ipx default-output-rip-delay

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

ipx default-output-rip-delay *delay*

no ipx default-output-rip-delay

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.

ipx default-output-sap-delay

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

ipx default-output-sap-delay *delay*

no ipx default-output-sap-delay

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx default-route

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

ipx default-route

no ipx default-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled. All packets for which a route to the destination is unknown are forwarded to the default network, which is -2 (0xFFFFFFFE).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When you use the **no ipx default-route** command, Cisco IOS software no longer uses -2 as the default network. Instead, the software interprets -2 as a regular network and packets for which a route to the destination network is unknown are dropped.

Examples

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

```
no ipx default-route
```

Related Commands

Command	Description
ipx advertise-default-route-only	Advertises only the default RIP route through the specified network.

ipx default-triggered-rip-delay

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

ipx default-triggered-rip-delay *delay*

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

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx broadcast-fastswitching	Sets the default interpacket delay for RIP updates sent on all interfaces
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.

ipx default-triggered-rip-holddown

To set the global default for the **ipx triggered-rip-holddown** interface configuration command, use the **ipx default-triggered-rip-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-rip-holddown *milliseconds*

no ipx default-triggered-rip-holddown *milliseconds*

Syntax Description

milliseconds	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Setting the global default for the **ipx triggered-rip-holddown** interface configuration command saves you from needing to configure the command on every interface.

Examples

The following example shows the hold-down time changed to 100 milliseconds:

```
ipx default-triggered-rip-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.
ipx triggered-sap-holddown	Sets an amount of time an IPX SAP process will wait before sending flashes about SAP changes.

ipx default-triggered-sap-delay

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

ipx default-triggered-sap-delay *delay*

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

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx default-triggered-sap-holddown

To set the global default for the **ipx triggered-sap-holddown** interface configuration command, use the **ipx default-triggered-sap-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-sap-holddown *milliseconds*

no ipx default-triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Setting the global default for the **ipx triggered-sap-holddown** interface configuration command saves you from needing to configure a **triggered-sap-holddown** command on every interface.

Examples

The following example shows the hold-down time changed to 100 ms:

```
ipx default-triggered-sap-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-rip-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-rip-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.
ipx triggered-sap-holddown	Sets an amount of time an IPX SAP process will wait before sending flashes about SAP changes.

ipx delay

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

ipx delay *ticks*

no ipx delay

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

IPXWAN links determine their delay dynamically. If you do not specify the **ipx delay** command on an interface and you have not changed the interface delays with the **interface delay** interface configuration command, all LAN interfaces have a delay of 1 and all WAN interfaces have a delay of 6. The preferred method of adjusting delays is to use the **ipx delay** command, not the **interface delay** command. The **show ipx interface** EXEC command display only the delay value configured with the **ipx delay** command.

With IPXWAN, if you change the interface delay with the **interface delay** command, the **ipx delay** command uses that delay when calculating a delay to use. Also, when changing delays with IPXWAN, the changes affect only the link's calculated delay on the side considered to be the master.

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

Examples

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

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

Related Commands

Command	Description
delay	Sets a delay value for an interface.
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.
ipx output-network-filter	Controls the list of networks included in routing updates sent out an interface.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.

ipx down

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

ipx down *network*

no ipx down

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

ipx eigrp-sap-split-horizon

To configure Enhanced Interior Gateway Routing Protocol (EIGRP) SAP split horizon, use the **ipx eigrp-sap-split-horizon** command in global configuration mode. To revert to the default, use the **no** form of this command.

ipx eigrp-sap-split-horizon

no ipx eigrp-sap-split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled on LANs and disabled on WANs.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When split horizon is enabled, Enhanced IGRP SAP update and packets are not sent back to the same interface where the SAP is received from. This reduces the number of Enhanced IGRP packets on the network.

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

Note When the **ipx sap-incremental split-horizon** interface configuration command is configured, it takes precedence over the **ipx eigrp-sap-split-horizon** command.

Examples

The following example disables split horizon on the router:

```
no ipx eigrp-sap-split-horizon
```

Related Commands

Command	Description
ipx sap-incremental split-horizon	Configures incremental SAP split horizon.
ipx split-horizon eigrp	Configures split horizon.
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

ipx encapsulation

To set the Ethernet frame type of the interface to that of the local file server, use the **ipx encapsulation** command in interface configuration mode. To reset the frame type to the default, use the **no** form of this command.

ipx encapsulation *encapsulation-type*

no ipx encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	(Required) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 48.

Table 48 describes the types of encapsulation available for specific interfaces.

Table 48 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses 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 all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 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—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (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.

Defaults

novell-ether

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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 that use 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.

Note If you have not yet enabled IPX routing on the interface, you can save time by using the **ipx network** command, which allows you to enable IPX routing on the interface and select the encapsulation type in one command.

To determine the frame type of the server, use the **config** command at the prompt of the local server.

Examples

The following example sets the frame type to Novell Ethernet II:

```
interface ethernet 0
 ipx encapsulation arpa
```

Related Commands

Command	Description
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
ipx routing	Enables IPX routing.

ipx flooding-unthrottled (NLSP)

To control whether a router will throttle NetWare Link Services Protocol (NLSP) packets, use the **ipx flooding-unthrottled** command in global configuration mode. To re-establish the default for unthrottled NLSP packets, use the **no** form of this command.

ipx flooding-unthrottled

no ipx flooding-unthrottled

Syntax Description

This command has no arguments or keywords.

Defaults

Unthrottled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Using the **ipx flooding-unthrottled** command may result in excessive NLSP traffic, causing network congestion. You can configure the router to throttle NLSP packets by using the **no ipx flooding-unthrottled** command.

Examples

The following example applies the default setting for unthrottled NLSP packets:

```
ipx flooding-unthrottled
```

ipx gns-reply-disable

To disable the sending of replies to IPX Get Nearest Server (GNS) queries, use the **ipx gns-reply-disable** command in interface configuration mode. To return to the default, use the **no** form of this command.

ipx gns-reply-disable

no ipx gns-reply-disable

Syntax Description

This command has no arguments or keywords.

Defaults

Replies are sent to IPX GNS queries.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

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

Related Commands

Command	Description
ipx gns-response-delay	Changes the delay when responding to GNS requests.

ipx gns-response-delay

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

ipx gns-response-delay [*milliseconds*]

no ipx gns-response-delay

Syntax Description

milliseconds	(Optional) Time, in milliseconds (ms), that the Cisco IOS software waits after receiving a GNS request from an IPX client before responding with a server name to that client. The default is zero, which indicates no delay.

Defaults

0 (no delay)

Command Modes

Global configuration (globally changes the delay for the router)
Interface configuration (overrides the globally configured delay for an interface)

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command can be used in two modes: global configuration or interface configuration. In both modes, the command syntax is the same. A delay in responding to GNS requests might be imposed so that, in certain topologies, any local Novell IPX servers respond to the GNS requests before our software 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 response. 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.

Examples

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

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

Related Commands

Command	Description
ipx gns-reply-disable	Disables the sending of replies to IPX GNS queries.
ipx rip-response-delay	Changes the delay when responding to RIP requests.

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** command in global configuration mode. 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

This command has no arguments or keywords.

Defaults

The most recently learned eligible server is used.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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 Cisco IOS software maintains a list of the nearest servers eligible to provide specific services. It uses this list when responding to 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.

Examples

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

Command	Description
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by the Cisco IOS software.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.

ipx hello-interval eigrp

To configure the interval between Enhanced Interior Gateway Routing Protocol (EIGRP) hello packets, use the **ipx hello-interval eigrp** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx hello-interval eigrp *autonomous-system-number seconds*

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

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can a number from 1 to 65,535.
seconds	Interval between hello packets, in seconds. The default interval is 5 seconds, which is one-third of the default hold time.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example changes the hello interval to 10 seconds:

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

Related Commands

Command	Description
ipx hold-down eigrp	Specifies the length of time a lost Enhanced IGRP route is placed in the hold-down state.

ipx helper-address

To forward broadcast packets to a specified server, use the **ipx helper-address** command in interface configuration mode. To disable this function, use the **no** form of this command.

ipx helper-address *network.node*

no ipx helper-address *network.node*

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

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. 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.

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

The Cisco IOS software supports 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 software takes 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.

To forward type 20 packets to only those nodes specified by the **ipx helper-address** command, use the **ipx helper-address** command in conjunction with the **ipx type-20-helpered** global configuration command.

To forward type 20 packets to all nodes on the network, use the **ipx type-20-propagation** command. See the **ipx type-20-propagation** command for more information.

Examples

The following example forwards 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

Command	Description
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

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** command in interface configuration mode. To remove the access list from an interface, use the **no** form of this command.

ipx helper-list {*access-list-number* | *name*}

no ipx helper-list {*access-list-number* | *name*}

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, the value for the *access-list-number* argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No access list is preassigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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

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

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx hold-down eigrp

To specify the length of time a lost Enhanced Interior Gateway Routing Protocol (EIGRP) route is placed in the hold-down state, use the **ipx hold-down eigrp** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipx hold-down eigrp *autonomous-system-number seconds*

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

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
seconds	Hold-down time, in seconds. The default hold time is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an Enhanced IGRP route is lost, it is placed into a hold-down state for a period of time. The purpose of the hold-down state is to ensure the validity of any new routes for the same destination.

The amount of time a lost Enhanced IGRP route is placed in the hold-down state is configurable. Set the amount of time to a value longer than the default of 5 seconds if your network requires a longer time for the unreachable route information to propagate.

Examples

The following example changes the hold-down time for autonomous system from 4 to 45 seconds:

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

ipx hold-time eigrp

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

ipx hold-time eigrp *autonomous-system-number seconds*

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

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
seconds	Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is 15 seconds, which is three times the hello interval.

Defaults

For low-speed nonbroadcast, multiaccess (NBMA) networks: 180 seconds
For all other networks: 15 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Increasing the hold time delays route convergence across the network.

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

Examples

The following example changes the hold time to 45 seconds:

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

Related Commands

Command	Description
ipx hello-interval eigrp	Configures the interval between Enhanced IGRP hello packets.

ipx input-network-filter (RIP)

To control which networks are added to the Cisco IOS software routing table, use the **ipx input-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx input-network-filter {*access-list-number* | *name*}

no ipx input-network-filter {*access-list-number* | *name*}

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, the value for the *access-list-number* argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

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

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx output-network-filter	Controls the list of networks included in routing updates sent out an interface.
ipx router-filter	Filters the routers from which packets are accepted.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx input-sap-filter

To control which services are added to the Cisco IOS software SAP table, use the **ipx input-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx input-sap-filter {*access-list-number* | *name*}

no ipx input-sap-filter {*access-list-number* | *name*}

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 number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx internal-network

To set an internal network number for use by NetWare Link Services Protocol (NLSP) and IPXWAN, use the **ipx internal-network** command in global configuration mode. To remove an internal network number, use the **no** form of this command.

ipx internal-network *network-number*

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

Syntax Description

network-number	Number of the internal network.

Defaults

No internal network number is set.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

An internal network number is a network number assigned to the router. This network number must be unique within the internetwork.

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

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

Examples

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

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

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
ipx routing	Enables IPX routing.

ipx ipxwan

To enable the IPX wide-area network (IPXWAN) protocol on a serial interface, use the **ipx ipxwan** command in interface configuration mode. To disable the IPXWAN protocol, use the **no** form of this command.

ipx ipxwan [*local-node* {*network-number* | **unnumbered**} *local-server-name retry-interval retry-limit*]

no ipx ipxwan

Syntax Description

local-node	(Optional) Primary network number of the router. This is an IPX network number that is unique across the entire internetwork. On NetWare 3.*x* servers, the primary network number is called the internal network number. The device with the higher number is determined to be the link master. A value of 0 causes the Cisco IOS software to use the configured internal network number.
network-number	(Optional) IPX network number to be used for the link if this router is the one determined to be the link master. The number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 0 to FFFFFFFD. A value 0 is equivalent to specifying the keyword **unnumbered**. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
unnumbered	(Optional) Specifies that no IPX network number is defined for the link. This is equivalent to specifying a value of 0 for the *network-number* argument.
local-server-name	(Optional) Name of the local router. It can be up to 47 characters long, and can contain uppercase letters, digits, underscores (_), hyphens (-), and at signs (@). On NetWare 3.*x* servers, this is the router name. For our routers, this is the name of the router as configured via the **hostname** command; that is, the name that precedes the standard prompt, which is an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.
retry-interval	(Optional) Retry interval, in seconds. This interval defines how often the software will retry the IPXWAN start-up negotiation if a start-up failure occurs. Retries will occur until the retry limit defined by the *retry-limit* argument is reached. It can be a value from 1 to 600. The default is 20 seconds.
retry-limit	(Optional) Maximum number of times the software retries the IPXWAN start-up negotiation before taking the action defined by the **ipx ipxwan error** command. It can be a value from 1 through 100. The default is 3.

Defaults

IPXWAN is disabled.

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keyword and argument were added: • **unnumbered** • *retry-interval*

Usage Guidelines

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

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

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

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

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

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

Examples

The following example enables IPXWAN on serial interface 0:

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

The following example enables IPXWAN on serial interface 1 on device CHICAGO-AS. When the link comes up, CHICAGO-AS will be the master because it has a larger internal network number. It will give the IPX number 100 to NYC-AS to use as the network number for the link. The link delay, in ticks, will be determined by the exchange of packets between the two access servers.

On the local access server (CHICAGO-AS):

```
interface serial 1
 no ipx network
 encapsulation ppp
 ipx ipxwan 6666 100 CHICAGO-AS
```

On the remote router (NYC-AS):

```
interface serial 0
 no ipx network
 encapsulation ppp
 ipx ipxwan 1000 101 NYC-AS
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
hostname	Specifies or modify the host name for the network server.
ipx delay	Sets the tick count.
ipx internal-network	Sets an internal network number for use by NLSP and IPXWAN.
ipx ipxwan error	Defines how to handle IPXWAN when IPX fails to negotiate properly at link startup.
ipx ipxwan static	Negotiates static routes on a link configured for IPXWAN.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx ipxwan error

To define how to handle IPX wide-area network (IPXWAN) when IPX fails to negotiate properly at link startup, use the **ipx ipxwan error** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx ipxwan error [**reset** | **resume** | **shutdown**]

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

Syntax Description

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

Defaults

The link is reset.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx ipxwan static	Negotiates static routes on a link configured for IPXWAN.

ipx ipxwan static

To negotiate static routes on a link configured for IPX wide-area network (IPXWAN), use the **ipx ipxwan static** command in interface configuration mode. To disable static route negotiation, use the **no** form of this command.

ipx ipxwan static

no ipx ipxwan static

Syntax Description

This command has no arguments or keywords.

Defaults

Static routing is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

The following example enables static routing with IPXWAN:

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

Related Commands

Command	Description
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx ipxwan error	Defines how to handle IPXWAN when IPX fails to negotiate properly at link startup.

ipx link-delay

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

ipx link-delay *microseconds*

no ipx link-delay *microseconds*

Syntax Description

microseconds	Delay, in microseconds.

Defaults

No link delay (delay of 0).

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

The following example sets the link delay to 20 microseconds:

```
ipx link-delay 20
```

Related Commands

Command	Description
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx spx-idle-time	Sets the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer.

ipx linkup-request (RIP)

To enable the sending of a general RIP and/or SAP query when an interface comes up, use the **ipx linkup-request** command in interface configuration mode. To disable the sending of a general RIP and/or SAP query when an interface comes up, use the **no** form of this command.

ipx linkup-request {**rip** | **sap**}

no ipx linkup-request {**rip** | **sap**}

Syntax Description

rip	Enables the sending of a general RIP query when an interface comes up.
sap	Enables the sending of a general SAP query when an interface comes up.

Defaults

General RIP and SAP queries are sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Under normal operation, when using serial or other point-to-point links, the router sends RIP and SAP information twice when an interface comes up. The RIP and SAP information is sent as soon as the link is up and is sent again when the router receives a general RIP query from the other end of the connection. By disabling the **ipx linkup-request** command, the router sends the RIP and SAP information once, instead of twice.

Examples

The following example configures the router to disable the general query for both RIP and SAP on serial interface 0:

```
interface serial 0
 no ipx linkup-request rip
 no ipx linkup-request sap
```

Related Commands

Command	Description
ipx update interval	Adjusts the RIP or SAP update interval.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx maximum-hops (RIP)

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

ipx maximum-hops *hops*

no ipx maximum-hops *hops*

Syntax Description

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

Defaults

16 hops

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
ipx maximum-hops 64
```

ipx maximum-paths

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

ipx maximum-paths *paths*

no ipx maximum-paths

Syntax Description

paths	Maximum number of equal-cost paths which the Cisco IOS software will use. It can be a number from 1 to 512. The default value is 1.

Defaults

1 path

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx maximum-paths** command increases throughput by allowing the software to choose among several equal-cost, parallel paths. (Note that when paths have differing costs, the software chooses lower-cost routes in preference to higher-cost routes.)

When per-host load sharing is disabled, IPX performs 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 with 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.

When you enable per-host load sharing, IPX performs load sharing by transmitting traffic across multiple, equal-cost paths while guaranteeing that packets for a given end host always take the same path. Per-host load sharing decreases the possibility that successive packets to a given end host will arrive out of order.

With per-host load balancing, the number of equal-cost paths set by the **ipx maximum-paths** command must be greater than one; otherwise, per-host load sharing has no effect.

Examples

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

```
ipx maximum-paths 3
```

Related Commands

Command	Description
ipx delay	Sets the tick count.
ipx per-host-load-share	Enables per-host load sharing.
show ipx route	Displays the contents of the IPX routing table.

ipx netbios input-access-filter

To control incoming IPX NetBIOS FindName messages, use the **ipx netbios input-access-filter** command in interface configuration mode. 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.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
netbios access-list host engineering permit eng*
netbios access-list host engineering deny manu*

interface tokenring 1
 ipx netbios input-access-filter engineering
```

Related Commands

Command	Description
ipx netbios output-access-filter	Controls outgoing NetBIOS FindName messages.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx netbios output-access-filter

To control outgoing NetBIOS FindName messages, use the **ipx netbios output-access-filter** command in interface configuration mode. 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.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
netbios access-list bytes engineering permit 20 AA**04

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

Related Commands

Command	Description
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx netbios-socket-input-checks

To enable additional checks that are performed on Network Basic Input/Output System (NetBIOS) packets that do not conform fully to Novell Type20 NetBIOS packets, use the **ipx netbios-socket-input-checks** command in global configuration mode. To disable the additional checking, use the **no** form of this command.

ipx netbios-socket-input-checks

no ipx netbios-socket-input-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use the **ipx netbios-socket-input-checks** command to enable additional checks on NetBIOS packets that do not fully conform to Novell Type20 NetBIOS packets, the same checks that are performed on Type20 packets to avoid broadcast loops are performed for any packet that does not have the netBIOS socket, even if it is not a Novell Type20 packet.

Note In order to forward non-Type20 broadcasts, you must configure a helper address on two or more interfaces. For more information, see the **ipx helper-address** command earlier in this chapter.

Examples

The following example enables the additional checks on NetBIOS packets:

```
ipx netbios-socket-input-checks
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-input-checks	Restricts the acceptance of IPX Type20 propagation packet broadcasts.
ipx type-20-output-checks	Restricts the forwarding of IPX Type20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX Type20 propagation packet broadcasts to other network segments.

ipx network

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

ipx network *network* [**encapsulation** *encapsulation-type* [**secondary**]]

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

Syntax Description

network	Network number. This is an 8-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
encapsulation *encapsulation-type*	(Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 49.
secondary	(Optional) Indicates an additional (secondary) network configured after the first (primary) network.

Table 49 describes the types of encapsulation available for specific interfaces.

Table 49 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses 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 all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.

Table 49 Encapsulation Types (continued)

Encapsulation Type	Description
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 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—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (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.

Defaults

IPX routing is disabled.

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

If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from **novell-ether** to **sap**.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to support the FDDI interface.

Usage Guidelines

The **ipx network** command allows you to configure a single logical network on a physical network or 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.

Note You cannot configure more than 200 IPX interfaces on a router using the **ipx network** command.

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.

Note In future Cisco IOS software releases, primary and secondary networks may not be supported.

NetWare Link-Services Protocol (NLSP) does not support secondary networks. You must use subinterfaces in order to use multiple encapsulations with NLSP.

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

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

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

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

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

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

Note If you have already enabled IPX routing on the specified interface, you can use the **ipx encapsulation** command to change the encapsulation type.

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*

Novell's FDDI_RAW encapsulation is common in bridged or switched environments that connect Ethernet-based Novell end hosts via a FDDI backbone. Packets with FDDI_RAW encapsulation are classified as Novell packets and are not automatically bridged when you enable both bridging and IPX

routing. Additionally, you cannot configure FDDI_RAW encapsulation on an interface configured for IPX autonomous or silicon switching engine (SSE) switching. Similarly, you cannot enable IPX autonomous or SSE switching on an interface configured with FDDI_RAW encapsulation.

With FDDI_RAW encapsulation, platforms that do not use CBUS architecture support fast switching. Platforms using CBUS architecture support only process switching of **novell-fddi** packets received on an FDDI interface.

Examples

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

```
ipx routing
interface ethernet 0
 ipx network 1 encapsulation novell-ether

interface ethernet 0.1
 ipx network 2 encapsulation snap

interface ethernet 0.2
 ipx network 3 encapsulation arpa

interface ethernet 0
 ipx network 4 encapsulation sap
```

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

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

The following example enables IPX routing on FDDI interfaces 0.2 and 0.3. On FDDI interface 0.2, the encapsulation type is SNAP. On FDDI interface 0.3, the encapsulation type is Novell's FDDI_RAW.

```
ipx routing

interface fddi 0.2 enc sde 2
 ipx network f02 encapsulation snap

interface fddi 0.3 enc sde 3
 ipx network f03 encapsulation novell-fddi
```

Related Commands

Command	Description
ipx encapsulation	Sets the Ethernet frame type of the interface to that of the local file server.
ipx routing	Enables IPX routing.

ipx nhrp authentication

To configure the authentication string for an interface using Next Hop Resolution Protocol (NHRP), use the **ipx nhrp authentication** command in interface configuration mode. To remove the authentication string, use the **no** form of this command.

ipx nhrp authentication *string*

no ipx nhrp authentication [*string*]

Syntax Description

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.

Defaults

No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

All routers configured with NHRP on a fabric (for an interface) must share the same authentication string.

Examples

In the following example, the authentication string specialxx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ipx nhrp authentication specialxx
```

ipx nhrp holdtime

To change the number of seconds for which Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ipx nhrp holdtime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nhrp holdtime *seconds-positive* [*seconds-negative*]

no ipx nhrp holdtime [*seconds-positive* [*seconds-negative*]]

Syntax Description

seconds-positive	Time in seconds for which NBMA addresses are advertised as valid in positive authoritative NHRP responses.
seconds-negative	(Optional) Time in seconds for which NBMA addresses are advertised as valid in negative authoritative NHRP responses.

Defaults

7200 seconds (2 hours) for both arguments.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The **ipx nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time for which the Cisco IOS software tells other routers to keep information that it is provided in authoritative NHRP responses. The cached IPX-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

If you want to change the valid time period for negative NHRP responses, you must also include a value for positive NHRP responses, as the arguments are position-dependent.

Examples

The following example advertises NHRP NBMA addresses as valid in positive authoritative NHRP responses for one hour:

```
ipx nhrp holdtime 3600
```

The following example advertises NHRP NBMA addresses as valid in negative authoritative NHRP responses for one hour and in positive authoritative NHRP responses for two hours:

```
ipx nhrp holdtime 7200 3600
```

ipx nhrp interest

To control which IPX packets can trigger sending a Next Hop Resolution Protocol (NHRP) request, use the **ipx nhrp interest** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nhrp interest *access-list-number*

no ipx nhrp interest [*access-list-number*]

Syntax Description

access-list-number	Standard or extended IPX access list number from 800 through 999.

Defaults

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command with the **access-list** command to control which IPX packets trigger NHRP requests.

Examples

In the following example, any NetBIOS traffic can cause NHRP requests to be sent, but no other IPX packets will cause NHRP requests:

```
ipx nhrp interest 901
access-list 901 permit 20
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.

ipx nhrp map

To statically configure the IPX-to-NBMA address mapping of IPX destinations connected to a nonbroadcast multiaccess (NBMA) network, use the **ipx nhrp map** command in interface configuration mode. To remove the static entry from NHRP cache, use the **no** form of this command.

ipx nhrp map *ipx-address nbma-address*

no ipx nhrp map *ipx-address nbma-address*

Syntax Description

ipx-address	IPX address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a network service access point (NSAP) address, and SMDS has an E.164 address. This address is mapped to the IPX address.

Defaults

No static IPX-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

You will probably have to configure at least one static mapping in order to reach the Next Hop Server. Repeat this command to statically configure multiple IPX-to-NBMA address mappings.

Examples

The following example statically configures this station in an SMDS network to be served by two Next Hop Servers 1.0000.0c14.59ef and 1.0000.0c14.59d0. The NBMA address for 1.0000.0c14.59ef is statically configured to be c141.0001.0001 and the NBMA address for 1.0000.0c14.59d0 is c141.0001.0002.

```
interface serial 0
 ipx nhrp nhs 1.0000.0c14.59ef
 ipx nhrp nhs 1.0000.0c14.59d0
 ipx nhrp map 1.0000.0c14.59ef c141.0001.0001
 ipx nhrp map 1.0000.0c14.59d0 c141.0001.0002
```

Related Commands

Command	Description
clear ipx nhrp	Clears all dynamic entries from the NHRP cache.

ipx nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ipx nhrp max-send** command in interface configuration mode. To restore this frequency to the default value, use the **no** form of this command.

ipx nhrp max-send *pkt-count* **every** *interval*

no ipx nhrp max-send

Syntax Description

pkt-count	Number of packets for which can be transmitted in the range 1 to 65,535.
every *interval*	Time (in seconds) in the range 10 to 65,535. Default is 10 seconds.

Defaults

pkt-count = 5 packets
interval = 10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The software maintains a per interface quota of NHRP packets that can be transmitted. NHRP traffic, whether locally generated, or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *interval* argument.

Examples

In the following example, only one NHRP packet can be sent out serial interface 0 each minute:

```
interface serial 0
 ipx nhrp max-send 1 every 60
```

Related Commands

Command	Description
ipx nhrp interest	Controls which IPX packets can trigger sending an NHRP Request.
ipx nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ipx nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ipx nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

ipx nhrp network-id *number*

no ipx nhrp network-id

Syntax Description

number	Globally unique, 32-bit network identifier for a nonbroadcast multiaccess (NBMA) network. The range is 1 to 4,294,967,295.

Defaults

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

In general, all NHRP stations within a fabric must be configured with the same network identifier.

Examples

The following example enables NHRP on the interface:

```
ipx nhrp network-id 1
```

ipx nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) Next Hop Servers, use the **ipx nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

ipx nhrp nhs *nhs-address* [*net-address*]

no ipx nhrp nhs *nhs-address* [*net-address*]

Syntax Description

nhs-address	Address of the Next Hop Server being specified.
net-address	(Optional) IPX address of a network served by the Next Hop Server.

Defaults

No Next Hop Servers are explicitly configured, so normal network layer routing decisions forward NHRP traffic.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to specify the address of a Next Hop Server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When Next Hop Servers are configured, the next hop addresses specified with the **ipx nhrp nhs** command override the forwarding path specified by the network layer forwarding table that would usually be used for NHRP traffic.

For any Next Hop Server that is configured, you can specify multiple networks that it serves by repeating this command with the same *nhs-address* address, but different *net-address* IPX network numbers.

Examples

In the following example, the Next Hop Server with address 1.0000.0c00.1234 serves IPX network 2:

```
ipx nhrp nhs 1.0000.0c00.1234 2
```

ipx nhrp record

To re-enable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) Request and Reply packets, use the **ipx nhrp record** command in interface configuration mode. To suppress the use of such options, use the **no** form of this command.

ipx nhrp record

no ipx nhrp record

Syntax Description

This command has no arguments or keywords.

Defaults

Forward record and reverse record options are enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Forward record and reverse record options provide loop detection and are used in NHRP Request and Reply packets. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ipx nhrp responder** command.

Examples

The following example suppresses forward record and reverse record options:

```
no ipx nhrp record
```

Related Commands

Command	Description
ipx nhrp responder	Designates the primary IPX address of the interface that the Next Hop Server uses in NHRP Reply packets when the NHRP requester uses the Responder Address option.

ipx nhrp responder

To designate which interface's primary IPX address that the Next Hop Server uses in Next Hop Resolution Protocol (NHRP) Reply packets when the NHRP requestor uses the Responder Address option, use the **ipx nhrp responder** command in interface configuration mode. To remove the designation, use the **no** form of this command.

ipx nhrp responder *type number*

no ipx nhrp responder [*type*] [*number*]

Syntax Description

type	Interface type whose primary IPX address is used when a Next Hop Server complies with a Responder Address option. Valid options are **atm**, **serial**, and **tunnel**.
number	Interface number whose primary IPX address is used when a Next Hop Server complies with a Responder Address option.

Defaults

The Next Hop Server uses the IPX address of the interface where the NHRP Request was received.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If an NHRP requestor wants to know which Next Hop Server generates an NHRP Reply packet, it can request that information through the Responder Address option. The Next Hop Server that generates the NHRP Reply packet then complies by inserting its own IPX address in the Responder Address option of the NHRP Reply. The Next Hop Server uses the primary IPX address of the specified interface.

If an NHRP Reply packet being forwarded by a Next Hop Server contains that Next Hop Server's own IPX address, the Next Hop Server generates an Error Indication of type "NHRP Loop Detected" and discards the Reply.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a Next Hop Server to supply the primary IPX address of interface serial 0 in the NHRP Reply packet:

```
ipx nhrp responder serial 0
```

ipx nhrp use

To configure the software so that Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ipx nhrp use** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nhrp use *usage-count*

no ipx nhrp use *usage-count*

Syntax Description

usage-count	Packet count in the range 1 to 65,535.

Defaults

The default is *usage-count* = 1. The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

When the software attempts to transmit a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally transmitted right away. Configuring the usage-count causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The usage-count for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage-count applies per destination. So if usage-count is configured to be 3, and 4 data packets are sent toward 10.0.0.1 and 1 packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests are performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ipx nhrp interest** command controls which packets cause NHRP address resolution to take place; the **ipx nhrp use** command controls how readily the system attempts such address resolution.

Examples

In the following example, if in the first minute four packets are sent to one IPX address and five packets are sent to a second IPX address, then a single NHRP request is generated for the second IPX address. If in the second minute the same traffic is generated and no NHRP responses have been received, then the system retransmits its request for the second IPX address.

```
ipx nhrp use 5
```

Related Commands

Command	Description
ipx nhrp interest	Controls which IPX packets can trigger sending an NHRP Request.
ipx nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ipx nlsp csnp-interval

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

ipx nlsp [*tag*] **csnp-interval** *seconds*

no ipx nlsp [*tag*] **csnp-interval** *seconds*

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
seconds	Time, in seconds, between the transmission of CSNPs on multiaccess networks. This interval applies to the designated router only. The interval can be a number in the range 1 to 600. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
interface ethernet 0
 ipx network 101
 ipx nlsp enable
 ipx nlsp csnp-interval 10
```

Command	Description
ipx nlsp hello-interval	Specifies the hello multiplier used on an interface.
ipx nlsp retransmit-interval	Configures RIP compatibility when NLSP is enabled.