CHAPTER 18

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 router connects Ethernet, Token Ring, and FDDI networks, either directly or through high-speed serial lines (56 kbps to T1 speeds), X.25, or Frame Relay. The Cisco X.25 and T1 support currently is not compatible with Novell. This means that our routers must be used on both ends of T1 and X.25 circuits.

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 of 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 (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 zeros in the network number. For example, for the network number 000000AA, you can enter just 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 zeros in the network number. For example, for the network number 000000AA, you can enter just 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

None

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 1.0000.0c00.1111 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 †

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-network-mask*.]*source-node-mask*]] *source-socket*
[*destination-network* [.*destination-node*
[[*destination-network-mask*.]*destination-node-mask*] *destination-socket*]]
no access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*[.*source-node*
[[*source-network-mask*.]*source-node-mask*]] *source-socket*
[*destination-network* [.*destination-node*
[[*destination-network-mask*.]*destination-node-mask*] *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 1-1 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 zeros in the network number. For example, for the network number 000000AA, you can enter just 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*. The entire mask must contain no spaces; that is, you must specify it as *source-network-mask.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 1-2 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 zeros in the network number. For example, for the network number 000000AA, you can enter just 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*. The entire mask must contain no spaces; that is, you must specify it as *destination-network-mask*.*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 1-2 in the "Usage Guidelines" section lists some IPX socket numbers.

Default

None

Command Mode

Global configuration

Usage Guidelines

Extended IPX access lists filter on protocol type. 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.

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

Table 1-1 Some IPX Protocol Numbers

IPX Protocol Number (Decimal)	Protocol (Packet Type)
0	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 1-2 Some IPX Socket Numbers

IPX Socket Number (Hexadecimal)	Socket
0	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	Well-known sockets as assigned by Novell

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 0 –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 1001 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 20 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.node-mask*] [*service-type* [*server-name*]]
no access-list *access-list-number* {**deny** | **permit**} *network*[**.***node*] [*network.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 zeros in the network number. For example, for the network number 000000AA, you can enter just 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.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 1-3 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

None

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 1-3 lists some sample IPX SAP types. For more information about SAP types, contact Novell.

Table 1-3 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
0	All SAP services; IPX defines server type 0 to be an unknown service, which means that you cannot define an access list to permit or deny unknown services
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
111	Test server
166	NetWare management
26A	NetWare management
FFFF	Wildcard (any SAP service)

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 †

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

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 route

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

clear ipx route [*network* | ***]

Syntax Description

network	(Optional.) 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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.
*	(Optional.) Deletes all routes in the routing table

Command Mode

EXEC

Example

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

```
clear ipx route 3
```

Related Command

show ipx route

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

None

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

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 *number*
no ipx delay

Syntax Description

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

Default

Determined from the delay configured on the interface with the **delay** command.

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.

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:

```
serial interface 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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just 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.

Example

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

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

ipx gns-response-delay

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

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

Syntax Description

time	(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

Usage Guidelines

The delay in responding to Get Nearest Server requests is 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, and 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 ms 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
```

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

Disabled

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-filter

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 FFFFFFFE. A network number of –1 indicates all-nets flooding. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter just 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-packet-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

None

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 (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 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

None

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 (standard)
access-list (extended)
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

None (no input SAP filters are applied)

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 SAP **access-list** 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 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 or 1, 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. The argument *paths* can be a value 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 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

None

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 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 token 1
ipx netbios output-access-filter bytes engineering
```

Related Commands

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

ipx netbios output-access-filter

To control outgoing NetBIOS 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

None

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 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 *number* [**encapsulation** *encapsulation-type* [**secondary**]]
no ipx network *number* [**encapsulation** *encapsulation-type*]

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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter just AA.
encapsulation *encapsulation-type*	(Optional.) Type of encapsulation. 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 network configured after the first (primary) network.

Default

Disabled

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

Command Mode

Interface configuration

Usage Guidelines

The extended **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 also can use this command to configure a single logical network on a physical network.

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.

If you use the standard **ipx network** and **ipx encapsulation** commands on an interface that supports more than one logical network, you can use them only to define the first, or primary, network on the interface. Use the extended **ipx network** command to define additional logical networks.

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.

This 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*

The following two commands also allow you to enable IPX routing on an interface and specify the encapsulation. These commands can be used on interfaces that support a single network or when enabling the primary subinterface on an interface that supports multiple networks. They are supported in this release of the software to provide compatibility with older versions of the router software.

ipx network
ipx encapsulation *encapsulation-type*

Example

The following example configures an interface that has four logical networks:

```
interface ethernet 0
ipx network 0123
ipx encapsulation snap
ipx network 0234 encapsulation arpa secondary
ipx network 0345 encapsulation iso1 secondary
ipx network 0456 encapsulation novell-ether secondary
```

Related Command

ipx routing

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 output GNS filter

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

None

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

ipx output-rip-delay

To adjust the delay between the individual packets sent in a multiple-packet routing update, 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

Syntax Description

delay	Delay, in milliseconds, between packets in a multipacket RIP update. The default delay is 0 (that is, no delay). The delay recommended by Novell is 55 ms.

Default

No delay between routing update packets

Command Mode

Interface configuration

Usage Guidelines

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 interface 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 establishes a 55-ms delay between packets in multiple-packet route updates on serial interface 0:

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

Related Command

ipx update-time

ipx output-sap-delay

To set a delay between packets sent in a multipacket Service Advertisement Protocol (SAP) update, use the **ipx output-sap-delay** interface configuration command. To disable the delay mechanism, use the **no** form of this command.

ipx output-sap-delay *delay*
no ipx output-sap-delay

Syntax Description

delay	Delay, in milliseconds, between packets in a multipacket SAP update. The default delay is 0 (that is, no delay). The delay recommended by Novell is 55 ms.

Default

No delay between SAP update packets

Command Mode

Interface configuration

Usage Guidelines

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 interface 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 establishes a 55-ms delay between packets in multipacket SAP updates on Ethernet interface 0:

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

Related Command

ipx sap-interval

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 variable *access-list-number* is a decimal number from 1000 to 1099.

Default

None

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 permits 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.

Related Commands

ipx route-cache

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 network.node*
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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.
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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just 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*).

Default

None

Command Mode

Global configuration

Usage Guidelines

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

Be careful when assigning static routes. When links associated with static routes are lost, traffic may stop being forwarded, even though alternative paths might be available.

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 Command

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

Syntax Description

cbus	(Optional.) Enables IPX autonomous switching.

Default

Fast switching enabled
Autonomous switching disabled

Type

Interface subcommand

Usage Guidelines

IPX 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.

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 cards, such as the CSC-HSCI, CSC-MEC, CSC-FCI, CSC-C2FCIT, and CSC-C2CTR, and with a CSC-CCTL2 ciscoBus controller running microcode version 11.0 or later.

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.

Examples

In the following example, autonomous switching is enabled on an interface:

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

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

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

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-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

None

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 (standard)
access-list (extended)
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

None

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 **c**ommand.

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 1-3 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 FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter just 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 1-2 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-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-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.

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 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 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.

Example

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

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

Related Commands

ipx helper-address
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 ($3 \times$ *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 ($4 \times$ *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
```

Related Commands

ipx route-cache

netbios access-list

To define an IPX NetBIOS 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 defined

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 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

ping (user)

To check host reachability and network connectivity, use the **ping** 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 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.

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 1-4 describes the test characters displayed in **ping** responses.

Table 1-4 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 Command

ping (privileged)

ping (privileged)

To check host reachability and network connectivity, use the **ping** privileged EXEC command.

ping [**ipx**] [*host* | *address*]

Syntax Description

ipx	(Optional.) Specifies the IPX protocol.
host	(Optional.) Host name of system to ping.
address	(Optional.) Address of system to ping.

Command Mode

Privileged EXEC

Usage Guidelines

The privileged **ping** (packet internet groper function) command provides a complete **ping** facility for users who have system privileges.

The **ping** command 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.

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 1-5 describes the test characters displayed in **ping** responses.

Table 1-5 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 Novell Address: 211.0000.0c01.f4cf
Repeat Count [5]:
Datagram Size [100]:
Timeout in seconds [2]:
Verbose [n]:
Type escape sequence to abort.
Sending 5 100-byte Novell echoes to 211.0000.0c01.f4cf, timeout is 2 seconds.
!!!!!
Success rate is 100%, round trip min/avg/max  = 1/2/4 ms.
```

Related Command

ping (user)

show ipx cache

To display the contents of the IPX fast-switching cache table, 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               Ethernet0              00000C0062E600000C003EB0064
*14BB                Ethernet 1             00000C003E2A00000C003EB0064
```

Table 1-6 describes the fields shown in the display.

Table 1-6 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 Command

clear ipx cache
ipx route-cache

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 [*interface unit*]

Syntax Description

interface unit	(Optional.) Interface and unit identifiers. The argument *interface* can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, tokenring, or tunnel. The variable *unit* is the number of the interface. For example, ethernet 0 specifies the first Ethernet interface.

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx interface** command:

```
router> show ipx interface ethernet 0
Ethernet0 is up, line protocol is up
  IPX address is 1111.0000.0c01.d87a, NOVELL-ETHER [up], RIPPQ: 0, SAPPQ: 0
  Secondary address is 2222.0000.0c01.d87a, SNAP [up]
  Outgoing access list is not set
  IPX type 20 propagation packet forwarding is disabled
  IPX SAP update interval is 1 minute(s)
  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
  Delay of this interface, in ticks is 1
  IPX Fast switching enabled
```

Table 1-7 describes the fields shown in the display.

Table 1-7 Show IPX Interface Field Descriptions

Field	Description
Ethernet 0 is up, 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...	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.
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, 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. This line is displayed only if you have configured a secondary address with the **ipx network** command.
Outgoing access list	Indicates whether an access list has been enabled with the **ipx access-group** 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.
IPX SAP update interval	Indicates the frequency of outgoing SAP updates (configured with the **ipx sap-interval** 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 output-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 output-access-filter bytes** command.
Update time	How often the router sends RIP updates, as configured with the **ipx update-time** command.

Field	Description
Delay of this interface	Value of the ticks field (configured with the **ipx delay** 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 Fast switching IPX Autonomous switching	Indicates whether IPX fast switching is enabled (default) or disabled for this interface, or whether IPX autonomous switching is enabled, as configured with the **ipx route-cache** command.

Related Commands

access-list (standard)
access-list (extended)
access-list (SAP)
ipx delay
ipx encapsulation
ipx helper-list
ipx input-network-filter
ipx input-sap-filter
ipx netbios input-access-filter
ipx netbios output-access-filter
ipx network
ipx output-gns-filter
ipx output-network-filter
ipx output-rip-delay
ipx output-sap-filter
ipx route-cache
ipx router filter
ipx router-sap-filter
ipx sap-interval
ipx update-time
ipx watchdog-spoof
netbios access-list

show ipx route

To display the contents of the IPX routing table, use the **show ipx route** EXEC command.

show ipx route [*network*]

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

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
       R - RIP, E - EIGRP, S - static,8 Total IPX routes

No parallel paths allowed        Novell routing algorithm variant in use

E  Net 1 [307200/0] via 2.0000.0c05.84b6, age 0:01:25,
                        1 uses, Ethernet2
C  Net 2 (NOVELL-ETHER), is directly connected, 30 uses, Ethernet2
E  Net 3 [2195456/0] via 2.0000.0c05.84b6, age 0:01:25,
                        1 uses, Ethernet2
E  Net 11 [281600/0] via 2.0000.0c05.84b6, age 0:01:25,
                        1 uses, Ethernet2
c  Net 2000 (SAP), is directly connected, 3 uses, Ethernet2
R  Net 22 [1/1] via 2.0000.0c05.84b6,  13 sec, 1 uses, Ethernet2
C  Net 55 (NOVELL-ETHER), is directly connected, 30 uses, Ethernet3
S  Net 70  via 55.0011.0022.0033, 1 uses, Ethernet3
```

Table 1-8 describes the fields shown in the display.

Table 1-8 Show IPX Route Field Descriptions

Field	Description
Codes	Codes defining how the route was learned.
C	Directly connected primary network.
c	Directly connected secondary network
R	Route learned from a RIP update.
E	Route learned from an EIGRP update.
S	Statically defined route via the **ipx route** command.
8 Total IPX routes	Numbers of routes in the IPX routing table.

Field	Description
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)	Encapsulation (frame) type. This is shown only for directly connected networks.
is directly connected	Indicates that the network is directly connected to the router.

Related Commands

clear ipx route
ipx maximum-paths
ipx route

show ipx servers

To list the IPX servers discovered through SAP advertisements, use the **show ipx servers** EXEC command.

show ipx servers [**sorted** [{**name** | **net** | **type**}]]

Syntax Description

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

type

Command Mode

EXEC

Sample Display

The following is sample output from the **show ipx servers** command:

```
router> show ipx servers
Codes: P - Periodic, I - Incremental, H - Holddown, S - static
1 Total IPX Servers

Table ordering is based on routing and server info

  Type Name                      Net     Address    Port     Route Hops Itf
P    4 MAXINE                AD33000.0000.1b04.0288:0451 332800/ 1   2  Et3
```

Table 1-9 describes the fields shown in the display.

Table 1-9 Show IPX Server Field Descriptions

Field	Description
Codes	Codes defining how the server was learned.
P	Server information was learned via the normal periodic SAP updates.
I	Server information was learned using the incremental SAP capability in IPX EIGRP.
H	Server is believed to have gone down and the router will no longer advertise this server's services.
S	Statically defined server (via the **ipx sap** command).

Field	Description
Total IPX servers	Number of servers in the list.
Table order is based on routing and server info	Entries listed are based on the routing information associated with this SAP. Server information is used as a tie breaker.
Type	SAP service number.
Name	Server name.
Net	Network number of the server.
Address	Node address of the server.
Port	Socket number.
Route	Metric/hop count for the route to the network.
Hops	SAP-advertised number of hops from the router to the server's network.
Itf	Interface through which this server was first discovered.

Related Command

ipx sap

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** 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:   32124925 total, 1691992 format errors, 0 checksum errors, 67 bad hop count,
        18563 packets pitched, 452467 local destination, 0 multicast
Bcast:  452397 received, 1237193 sent
Sent:   2164776 generated, 31655567 forwarded
        0 encapsulation failed, 2053 no route
SAP:    3684 SAP requests, 10382 SAP replies
        259288 SAP advertisements received, 942564 sent
        0 SAP flash updates sent, 0 SAP poison sent
        0 SAP format errors
RIP:    0 RIP format errors
Echo:   Rcvd 0 requests, 0 replies
        Sent 0 requests, 0 replies
        4252 unknown, 0 SAPs throttled, freed NDB len 0
Watchdog:
        0 packets received, 0 replies spoofed
Queue lengths:
        IPX input: 1, SAP 0, RIP 0, GNS 0
        Total length for SAP throttling purposes: 1/(no preset limit)
IGRP:   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
```

Table 1-10 describes the fields that might possibly be shown in the display.

Table 1-10 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 using a frame type not configured on an interface).
0 checksum errors	Number of packets containing a checksum error.
0 bad hop count	Number of packets discarded because their hop count exceeded 16 (that is, the packets timed out).

Field	Description
0 packets pitched	Number of times the router has discarded packets. This can happen when a type 20 propagation or all-nets broadcast fails the **ipx type-20-input-checks** command; when type 20 propagation packet handling detects a loop, an excessive hop count, or is malformed; RIP or SAP packets are received for the wrong network; the router receives its own broadcast; or the router receives local packets from the wrong source network.
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 in the routing table a route to the destination.
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.
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.
Echo:	Description of the ping replies and requests the router has sent and received.
Rcvd 55 request 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 unrecognized packets sent to the router.
0 SAPs throttled	Number of SAP packets discarded because they exceeded buffer capacity.
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.

Field	Description
0 replies spoofed	Number of times the router has responded to a watchdog packet on behalf of the remote client.
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 incoming SAP packets waiting to be processed.
RIP	Number of incoming RIP packets waiting to be processed.
GNS	Number of incoming GNS packets waiting to be processed.
Total length for SAP throttling purposes	Maximum number of incoming RIP and SAP packets allowed in the buffer. Any SAP request packets received beyond this number are discarded.
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.