

Related Command

ipx default-output-rip-delay
ipx default-triggered-rip-delay
ipx output-rip-delay

ipx triggered-sap-delay

To set the interpacket delay for triggered SAP updates sent on a single interface, use the **ipx triggered-sap-delay** interface configuration command. To return to the default delay, use the **no** form of this command.

ipx triggered-sap-delay *delay*
no ipx triggered-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms. With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms. Novell recommends a delay of 55 ms.

Default

With Cisco IOS Release 10.0 and Release 10.2, the default delay is 0 ms (that is, no additional delay between update packets). With Cisco IOS Release 10.3 and Release 11.0, the default delay is 5 ms.

Command Mode

Interface configuration

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. A triggered SAP update is one that the system sends in response to a “trigger” event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx triggered-sap-delay** command sets the interpacket delay for triggered updates sent on a single interface. The delay value set by this command overrides the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered updates sent on the interface.

If the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command is high, then we strongly recommend a low delay value for triggered updates so that updates triggered by special events are sent in a more timely manner than periodic updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX servers.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for both periodic and triggered SAP updates.

When you use the **no** form of the **ipx triggered-sap-delay** command, the system uses the global default delay set by the **ipx default-triggered-sap-delay** command for triggered SAP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the "Default" section.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Example

The following example sets an interpacket delay of 55 ms for triggered SAP updates sent on interface FDDI 0:

```
int FDDI 0
ipx triggered-sap-delay 55
```

Related Commands

ipx default-output-sap-delay
ipx default-triggered-sap-delay
ipx output-sap-delay

ipx type-20-helpered

To forward IPX type 20 propagation packet broadcasts to specific network segments, use the **ipx type-20-helpered** interface configuration command. To disable this function, use the **no** form of this command.

ipx type-20-helpered
no ipx type-20-helpered

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

The **ipx type-20-helpered** command disables the input and output of type 20 propagation packets as done by the **ipx type-20-propagation** interface configuration command.

The **ipx type-20-propagation** command broadcasts type 20 packets to all nodes on the network and imposes a hop-count limit of eight routers for broadcasting these packets. These functions are in compliance with the Novell IPX router specification. In contrast, the **ipx type-20-helpered** command broadcasts type 20 packets to only those nodes indicated by the **ipx helper-address** interface configuration command and extends the hop-count limit to 16 routers.

Use of the **ipx type-20-helpered** command does not comply with the Novell IPX router specification.

Example

The following example forwards IPX type 20 propagation packet broadcasts to specific network segments:

```
interface ethernet 0
ipx network aa
ipx type-20-helpered
ipx helper-address bb.ffff.ffff.ffff
```

Related Commands

ipx helper-address
ipx type-20-propagation

ipx type-20-input-checks

To restrict the acceptance of IPX type 20 propagation packet broadcasts, use the **ipx type-20-input-checks** global configuration command. To remove these restrictions, use the **no** form of this command.

ipx type-20-input-checks
no type-20-input-checks

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

By default, the router is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-input-checks** command to impose additional restrictions on the acceptance of type 20 packets. Specifically, the router will accept type 20 propagation packets only on the single network that is the primary route back to the source network. Similar packets received via other networks will be dropped. This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Example

The following example imposes additional restrictions on incoming type 20 broadcasts:

```
ipx type-20-input-checks
```

Related Commands

ipx type-20-output-checks
ipx type-20-propagation

ipx type-20-output-checks

To restrict the forwarding of IPX type 20 propagation packet broadcasts, use the **ipx type-20-output-checks** global configuration command. To remove these restrictions, use the **no** form of this command.

ipx type-20-output-checks
no type-20-output-checks

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

By default, the router is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-output-checks** command to impose additional restrictions on outgoing type 20 packets. Specifically, the router will forward these packets only to networks that are not routes back to the source network. (The router uses the current routing table to determine routes.) This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Example

The following example imposes restrictions on outgoing type 20 broadcasts:

```
ipx type-20-output-checks
```

Related Commands

ipx type-20-input-checks
ipx type-20-propagation

ipx type-20-propagation

To forward IPX type 20 propagation packet broadcasts to other network segments, use the **ipx type-20-propagation** interface configuration command. To disable both the reception and forwarding of type 20 broadcasts on an interface, use the **no** form of this command.

ipx type-20-propagation
no ipx type-20-propagation

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Routers normally block all broadcast requests. To allow input and output of type 20 propagation packets on an interface, use the **ipx type-20-propagation** command. Note that type 20 packets are subject to loop detection and control as specified in the IPX router specification.

Additional input and output checks may be imposed by the **ipx type-20-input-checks** and **ipx type-20-output-checks** commands.

IPX type 20 propagation packet broadcasts are subject to any filtering defined by the **ipx helper-list** command.

Examples

The following example enables both the reception and forwarding of type 20 broadcasts on Ethernet interface 0:

```
interface ethernet 0
ipx type-20-propagation
```

The following example enables the reception and forwarding of type 20 broadcasts between networks 123 and 456, but does not enable reception and forwarding of these broadcasts to and from network 789.

```
interface ethernet 0
ipx network 123
ipx type-20-propagation
!
interface ethernet 1
ipx network 456
ipx type-20-propagation
!
interface ethernet 2
ipx network 789
```

Related Commands

ipx helper-list
ipx type-20-input-checks
ipx type-20-output-checks

ipx update-time

To adjust the IPX routing update timers, use the **ipx update-time** interface configuration command. To restore the default value, use the **no** form of this command.

ipx update-time *interval*
no ipx update-time

Syntax Description

interval	Interval, in seconds, at which IPX routing updates are sent. The default is 60 seconds. The minimum interval is 10 seconds.

Default

60 seconds

Command Mode

Interface configuration

Usage Guidelines

The **ipx update-time** command sets the routing update timer on a per-interface basis.

Routers exchange information about routes by sending broadcast messages when they are brought up and shut down, and periodically while they are running. The **ipx update-time** command lets you modify the periodic update interval. By default, this interval is 60 seconds (this default is defined by Novell).

You can set RIP timers only in a configuration in which all routers are our routers or in which the IPX routers allow configurable timers. The timers should be the same for all routers connected to the same cable segment.

The update value you choose affects the internal IPX timers as follows:

- IPX routes are marked invalid if no routing updates are heard within three times the value of *the update interval* (3 × *interval*) and are advertised with a metric of infinity.
- IPX routes are removed from the routing table if no routing updates are heard within four times the value of *the update interval* (4 × *interval*).
- If you define an update timer for more than one interface in a router, the granularity of the update timer is determined by the lowest value defined for one of the interfaces in the router. The router “wakes up” at this granularity interval and determines what updates need to be sent.

  The concept of granularity is best explained by an example. (This example is illustrated in the “Example” section following.) If you have two interfaces in the router and you set the update timer on one to 20 seconds and the second to 30 seconds, the router wakes up every 20 seconds to try to send routing updates. So at time 0:00:20, the router sends an update out the first interface only, and at time 0:00:40 it sends updates out the first and second interfaces. The router does not wake up at 0:00:30 to see if it needs to send an update out the second interface. This means that routing updates are sent out the second interface at N:NN:40 and N:NN:00. That is, the interval alternates between 40 seconds and 20 seconds; it is never 30 seconds. The interval on the first interface is always 20 seconds.

Example

The following example sets the update timers on two interfaces in the router. The update timer granularity would be 20 seconds because this is the lowest value specified.

```
interface serial 0
ipx update-time 40
interface ethernet 0
ipx update-time 20
```

Related Command

show ipx interface

ipx watchdog-spoof

To have the router respond to a server's watchdog packets on behalf of a remote client, use the **ipx watchdog-spoof** interface configuration command. To disable spoofing, use the **no** form of this command.

ipx watchdog-spoof
no ipx watchdog-spoof

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

You can use the **ipx watchdog-spoof** command only on a serial interface on which dial-on-demand routing (DDR) has been enabled. Also, fast switching and autonomous switching must be disabled on the interface.

IPX watchdog packets are keepalive packets that are sent from servers to clients after a client session has been idle for approximately 5 minutes. On a DDR link, this would mean that a call would be made every 5 minutes, regardless of whether there were data packets to send. You can prevent these calls from being made by configuring the router to respond to the server's watchdog packets on a remote client's behalf. This is sometimes referred to as "spoofing the server."

Example

The following example enables spoofing on serial interface 0:

```
interface serial 0
ipx watchdog-spoof
no ipx route-cache
```

Related Command

ipx route-cache
ipx spx-spoof

log-neighbor-changes

To enable the logging of changes in Enhanced IGRP neighbor adjacencies, use the **log-neighbor-change** command.

log-neighbor-changes
no log-neighbor-changes

Default

No adjacency changes are logged.

Command Mode

Router configuration

Usage Guidelines

Enable the logging of neighbor adjacency changes in order to monitor the stability of the routing system and to help detect problems. Log messages are of the form:

%DUAL-5-NBRCHANGE: IPX EIGRP *as-number*: Neighbor *address* (*interface*) is *state*: *reason*

as-number	Autonomous system number.
address	Neighbor address
State	Up or down
reason	Reason for change

Example

The following configuration will log neighbor changes for Enhanced IGRP process 209.

```
ipx router eigrp 209
log-neighbor-changes
```

Related Commands

ipx router

lsp-gen-interval

To set the minimum interval at which link-state packets (LSPs) are generated, use the **lsp-gen-interval** router configuration command. To restore the default interval, use the **no** form of this command.

lsp-gen-interval *seconds*
no lsp-gen-interval *seconds*

Syntax Description

seconds	Minimum interval, in seconds. It can be a number in the range 0 through 120. The default is 5 seconds.

Default

5 seconds

Command Mode

Router configuration

Usage Guidelines

The **lsp-gen-interval** command controls the rate at which LSPs are generated on a per-LSP basis. For instance, if a link is changing state at a high rate, the default value of the LSP generation interval limits the signaling of this change to once every 5 seconds. Because the generation of an LSP may cause all routers in the area to perform the SPF calculation, controlling this interval may have area-wide impact. Raising this interval can reduce the load on the network imposed by a rapidly changing link.

Example

The following example sets the minimum interval at which LSPs are generated to 10 seconds:

```
lsp-gen-interval 10
```

Related Commands

ipx router nlsp
spf-interval

lsp-mtu

To set the maximum size of a link-state packet (LSP) generated by the router, use the **lsp-mtu** router configuration command. To restore the default MTU size, use the **no** form of this command.

lsp-mtu *bytes*
no lsp-mtu *bytes*

Syntax Description

bytes	MTU size, in bytes. It can be a decimal number in the range 512 through 4096. The default is 512 bytes.

Default

512 bytes

Command Mode

Router configuration

Usage Guidelines

You can increase the LSP MTU if there is a very large amount of information generated by a single router, because each router is limited to approximately 250 LSPs. In practice, this should never be necessary.

The LSP MTU must never be larger than the smallest MTU of any link in the area. This is because LSPs are flooded throughout the area.

The **lsp-mtu** command limits the size of LSPs generated by this router only; the router can receive LSPs of any size up to the maximum.

Example

The following example sets the maximum LSP size to 1500 bytes:

```
lsp-mtu 1500
```

Related Command

ipx router nlsp

lsp-refresh-interval

To set the link-state packet (LSP) refresh interval, use the **lsp-refresh-interval** router configuration command. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds*
no lsp-refresh-interval *seconds*

Syntax Description

seconds	Refresh interval, in seconds. It can be a value in the range 1 through 50000 seconds. The default is 7200 seconds (2 hours).

Default

7200 seconds (2 hours)

Command Mode

Router configuration

Usage Guidelines

The refresh interval determines the rate at which a router periodically transmits the route topology information that it originates. This is done in order to keep the information from becoming too old. By default, the refresh interval is 2 hours.

LSPs must be periodically refreshed before their lifetime expires. The refresh interval must be less than the LSP lifetime specified with the **max-lsp-lifetime** router configuration command. Reducing the refresh interval reduces the amount of time that undetected link state database corruption can persist (this is an extremely unlikely event, however, because there are other safeguards against corruption) at the cost of increased link utilization. Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Example

The following example changes the LSP refresh interval to 10800 seconds (3 hours):

```
lsp-refresh-interval 10800
```

Related Commands

ipx router nlsp
max-lsp-lifetime

max-lsp-lifetime

To set the maximum time that link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** router configuration command. To restore the default time, use the **no** form of this command.

max-lsp-lifetime *seconds*
no max-lsp-lifetime *seconds*

Syntax Description

seconds	Lifetime of LSP, in seconds. It can be a number in the range 1 through 50000 seconds. The default is 7500 seconds.

Default

7500 seconds (2 hours, 5 minutes)

Command Mode

Router configuration

Usage Guidelines

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** router configuration command. The maximum LSP lifetime must be greater than the LSP refresh interval.

Example

The following example sets the maximum time that the LSP persists to 11000 seconds (just over 3 hours):

```
max-lsp-lifetime 11000
```

Related Commands

ipx router nlsp
lsp-refresh-interval

netbios access-list

To define an IPX NetBIOS FindName access list filter, use the **netbios access-list** interface configuration command. To remove a filter, use the **no** form of the command.

netbios access-list host *name* {**deny** | **permit**} *string*
no netbios access-list host *name* {**deny** | **permit**} *string*

netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*
no netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

Syntax Description

host — Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.

bytes — Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.

name — Name of the access list being defined. The name can be an alphanumeric string.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

string — Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument *string* can include the following wildcard characters:

- *—Match one or more characters. You can use this wildcard character only at the end of a string.
- ?—Match any single character.

offset — Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.

byte-pattern — Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument *byte-pattern* can include the following wildcard character:

- **—Match any digits for that byte.

Default

No filters are predefined.

Command Mode

Global configuration

Usage Guidelines

Keep the following points in mind when configuring IPX NetBIOS access control:

- Host (node) names are case sensitive.
- Host and byte access lists can have the same names. They are independent of each other.
- When filtering by node name for IPX NetBIOS, the names in the access lists are compared with the destination name field for IPX NetBIOS “find name” requests.
- When filtering by byte offset, note that these access filters can have a significant impact on the packets’ transmission rate across the bridge because each packet must be examined. You should use these access lists only when absolutely necessary.
- If a node name is not found in an access list, the default action is to deny access.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

To delete an IPX NetBIOS access list, specify the minimum number of keywords and arguments needed to delete the proper list. For example, to delete the entire list, use the following command:

no netbios access-list {**host** | **bytes**} *name*

To delete a single entry from the list, use the following command:

no netbios access-list host *name* {**permit** | **deny**} *string*

Examples

The following example defines the IPX NetBIOS access list *engineering*:

```
netbios access-list host engineering permit eng-ws1 eng-ws2 eng-ws3
```

The following example removes a single entry from the *engineering* access list:

```
netbios access-list host engineering deny eng-ws3
```

The following example removes the entire *engineering* NetBIOS access list:

```
no netbios access-list host engineering
```

Related Commands

ipx netbios input-access-filter
ipx netbios output-access-filter
show ipx interface

network

To enable Enhanced IGRP on the router, use the **network** IPX-router configuration command. To disable Enhanced IGRP on the router, use the **no** form of this command.

network {*network-number* | **all**}
no network {*network-number* | **all**}

Syntax Description

network-number	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

Default

Disabled

Command Mode

IPX-router configuration

Usage Guidelines

Use the **network** command to enable the routing protocol specified in the **ipx router** command on each network.

Example

The following commands disable RIP on network 10 and enable Enhanced IGRP on networks 10 and 20:

```
ipx router rip
no network 10
ipx router eigrp 12
network 10
network 20
```

Related Command

ipx router

ping (privileged)

To check host reachability and network connectivity, use the **ping** privileged EXEC command.

ping [**ipx**] [*network***.***node*]

Syntax Description

ipx	(Optional) Specifies the IPX protocol.
*network***.***node*	(Optional) Address of the system to ping.

Command Mode

Privileged EXEC

Usage Guidelines

The privileged **ping** (IPX echo) command provides a complete **ping** facility for users who have system privileges.

The **ping** command with **ipx ping-default** set to Cisco works only on our routers running Software Release 8.2 or later.

Novell IPX devices that support the echo function defined in version 1.0 of the NLSP specification will respond to this command if you answer **y** to the prompt Novell Standard Echo that is displayed when you use the ping command or if **ipx ping-default** is set to Novell. If you answer **n** to this prompt, Novell IPX devices will not respond.

To abort a **ping** session, type the escape sequence. By default, this is Ctrl-^ X. You enter this by simultaneously pressing the Ctrl, Shift, and 6 keys, letting go, and then pressing the X key.

Table 21-5 describes the test characters displayed in **ping** responses.

Table 21-5 Ping Test Characters

Character	Meaning
!	Each exclamation point indicates the receipt of a reply from the target address.
.	Each period indicates the network server timed out while waiting for a reply from the target address.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted the test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Sample Display

The following sample display shows input to and output from the **ping** command:

```
Router# ping

Protocol [ip]: ipx
Target IPX address: 211.0000.0c01.f4cf
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Verbose [n]:
Novell Standard Echo [n]:
Type escape sequence to abort.
Sending 5 100-byte IPX echoes to 211.0000.0c01.f4cf, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (0/5)
```

Related Commands

ipx ping-default
ping (user)

ping (user)

To check host reachability and network connectivity, use the **ping** user EXEC command.

ping ipx {*host* | *address*}

Syntax Description

ipx	Specifies the IPX protocol.
host	Host name of system to ping.
address	Address of system to ping.

Command Mode

EXEC

Usage Guidelines

The user-level **ping** (packet internet groper function) command provides a basic ping facility for users who do not have system privileges. This command is equivalent to the nonverbose form of the privileged **ping** command. It sends five 100-byte ping packets.

The **ping** command with **ipx ping-default** set to Cisco works only on our routers running Software Release 8.2 or later. Novell IPX devices will not respond to this command.

You cannot ping a router from itself except on AGS+ and Cisco 7000 systems.

If the system cannot map an address for a host name, it will return an "%Unrecognized host or address" error message.

To abort a **ping** session, type the escape sequence. By default, this is Ctrl-^ X. You enter this by simultaneously pressing the Ctrl, Shift, and 6 keys, letting go, and then pressing the X key.

Table 21-6 describes the test characters displayed in **ping** responses.

Table 21-6 Ping Test Characters

Character	Meaning
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted the test.
?	Unknown packet type.
&	Packet lifetime exceeded.

Sample Display

The following sample display shows input to and output from the user **ping** command:

```
Router> ping ipx 211.0000.0c01.f4cf

Type escape sequence to abort.
Sending 5, 100-byte Novell Echoes to 211.0000.0c01.f4cf, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Related Commands

ipx ping-default
ping (privileged)

redistribute

To redistribute from one routing domain into another, and vice versa, use the **redistribute** IPX-router configuration command. To disable this feature, use the **no** form of this command.

redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}
no redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

Syntax Description

connected	Specifies connected routes.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.
rip	Specifies the RIP protocol.
static	Specifies static routes.

Default

Redistribution is enabled between all routing domains except between separate Enhanced IGRP processes.

Redistribution of floating static routes is disabled.

Command Mode

IPX-router configuration

Usage Guidelines

Redistribution provides for routing information generated by one protocol to be advertised in another.

The only connected routes affected by this redistribute command are the routes not specified by the **network** command.

If you have enabled floating static routes by specifying the **floating** keyword in the **ipx route** global configuration command and you redistribute floating static routes into a dynamic IPX routing protocol, any nonhierarchical topology causes the floating static destination to be redistributed immediately via a dynamic protocol back to the originating router, causing a routing loop. This occurs because dynamic protocol information overrides floating static routes. For this reason, automatic redistribution of floating static routes is off by default. If you redistribute floating static routes, you should specify filters to eliminate routing loops.

Examples

In the following example, RIP routing information is not redistributed:

```
ipx router eigrp 222
no redistribute rip
```

In the following example, Enhanced IGRP routes from autonomous system 100 are redistributed into Enhanced IGRP autonomous system 300:

```
router eigrp 300
redistribute eigrp 100
```

Related Command

ipx route

show ipx accounting

To display the active accounting or checkpointed database, use the **show ipx accounting** EXEC command.

show ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Displays entries in the checkpointed database should be displayed.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx accounting** command:

```
Router# show ipx accounting

Source                  Destination                Packets           Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72            2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14             624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62            3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20            1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20            1470

Accounting data age is     6
```

Table 21-7 describes the fields shown in the display.

Table 21-7 Show IPX Accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets transmitted from the source address to the destination address.
Bytes	Number of bytes transmitted from the source address to the destination address.
Accounting data age is ...	Time since the accounting database has been cleared. It can be in one of the following formats: *mm*, *hh*:*mm*, *dd*:*hh*, and *x*w *y*d, where *m* is minutes, *h* is hours, *d* is days, and *w* is weeks.

Related Commands

clear ipx accounting
ipx accounting
ipx accounting-list
ipx accounting-threshold
ipx accounting-transits

show ipx cache

To display the contents of the IPX fast-switching cache, use the **show ipx cache** EXEC command.

show ipx cache

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx cache** command:

```
Router# show ipx cache

Novell routing cache version is 9
Destination          Interface              MAC Header
*1006A               Ethernet 0             00000C0062E600000C003EB0064
*14BB                Ethernet 1             00000C003E2A00000C003EB0064
```

Table 21-8 describes the fields shown in the display.

Table 21-8 Show IPX Cache Field Descriptions

Field	Description
Novell routing cache version is ...	Number identifying the version of the fast-switching cache table. It increments each time the table changes.
Destination	Destination network for this packet. Valid entries are marked by an asterisk (*).
Interface	Router interface through which this packet is transmitted.
MAC Header	Contents of this packet's MAC header.

Related Commands

clear ipx cache
ipx route-cache

show ipx eigrp interfaces

To display information about interfaces configured for Enhanced IGRP, use the **show ipx eigrp interfaces** EXEC command.

show ipx eigrp interfaces [*type number*] [*as-number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
as-number	(Optional) Autonomous System number.

Command Mode

EXEC

Usage Guidelines

Use the **show ipx eigrp interfaces** command to determine on which interfaces Enhanced IGRP is active and to find out information about Enhanced IGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which Enhanced IGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all Enhanced IGRP processes are displayed.

Sample Display

The following is sample output from the **show ipx eigrp interfaces** command:

```
Router> show ipx eigrp interfaces
IPX EIGRP interfaces for process 109

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

Table 21-9 describes the fields shown in the display.

Table 21-9 Show IPX Enhanced IGRP Interfaces Field Descriptions

Field	Description
process 109	Autonomous system number of the process.
Interface	Interface name.
Peers	Number of neighbors on the interface.
Xmit Queue	Count of unreliable and reliable packets queued for transmission.
Mean SRTT	Average round-trip time for all neighbors on the interface.

Field	Description
Pacing Time	Number of milliseconds to wait after transmitting unreliable and reliable packets.
Multicast Flow Timer	Number of milliseconds to wait for acknowledgment of a multicast packet by all neighbors before transmitting the next multicast packet.
Pending Routes	Number of routes still to be transmitted on this interface.

Related Commands

show ipx eigrp neighbors

show ipx eigrp neighbors

To display the neighbors discovered by Enhanced IGRP, use the **show ipx eigrp neighbors** EXEC command.

show ipx eigrp neighbors [**servers**] [*autonomous-system-number* | *interface*]

Syntax Description

servers	(Optional) Displays the server list advertised by each neighbor. This is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
autonomous-system-number	(Optional) Autonomous system number. It can be a decimal integer from 1 to 65535.
interface	(Optional) Interface type and number.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx eigrp neighbors** command:

```
Router# show ipx eigrp neighbors

IPX EIGRP Neighbors for process 200
H  Address                 Interface     Hold   Uptime   Q    Seq    SRTT  RTO
                                         (secs) (h:m:s)  Cnt  Num    (ms)  (ms)
6  90.0000.0c02.096e       Tunnel44444   13     0:30:57  0    21     9     20
5  80.0000.0c02.34f2       Fddi0         12     0:31:17  0    62     14    28
4  83.5500.2000.a83c       TokenRing2    13     0:32:36  0    626    16    32
3  98.0000.3040.a6b0       TokenRing1    12     0:32:37  0    43     9     20
2  80.0000.0c08.cbf9       Fddi0         12     0:32:37  0    624    19    38
1  85.aa00.0400.153c       Ethernet2     12     0:32:37  0    627    15    30
0  82.0000.0c03.4d4b       Hssi0         12     0:32:38  0    629    12    24
```

Table 21-10 explains the fields in the display.

Table 21-10 Show IPX EIGRP Neighbors Field Descriptions

Field	Description
process 200	Autonomous system number specified in the **ipx router** configuration command.
H	Handle. An arbitrary and unique number inside this router that identifies the neighbor.
Address	IPX address of the Enhanced IGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time, in seconds, that the router will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.

Field	Description
Uptime	Elapsed time, in hours, minutes, and seconds, since the local router first heard from this neighbor.
Q Cnt	Number of IPX Enhanced IGRP packets (Update, Query, and Reply) that the router is waiting to send.
Seq Num	Sequence number of the last Update, Query, or Reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds it takes for an IPX Enhanced IGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. This is the amount of time the router waits before retransmitting a packet from the retransmission queue to a neighbor.

show ipx eigrp topology

To display the Enhanced IGRP topology table, use the **show ipx eigrp topology** EXEC command.

show ipx eigrp topology [*network-number*]

Syntax Description

network-number	(Optional) IPX network number whose topology table entry to display.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx eigrp topology** command:

```
Router# show ipx eigrp topology

IPX EIGRP Topology Table for process 109
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 42, 1 successors, FD is 0
     via 160.0000.0c00.8ea9 (345088/319488), Ethernet0
P 160, 1 successor via Connected, Ethernet
     via 160.0000.0c00.8ea9 (307200/281600), Ethernet0
P 165, 1 successors, FD is 307200
     via Redistributed (287744/0)
     via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
P 164, 1 successors, flags: U, FD is 200
     via 160.0000.0c00.8ea9 (307200/281600), Ethernet1
     via 160.0000.0c01.2b71 (332800/307200), Ethernet1
P A112, 1 successors, FD is 0
     via Connected, Ethernet2
     via 160.0000.0c00.8ea9 (332800/307200), Ethernet0
P AAABBB, 1 successors, FD is 10003
     via Redistributed (287744/0),
     via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
A A112, 0 successors, 1 replies, state: 0, FD is 0
     via 160.0000.0c01.2b71 (307200/281600), Ethernet1
     via 160.0000.0c00.8ea9 (332800/307200), r, Ethernet1
```

Table 21-11 explains the fields in the output.

Table 21-11 Show IPX EIGRP Topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the Enhanced IGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No Enhanced IGRP computations are being performed for this destination.
A – Active	Enhanced IGRP computations are being performed for this destination.
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set after the router has sent a query and is waiting for a reply.
42, 160, and so on	Destination IPX network number.
successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
FD	Feasible distance. This value is used in the feasibility condition check. If the neighbor’s reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the router determines it has a feasible successor, it does not have to send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
via	IPX address of the peer who told the router about this destination. The first *n* of these entries, where *n* is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(345088/319488)	The first number is the Enhanced IGRP metric that represents the cost to the destination. The second number is the Enhanced IGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.

The following is sample output from the **show ipx eigrp topology** command when you specify an IPX network number:

```
Router# show ipx eigrp topology 160

IPX-EIGRP topology entry for 160
State is Passive, Query origin flag is 1, 1 Successor(s)
Routing Descriptor Blocks:
  Next hop is Connected (Ethernet0), from 0.0000.0000.0000
  Composite metric is (0/0), Send flag is 0x0, Route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
Next hop is 164.0000.0c00.8ea9 (Ethernet1), from 164.0000.0c00.8ea9
  Composite metric is (307200/281600), Send flag is 0x0, Route is External
  This is an ignored route
```

```
Vector metric:
  Minimum bandwidth is 10000 Kbit
  Total delay is 2000000 nanoseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 1
External data:
  Originating router is 0000.0c00.8ea9
  External protocol is RIP, metric is 1, delay 2
  Administrator tag is 0 (0x00000000)
  Flag is 0x00000000
```

Table 21-12 explains the fields in the output.

Table 21-12 Show IPX EIGRP Topology Field Descriptions for a Specified Network

Field	Description
160	IPX network number of the destination.
State is ...	State of this entry. It can be either Passive or Active. Passive means that no Enhanced IGRP computations are being performed for this destination, and Active means that they are being performed.
Query origin flag	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
Successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
Next hop is ...	Indicates how this destination was learned. It can be one of the following: • Connected—The destination is on a network directly connected to this router. • Redistributed—The destination was learned via RIP or another Enhanced IGRP process. • IPX host address—The destination was learned from that peer via this Enhanced IGRP process.
Ethernet0	Interface from which this information was learned.
from	Peer from whom the information was learned. For connected and redistributed routers, this is 0.0000.0000.0000. For information learned via Enhanced IGRP, this is the peer's address. Currently, for information learned via Enhanced IGRP, the peer's IPX address always matches the address in the "Next hop is" field.
Composite metric is	Enhanced IGRP composite metric. The first number is this router's metric to the destination, and the second is the peer's metric to the destination.
Send flag	Numeric representation of the "flags" field described in Table 21-10. It is 0 when nothing is being sent, 1 when an Update is being sent, 3 when a Query is being sent, and 4 when a Reply is being sent. Currently, 2 is not used.
Route is ...	Type of router. It can be either internal or external. Internal routes are those that originated in an Enhanced IGRP autonomous system, and external are routes that did not. Routes learned via RIP are always external.
This is an ignored route	Indicates that this path is being ignored because of filtering.
Vector metric:	This section describes the components of the Enhanced IGRP metric.
Minimum bandwidth	Minimum bandwidth of the network used to reach the next hop.
Total delay	Delay time to reach the next hop.
Reliability	Reliability value used to reach the next hop.

Field	Description
Load	Load value used to reach the next hop.
Minimum MTU	Minimum MTU size of the network used to reach the next hop.
Hop count	Number of hops to the next hop.
External data	This section describes the original protocol from which this route was redistributed. It appears only for external routes.
Originating router	Network address of the router that first distributed this route into Enhanced IGRP.
External protocol..metric..delay	External protocol from which this route was learned. The metric will match the external hop count displayed by the **show ipx route** command for this destination. The delay is the external delay.
Administrator tag	Not currently used.
Flag	Not currently used.

Related Command

show ipx route

show ipx interface

To display the status of the IPX interfaces configured in the router and the parameters configured on each interface, use the **show ipx interface** EXEC command.

show ipx interface [*type number*]

Syntax Description

type (Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.

number (Optional) Interface number.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx interface** command:

```
Router# show ipx interface ethernet 1

Ethernet1 is up, line protocol is up
  IPX address is C03.0000.0c05.6030, NOVELL-ETHER [up] line-up, RIPPQ: 0, SAPPQ : 0
  Delay of this Novell network, in ticks is 1
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Outgoing access list is not set
  IPX Helper access list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  SAP GNS output filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Update time is 60 seconds
  IPX accounting is enabled
  IPX fast switching is configured (enabled)
  IPX SSE switching is disabled
```

The following is sample output from the **show ipx interface** command when NLSP is enabled on the router:

```
Router# show ipx interface ethernet 1

Ethernet0 is up, line protocol is up
  IPX address is E001.0000.0c02.8cf9, SAP [up] line-up, RIPPQ: 0, SAPPQ : 0
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
```

```
     Outgoing access list is not set
     IPX Helper access list is not set
     SAP Input filter list is not set
     SAP Output filter list is not set
     SAP Router filter list is not set
     SAP GNS output filter list is not set
     Input filter list is not set
     Output filter list is not set
     Router filter list is not set
     Netbios Input host access list is not set
     Netbios Input bytes access list is not set
     Netbios Output host access list is not set
     Netbios Output bytes access list is not set
     Update time is 60 seconds
     IPX accounting is enabled
     IPX fast switching is configured (enabled)
     IPX SSE switching is disabled
     IPX NLSP is running on primary network E001
     RIP compatibility mode is AUTO (OFF)
     SAP compatibility mode is AUTO (OFF)
     Level 1 Hello interval 20 sec
     Level 1 Designated Router Hello interval 10 sec
     Level 1 CSNP interval 30 sec, LSP retransmit interval 5 sec
     Level 1 adjacency count is 1
     Level 1 circuit ID is 0000.0C02.8CF9.02
```

Table 21-13 describes the fields shown in the display.

Table 21-13 Show IPX Interface Field Descriptions

Field	Description
Ethernet1 is ..., line protocol is ...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
IPX address is ...	Network and node address of the local router interface, followed by the type of encapsulation configured on the interface and the interface's status. Refer to the **ipx network** command for a list of possible values.
NOVELL-ETHER	Type of encapsulation being used on the interface, if any.
[up] line-up	Indicates whether IPX routing is enabled or disabled on the interface. "line-up" indicates that IPX routing has been enabled with the **ipx routing** command. "line-down" indicates that it is not enabled. The word in square brackets provides more detail about the status of IPX routing when it is in the process of being enabled or disabled.
RIPPQ:	Number of packets in the RIP queue.
SAPPQ:	Number of packets in the SAP queue.
Secondary address is ...	Address of a secondary network configured on this interface, if any, followed by the type of encapsulation configured on the interface and the interface's status. Refer to the **ipx routing** command for a list of possible values. This line is displayed only if you have configured a secondary address with the **ipx routing** command.
Delay of this IPX network, in ticks, ...	Value of the ticks field (configured with the **ipx delay** command).
throughput	Throughput of the interface (configured with the **ipx spx-idle-time** interface configuration command).

Field	Description
link delay	Link delay of the interface (configured with the **ipx link-delay** interface configuration command).
IPXWAN processing...	Indicates whether IPXWAN processing has been enabled on this interface with the **ipx ipxwan** command.
IPX SAP update interval	Indicates the frequency of outgoing SAP updates (configured with the **ipx sap-interval** command).
IPX type 20 propagation packet forwarding...	Indicates whether forwarding of IPX type 20 propagation packets (used by NetBIOS) is enabled or disabled on this interface, as configured with the **ipx type-20-propagation** command.
Outgoing access list	Indicates whether an access list has been enabled with the **ipx access-group** command.
IPX Helper access list	Number of the broadcast helper list applied to the interface with the **ipx helper-list** command.
SAP Input filter list	Number of the input SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Output filter list	Number of the output SAP filter applied to the interface with the **ipx output-sap-filter** command.
SAP Router filter list	Number of the router SAP filter applied to the interface with the **ipx router-sap-filter** command.
SAP GNS output filter	Number of the Get Nearest Server (GNS) response filter applied to the interface with the **ipx output-gns-filter** command.
Input filter	Number of the input filter applied to the interface with the **ipx input-network-filter** command.
Output filter	Number of the output filter applied to the interface with the **ipx output-network-filter** command.
Router filter	Number of the router entry filter applied to the interface with the **ipx router-filter** command.
Netbios Input host access list	Name of the IPX NetBIOS input host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Input bytes access list	Name of the IPX NetBIOS input bytes filter applied to the interface with the **ipx netbios input-access-filter bytes** command.
Netbios Output host access list	Name of the IPX NetBIOS output host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Output bytes access list	Name of the IPX NetBIOS output bytes filter applied to the interface with the **ipx netbios input-access-filter bytes** command.
Update time	How often the router sends RIP updates, as configured with the **ipx update-time** command.
Watchdog spoofing ...	Indicates whether watchdog spoofing is enabled of disabled for this interface, as configured with the **ipx watchdog-spoof** command. This information is displayed only on serial interfaces.
IPX accounting	Indicates whether IPX accounting has been enabled with the **ipx accounting** command.
IPX Fast switching IPX Autonomous switching	Indicates whether IPX fast switching is enabled (default) or disabled for this interface, as configured with **ipx route-cache** command. (If IPX autonomous switching is enabled, it is configured with the **ipx route-cache cbus** command.)

Field	Description
IPX SSE switching	Indicates whether IPX SSE switching is enabled for this interface, as configured with the **ipx route-cache sse** command.
IPX NLSP is running on primary network E001	Indicates that NLSP is running and the number of the primary IPX network on which it is running.
RIP compatibility mode	State of RIP compatibility (configured by the **ipx nlsp rip** interface configuration command).
SAP compatibility mode	State of SAP compatibility (configured by the **ipx nlsp sap** interface configuration command).
Level 1 Hello interval	Interval between transmission of hello packets for nondesignated routers (configured by the **ipx nlsp hello-interval** interface configuration command).
Level 1 Designated Router Hello interval	Interval between transmission of hello packets for designated routers (configured by the **ipx nlsp hello-interval** interface configuration command).
Level 1 CSNP interval	CSNP interval (as configured by the **ipx nlsp csnp-interval** interface configuration command).
LSP retransmit interval	LSP retransmisison interval (as configured by the **ipx nlsp retransmit-interval** interface configuration command).
Level 1 adjacency count	Number of Level 1 adjacencies in the adjacency database.
Level 1 circuit ID	System ID and pseudonode number of the designated router. In this example, 0000.0C02.8CF9 is the system ID, and 02 is the pseudonode number.

show ipx nlsp database

To display the entries in the link-state packet (LSP) database, use the **show ipx nlsp database** EXEC command.

show ipx nlsp database [*lspid*] [**detail**]

Syntax Description

lspid

(Optional) Link-state protocol ID (LSPID). You must specify this in the format *xxxx.xxxx.xxxx.yy-zz*. The components of this argument have the following meaning:

- *xxxx.xxxx.xxxx* is the system identifier.
- *yy* is the pseudo identifier.
- *zz* is the LSP number.

detail

(Optional) Displays the contents of the LSP database entries. If you omit this keyword, only a summary display is shown.

Command Mode

EXEC

Usage Guidelines

If you omit all options, a summary display is shown.

Sample Displays

The following is sample output from the **show ipx nlsp database** command:

```
Router# show ipx nlsp database detail

LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.3097.00-00* 0x00000042   0xC512        699           0/0/0
0000.0C00.3097.06-00* 0x00000027   0x0C27        698           0/0/0
0000.0C02.7471.00-00  0x0000003A   0x4A0F        702           0/0/0
0000.0C02.7471.08-00  0x00000027   0x0AF0        702           0/0/0
0000.0C02.7471.0A-00  0x00000027   0xC589        702           0/0/0
0000.0C02.747D.00-00  0x0000002E   0xC489        715           0/0/0
0000.0C02.747D.06-00  0x00000027   0xEEFE        716           0/0/0
0000.0C02.747D.0A-00  0x00000027   0xFE38        716           0/0/0
0000.0C02.74AB.00-00  0x00000035   0xE4AF        1059          0/0/0
0000.0C02.74AB.0A-00  0x00000027   0x34A4        705           0/0/0
0000.0C06.FBEE.00-00  0x00000038   0x3838        1056          0/0/0
0000.0C06.FBEE.0D-00  0x0000002C   0xD248        1056          0/0/0
0000.0C06.FBEE.0E-00  0x0000002D   0x7DD2        1056          0/0/0
0000.0C06.FBEE.17-00  0x00000029   0x32FB        1056          0/0/0

0000.0C00.AECC.00-00* 0x000000B6   0x62A8        7497          0/0/0
  IPX Area Address: 00000000 00000000
  IPX Mgmt Info 87.0000.0000.0001  Ver 1  Name oscar
  Metric: 45 Lnk 0000.0C00.AECC.06  MTU 1500  Dly 8000  Thru 64K  PPP
  Metric: 20 Lnk 0000.0C00.AECC.02  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
  Metric: 20 Lnk 0000.0C01.EF90.0C  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
```

```
0000.0C00.AECC.02-00* 0x00000002   0xDA74        3118          0/0/0
  IPX Mgmt Info E0.0000.0c00.aecc  Ver 1  Name Ethernet0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  802.3 Raw
0000.0C00.AECC.06-00* 0x00000002   0x5DB9        7494          0/0/0
  IPX Mgmt Info 0.0000.0000.0000  Ver 1  Name Serial0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  PPP
  Metric: 1  IPX Ext D001  Ticks 0
  Metric: 1  IPX SVC Second-floor-printer  D001.0000.0000.0001  Sock 1  Type 4
```

Table 21-14 explains the fields in the display.

Table 21-14 Show IPX NLSP Database Field Descriptions

Field	Description
LSPID	System ID (network number), pseudonode circuit identifier, and fragment number.
LSP Seq Num	Sequence number of this LSP.
LSP Checksum	Checksum of this LSP.
LSP Holdtime	Time until this LSP expires, in seconds.
ATT/P/OL	Indicates which of three bits are set. A “1” means the bit is set, and a “0” means it is not set. ATT is the L2-attached bit. OL is the overload bit. P is the partition repair bit. This bit is not used in NLSP.
IPX Area Address:	Area address of the router advertising the LSP.
IPX Mgmt Info	Management information. For nonpseudonode LSPs, the internal network number is advertised in this field. For pseudonode LSPs, the network number of the associated interface is advertised.
Ver	NLSP version running on the advertising router.
Name	For nonpseudonode LSPs, the name of the router. For pseudonode LSPs, the name (or description, if configured) of the associated interface.
Link Information	Information about the link.
Metric:	NLSP metric (cost) for the link. Links from a pseudonode to real nodes have a cost of 0 so that this link cost is not counted twice.
Lnk	System ID of the adjacent node.
MTU	MTU of the link in bytes. For pseudonode LSPs, the value in this field is always 0.
Dly	Delay of the link in microseconds. For pseudonode LSPs, the value in this field is always 0.
Thru	Throughput of the link in bits per second. For pseudonode LSPs, the value in this field is always 0.
802.3 Raw, Generic LAN	Link media type.
External (RIP) Networks	Information about an external (RIP) network.
Metric:	Received RIP hop count.
IPX Ext	IPX network number.
Ticks	Received RIP tick count.

Field	Description
SAP Services	Information about SAP services.
Metric:	Received SAP hop count.
IPX SVC	Name of the IPX service.
D001.000.0000.0001	IPX address of the server advertising this service.
Sock	Socket number of the service.
Type	Type of service.

show ipx nlsp neighbors

To display the router’s NLSP neighbors and their states, use the **show ipx nlsp neighbors** EXEC command.

show ipx nlsp neighbors [*interface*] [**detail**]

Syntax Description

interface	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about the neighbor. If you omit this keyword, only a summary display is shown.

Command Mode

EXEC

Usage Guidelines

If you omit the keyword **detail**, a summary display is shown.

Sample Displays

The following is sample output from the **show ipx nlsp neighbors** command:

```
Router# show ipx nlsp neighbors detail

System Id       Interface   State  Holdtime  Priority  Circuit Id
0000.0C01.EF90  Ethernet1   Up     25        64        0000.0C01.EF90.0C
  IPX Address: E1.0000.0c01.ef91
  IPX Areas:  00000000/00000000
  Uptime: 2:59:11
```

Table 21-15 explains the fields in the display.

Table 21-15 Show IPX NLSP Neighbors Field Descriptions

Field	Description
System Id	System ID of the neighbor.
Interface	Interface on which the neighbor was discovered.
State	State of the neighbor adjacency.
Holdtime	Remaining time before the neighbor is assumed to have failed.
Priority	Designated router election priority.
Circuit Id	Neighbor’s view of the identity of the designated router.
IPX Address:	IPX address on this network of the neighbor.
IPX Areas:	IPX area addresses configured on the neighbor.
Uptime:	Time since the neighbor was discovered.

show ipx route

To display the contents of the IPX routing table, use the **show ipx route** user EXEC command.

show ipx route [*network*] [**default**] [**detailed**]

Syntax Description

network	(Optional) Number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeroes in the network number. For example, for the network number 000000AA, you can enter AA.
default	(Optional) Displays the default route. This is equivalent to specifying a value of FFFFFFFE for the argument *network*.
detailed	(Optional) Displays detailed route information.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx route** command:

```
Router# show ipx route

Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, s - seconds, u - uses

7 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D40 is the internal network
C        100 (NOVELL-ETHER), Et1
C       7000 (TUNNEL),        Tu1
S        200 via     7000.0000.0c05.6023,        Tu1
R        300 [02/01] via      100.0260.8c8d.e748,   19s, Et1
S       2008 via     7000.0000.0c05.6023,        Tu1
R     CC0001 [02/01] via      100.0260.8c8d.e748,   19s, Et1
```

Table 21-16 describes the fields shown in the display.

Table 21-16 Show IPX Route Field Descriptions

Field	Description
Codes	Codes defining how the route was learned.
L	Internal network number.
C	Directly connected primary network.

Field	Description
c	Directly connected secondary network
R	Route learned from a RIP update.
E	Route learned from an Enhanced IGRP (EIGRP) update.
S	Statically defined route via the **ipx route** command.
8 Total IPX routes	Number of routes in the IPX routing table.
No parallel paths allowed	Maximum number of parallel paths for which the router has been configured with the **ipx maximum-paths** command.
Novell routing algorithm variant in use	Indicates whether the router is using the IPX-compliant routing algorithms (default).
Net 1	Network to which the route goes.
[3/2]	Delay/Metric. Delay is the number of IBM clock ticks (each tick is 1/18 seconds) reported to the destination network. Metric is the number of hops reported to the same network. Delay is used as the primary routing metric, and the metric (hop count) is used as a tie breaker.
via *network.node*	Address of a router that is the next hop to the remote network.
age	Amount of time, in hours, minutes, and seconds, that has elapsed since information about this network was last received.
uses	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
Ethernet0	Interface through which packets to the remote network will be sent.
(NOVELL-ETHER) (HDLC) (SAP) (SNAP)	Encapsulation (frame) type. This is shown only for directly connected networks.
is directly connected	Indicates that the network is directly connected to the router.

The following is sample output from the **show ipx route detailed** command:

```
Router# show ipx route detailed

Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, s - seconds, u - uses

9 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D35 is the internal network
C       E001 (SAP),           Et0
C      D35E2 (NOVELL-ETHER),  Et2
R        D34 [02/01]
          -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
N        D36 [20][02/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                  10000000:1000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
NX       D40 [20][03/02][02/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
R      D34E1 [01/01]
          -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
```

```
NX     D40E1 [20][02/02][01/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     3u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
N     D36E02 [20][01/01]
          -- via    D35E2.0000.0c02.8cfc, 705s,     2u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
```

Table 21-17 explains the additional fields shown in the display.

Table 21-17 Show IPX Route Detailed Field Descriptions

Field	Description
1u	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
10000000	(NLSP only) Throughput (end to end).
3000	(NLSP only) Link delay (end to end).
1500	(NLSP only) MTU (end to end).
0000.0c02.8cfb	(NLSP only) System ID of the next-hop router.
0000.0c02.8cfc	(NLSP only) MAC address of the next-hop router.
6	(NLSP only) Local circuit ID.

Related Commands

clear ipx route
ipx maximum-paths
ipx nlsp metric
ipx route

show ipx servers

To list the IPX servers discovered through SAP advertisements, use the **show ipx servers** EXEC command.

show ipx servers [**unsorted** | [**sorted** [**name** | **net** | **type**]]

Syntax Description

unsorted	(Optional) Does not sort entries when displaying IPX servers.
sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
net	(Optional) Displays the IPX servers numerically by network number.
type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.

Default

IPX servers are displayed numerically by SAP service type.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx servers** command when NLSP is enabled:

```
Router# show ipx servers

Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP, H - Holddown, + = detail
9 Total IPX Servers

Table ordering is based on routing and server info

Type Name                      Net  Address          Port Route Hops Itf
N+   4 MERLIN1-VIA-E03         E03E03.0002.0004.0006:0451 4/03  4    Et0
N+   4 merlin                  E03E03.0002.0004.0006:0451 4/03  3    Et0
N+   4 merlin 123456789012345  E03E03.0002.0004.0006:0451 4/03  3    Et0
S    4 WIZARD1--VIA-E0         E0.0002.0004.0006:0451     none  2
N+   4 dtp-15-AB               E002.0002.0004.0006:0451   none  4    Et0
N+   4 dtp-15-ABC              E002.0002.0004.0006:0451   none  4    Et0
N+   4 dtp-15-ABCD             E002.0002.0004.0006:0451   none  4    Et0
N+   4 merlin                  E03E03.0002.0004.0006:0451 4/03  3    Et0
N+   4 dtp-15-ABC              E002.0002.0004.0006:0451   none  4    Et0
```

Table 21-18 describes the fields shown in the display.

Table 21-18 Show IPX Servers Field Descriptions

Field	Description
Codes	Codes defining how the route was learned.
S	Statically defined route via the **ipx route** command.
P	Route learned via a SAP update.
E	Route learned via Enhanced IGRP.
N	Route learned via NLSP.
H	Indicates that the entry is in holddown mode and is not reachable.
+	Indicates that multiple paths to the server exist. Use the **show ipx servers detailed** EXEC command to display more detailed information about the paths.
Type	Indicates how route was learned.
Name	Name of server.
Net	Network on which server is located.
Address	Network address of server.
Port	Source socket number.
Route	Ticks/hops (from the routing table).
Hops	Hops (from the SAP protocol).
Itf	Interface through which to reach server.

Related Commands

ipx sap
show ipx servers

show ipx spx-spoof

To display the table of SPX connections through interfaces for which SPX spoofing is enabled, use the **show ipx spx-spoof** EXEC command.

show ipx spx-spoof

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx spx-spoof** command:

```
Router> show ipx spx-spoof

Local SPX Network.Host:sock Cid  Remote SPX Network.Host:sock Cid   Seq  Ack  Idle
CC0001.0000.0000.0001:8104  0D08 200.0260.8c8d.e7c6:4017      7204  09   0021 120
CC0001.0000.0000.0001:8104  0C08 200.0260.8c8d.c558:4016      7304  07   0025 120
```

Table 21-19 describes the fields shown in the display.

Table 21-19 Show SPX Spoofing Field Descriptions

Field	Description
Local SPX Network.Host:sock	Address of the local end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the local end of the SPX connection.
Remote SPX Network.Host:sock	Address of the remote end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the remote end of the SPX connection.
Seq	Sequence number of the last data packet transferred.
Ack	Number of the last solicited acknowledge received.
Idle	Amount of time elapsed since the last data packet was transferred.

Related Commands

ipx spx-idle-time
ipx spx-spoof

show ipx traffic

To display information about the number and type of IPX packets transmitted and received by the router, use the **show ipx traffic** user EXEC command.

show ipx traffic

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx traffic** command:

```
Router> show ipx traffic

Rcvd:   644 total, 1705 format errors, 0 checksum errors, 0 bad hop count,
        0 packets pitched, 644 local destination, 0 multicast
Bcast:  589 received, 324 sent
Sent:   380 generated, 0 forwarded
        0 encapsulation failed, 4 no route
SAP:    1 SAP requests, 1 SAP replies
        61 SAP advertisements received, 120 sent
        0 SAP flash updates sent, 0 SAP poison sent
        0 SAP format errors
RIP:    0 RIP format errors
Echo:   Rcvd 55 requests, 0 replies
        Sent 0 requests, 55 replies
        0 unknown, 0 SAPs throttled, freed NDB len 0
Watchdog:
        0 packets received, 0 replies spoofed
Queue lengths: IPX input: 0, SAP 0, RIP 0, GNS 0
               Total length for SAP throttling purposes: 0/(no preset limit)
EIGRP:  Total received 0, sent 0
        Updates received 0, sent 0
        Queries received 0, sent 0
        Replies received 0, sent 0
        SAPs received 0, sent 0
```

The following is sample output from the **show ipx traffic** command when NLSP is enabled:

```
Router> show ipx traffic

Rcvd:   644 total, 1705 format errors, 0 checksum errors, 0 bad hop count,
        0 packets pitched, 644 local destination, 0 multicast
Bcast:  589 received, 324 sent
Sent:   380 generated, 0 forwarded
        0 encapsulation failed, 4 no route
SAP:    1 SAP requests, 1 SAP replies
        61 SAP advertisements received, 120 sent
        0 SAP flash updates sent, 0 SAP poison sent
        0 SAP format errors
RIP:    0 RIP format errors
Echo:   Rcvd 55 requests, 0 replies
        Sent 0 requests, 55 replies
        0 unknown, 0 SAPs throttled, freed NDB len 0
```

```
Watchdog:
        0 packets received, 0 replies spoofed
Queue lengths: IPX input: 0, SAP 0, RIP 0, GNS 0
               Total length for SAP throttling purposes: 0/(no preset limit)
NLSP: Level-1 Hellos received 7310, sent 14564
      PTP Hello received 3662, send 3672
      Level-1 LSPs received 949, send 769
      Level-1 CSNPs received 2, sent 4872
      Level-1 PSNPs received 118, sent 124
      Level-1 DR Elections: 10
      Level-1 SPF Calculations: 35
      Level-1 Partial Route Calculations: 42
```

Table 21-20 describes the fields that might possibly be shown in the display.

Table 21-20 Show IPX Traffic Field Descriptions

Field	Description
Rcvd:	Description of the packets the router has received.
644 total	Total number of packets the router has received.
1705 format errors	Number of bad packets discarded (for example, packets with a corrupted header).
0 checksum errors	Number of packets containing a checksum error. This number should always be 0, because IPX does not use a checksum.
0 bad hop count	Number of packets discarded because their hop count exceeded 16 (that is, the packets timed out).
0 packets pitched	Number of times the router received its own broadcast packet.
644 local destination	Number of packets sent to the local broadcast address or specifically to the router.
0 multicast	Number of packets received that were addressed to multiple destinations.
Bcast:	Description of the broadcast packets the router has received and sent.
589 received	Number of broadcast packets received.
324 sent	Number of broadcast packets sent. It includes broadcast packets the router is either forwarding or has generated.
Sent:	Description of those packets that the router generated and then sent, and also those the router has received and then routed to other destinations.
380 generated	Number of packets the router transmitted that it generated itself.
0 forwarded	Number of packets the router transmitted that it forwarded from other sources.
0 encapsulation failed	Number of packets the router was unable to encapsulate.
4 no route	Number of times the router could not locate a route to the destination in the routing table.
SAP:	Description of the SAP packets the router has sent and received.
1 SAP requests	Number of SAP requests the router has received.
1 SAP replies	Number of SAP replies the router has sent in response to SAP requests.
61 SAP advertisements received	Number of SAP advertisements the router has received from another router.
120 sent	Number of SAP advertisements the router has generated and then sent.
0 SAP flash updates sent	Number of SAP advertisements the router has generated and then sent as a result of a change in its routing table.

Field	Description
0 SAP poison sent	Number of times the router has generated an update indicating that a service is no longer reachable.
0 SAP format errors	Number of SAP advertisements that were incorrectly formatted.
RIP:	Description of the RIP packets the router has sent and received.
0 RIP format errors	Number of RIP packets that were incorrectly formatted.
freed NDB length	Number of Network Descriptor Blocks (NDBs) that have been removed from the network but still need to be removed from the router's routing table.
Watchdog:	Description of the watchdog packets the router has handled.
0 packets received	Number of watchdog packets the router has received from IPX servers on the local network.
0 replies spoofed	Number of times the router has responded to a watchdog packet on behalf of the remote client.
Echo:	Description of the ping replies and requests the router has sent and received.
Rcvd 55 requests, 0 replies	Number of ping requests and replies received by the router.
Sent 0 requests, 55 replies	Number of ping requests and replies sent by the router.
0 unknown	Number of incomprehensible ping packets received by the router.
0 SAPs throttled	Number of ping packets discarded because they exceeded buffer capacity.
Queue lengths	Description of outgoing packets currently in buffers that are waiting to be processed.
IPX input	Number of incoming packets waiting to be processed.
SAP	Number of outgoing SAP packets waiting to be processed.
RIP	Number of outgoing RIP packets waiting to be processed.
GNS	Number of outgoing GNS packets waiting to be processed.
Total length for SAP throttling purposes	Maximum number of outgoing SAP packets allowed in the buffer. Any packets received beyond this number are discarded.
EIGRP:	Description of the Enhanced IGRP packets the router has sent and received.
Updates	Number of Enhanced IGRP updates the router has sent and received.
Queries	Number of Enhanced IGRP queries the router has sent and received.
Replies	Number of Enhanced IGRP replies the router has sent and received.
SAPs	Number of SAP packets the router has sent to and received from Enhanced IGRP neighbors.
unknown counter	Number of packets the router was unable to forward, for example, because of a misconfigured helper address or because no route was available.
NLSP:	Description of the NLSP packets the router has sent and received.
Level-1 Hellos	Number of LAN hello packets the router has sent and received.
PTP Hello	Number of point-to-point packets the router has sent and received.
Level-1 LSPs	Number of link-state packets (LSPs) the router has sent and received.
Level-1 CSNPs	Number of complete sequence number PDU (CSNP) packets the router has sent and received.
Level-1 PSNPs	Number of partial sequence number PDU (PSNP) packets the router has sent and received.
Level-1 DR Elections	Number of times the router has calculated its designated router election priority.

Field	Description
Level-1 SPF Calculations	Number of times the router has perform the shortest path first (SPF) calculation.
Level-1 Partial Route Calculations	Number of times the router has recalculated routes without running SPF.

show sse summary

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** EXEC command.

show sse summary

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show sse summary** command:

```
Router# show sse summary

SSE utilization statistics

               Program words  Rewrite bytes  Internal nodes  Depth
Overhead                 499              1               8
IP                         0              0               0      0
IPX                        0              0               0      0
SRB                        0              0               0      0
CLNP                       0              0               0      0
IP access lists            0              0               0
Total used               499              1               8
Total free             65037         262143
Total available        65536         262144

Free program memory
  [499..65535]
Free rewrite memory
  [1..262143]

Internals
  75032 internal nodes allocated, 75024 freed
  SSE manager process enabled, microcode enabled, 0 hangs
  Longest cache computation 4ms, longest quantum 160ms at 0x53AC8
```

spf-interval

To control how often the router performs the shortest path first (SPF) calculation, use the **spf-interval** router configuration command. To restore the default interval, use the **no** form of this command.

spf-interval *seconds*
no spf-interval *seconds*

Syntax Description

seconds	Minimum amount of time between shortest path first (SPF) calculations, in seconds. It can be a number in the range 1 through 120. The default is 5 seconds.

Default

5 seconds

Command Mode

Router configuration

Usage Guidelines

SPF calculations are performed only when the router topology changes. They are not performed when external routes change.

The **spf-interval** command controls how often the router can perform the shortest path first (SPF) calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows down the rate of convergence.

Example

The following example sets the SPF calculation interval to 30 seconds:

```
spf-interval 30
```

Related Commands

ipx router nlsp
lsp-gen-interval