ipx sap-incremental (EIGRP)

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

ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

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

Syntax Description

eigrp *autonomous-system-number*	IPX Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
rsup-only	(Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

Defaults

Enabled on serial interfaces

Disabled on LAN media (Ethernet, Token Ring, FDDI)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

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

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

To take advantage of Enhanced IGRP's incremental SAP update mechanism while using the RIP routing protocol instead of the Enhanced IGRP routing protocol, specify the **rsup-only** keyword. SAP updates are then sent only when changes occur, and only changes are sent. Use this feature only when you want to use RIP routing; Cisco IOS software disables the exchange of route information via Enhanced IGRP for that interface.

Examples

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

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

ipx sap-incremental split-horizon

To configure incremental SAP split horizon, use the **ipx sap-incremental split-horizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipx sap-incremental split-horizon

no ipx sap-incremental split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Caution For IPX incremental SAP split horizon to work properly, IPX Enhanced **IGRP** should be turned on. Otherwise, a warning message like the following will be displayed:

```
%IPX EIGRP not running.
```

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

Split horizon blocks information about SAPs from being advertised by a router to the same interface from where that SAP is received. 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 IPX incremental SAP split horizon is off for WAN interfaces and subinterfaces, and on for LAN interfaces. The global default stays off. The interface setting takes precedence if the interface setting is modified or when both the global and interface settings are unmodified. The global setting is used only when global setting is modified and the interface setting is unmodified.

Examples

The following example disables split horizon on serial interface 0:

```
interface serial 0
```

```
no ipx sap-incremental split-horizon
```

Related Commands

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

ipx sap-max-packetsize

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

ipx sap-max-packetsize *bytes*

no ipx sap-max-packetsize *bytes*

Syntax Description

bytes	Maximum packet size, in bytes. The default is 480 bytes, which allows for 7 servers (64 bytes each), plus 32 bytes of IPX network and SAP header information.

Defaults

480 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The maximum size is for the IPX packet, including the IPX network and SAP header information. For example, to allow 10 servers per SAP packet, you would configure (32 + (10 * 64)), or 672 bytes for the maximum packet size.

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

Examples

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

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

Related Commands

Command	Description
ipx rip-max-packetsize	Configures the maximum packet size of RIP updates sent out the interface.

ipx sap-multiplier

To configure the interval at which a Service Advertising Protocol (SAP) entry for a network or server ages out, use the **ipx sap-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx sap-multiplier *multiplier*

no ipx sap-multiplier *multiplier*

Syntax Description

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

Defaults

Three times the SAP update interval.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ipx sap-max-packetsize	Configures the maximum packet size of SAP updates sent out the interface.

ipx sap-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many SAP packets can be waiting to be processed at any given time, use the **ipx sap-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

ipx sap-queue-maximum *queue-maximum*

no ipx sap-queue-maximum *queue-maximum*

Syntax Description

queue-maximum	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit

Command Modes

Global configuration

Command History

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

Usage Guidelines

When you use the **ipx sap-queue-maximum** command to control how many SAP packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming SAP request packets are dropped. Be sure to set a large enough queue limit to handle normal incoming SAP requests on all interfaces, or else the SAP information may time out.

Examples

The following example sets a SAP queue maximum of 500 milliseconds:

```
ipx sap-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx sap-update-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time, use the **ipx sap-update-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

ipx sap-update-queue-maximum *queue-maximum*

no ipx sap-update-queue-maximum *queue-maximum*

Syntax Description

queue-maximum	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit

Command Modes

Global configuration

Command History

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

Usage Guidelines

When you use the **ipx sap-update-queue-maximum** command to control how many incoming SAP update packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming SAP update packets are dropped.

Note When using the **ipx sap-update-queue-maximum** command, be sure to set this queue high enough to handle a full update on all interfaces, or else the SAP information may time out.

Examples

The following example sets a SAP update queue maximum of 500:

```
ipx sap-update-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.

ipx server-split-horizon-on-server-paths

To control whether Service Information split horizon checking should be based on Router Information Protocol (RIP) paths or Service Advertising Protocol (SAP) paths, use the **ipx server-split-horizon-on-server-paths** command in global configuration mode. To return to the normal mode of following route paths, use the **no** form of this command.

ipx server-split-horizon-on-server-paths

no ipx server-split-horizon-on-server-paths

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

By default, split horizon prevents information about periodic SAPs from being advertised by a router to the same interface in which the best route to that SAP is learned. However, in an instance where the SAP may be learned from interfaces other than, or in addition to, the interface on which the best route to that SAP is learned, using the **ipx server-split-horizon-on-server-paths** command may reduce the number of unnecessary periodic SAP updates. The reduction in the number of SAP updates occurs because each SAP will not be advertised on the interface or interfaces it was learned from. The reduction in the number of SAP updates will also prevent a potential SAP loop in the network.

Examples

The following example shows the application of split horizon blocks:

```
ipx server-split-horizon-on-server-paths
```

Related Commands

Command	Description
ipx eigrp-sap-split-horizon	Configures EIGRP SAP split horizon.
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.
ipx sap-incremental split-horizon	Configures incremental SAP split horizon.
ipx split-horizon eigrp	Configures split horizon.

ipx split-horizon eigrp

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

ipx split-horizon eigrp *autonomous-system-number*

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

Syntax Description

autonomous-system-number	Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system number. It can be a number from 1 to 65,535.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Split horizon blocks information about routes from being advertised by Cisco IOS software to 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 Switched Multimegabit Data Service (SMDS), situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.

Examples

The following example disables split horizon on serial interface 0:

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

ipx spx-idle-time

To set the amount of time to wait before starting the spoofing of Sequenced Packet Exchange (SPX) keepalive packets following inactive data transfer, use the **ipx spx-idle-time** command in interface configuration mode. To disable the current delay time set by this command, use the **no** form of this command.

ipx spx-idle-time *delay-in-seconds*

no ipx spx-idle-time

Syntax Description

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

Defaults

60 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins when SPX spoofing begins. For example, if the dialer idle time is 3 minutes, the elapse time before SPX spoofing begins is 4 minutes: 3 minutes of dialer idle time plus 1 minute of SPX spoofing idle time.

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

Examples

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

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

Related Commands

Command	Description
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.
show ipx spx-spoof	Displays the table of SPX connections through interfaces for which SPX spoofing is enabled.

ipx spx-spoof

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

ipx spx-spoof [**session-clear** *session-clear-minutes* | **table-clear** *table-clear-hours*]

no ipx spx-spoof [**session-clear** | **table-clear**]

Syntax Description

session-clear	(Optional) Sets the time to clear inactive entries. Values are 0 through 4,294,967,295.
table-clear	(Optional) Sets the time to clear the SPX table.
session-clear-minutes	(Optional) Number of minutes before inactive entries are cleared from the session. Values are 0 through 4,294,967,295.
table-clear-hours	(Optional) Number of hours before the IPX table is cleared. Values are 0 through 4,294,967,295.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

The following example enables spoofing on serial interface 0:

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

Related Commands

Command	Description
ipx throughput	Configures the throughput.
show ipx spx-spoof	Displays the table of SPX connections through interfaces for which SPX spoofing is enabled.

ipx throughput

To configure the throughput, use the **ipx throughput** command in interface configuration mode. To revert to the current bandwidth setting for the interface, use the **no** form of this command.

ipx throughput *bits-per-second*

no ipx throughput *bits-per-second*

Syntax Description

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

Defaults

Current bandwidth setting for the interface

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

The following example changes the throughput to 1,000,000 bits per second:

```
ipx throughput 1000000
```

Related Commands

Command	Description
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.

ipx triggered-rip-delay

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

ipx triggered-rip-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

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

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

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

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

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

When you use the **no** form of the **ipx triggered-rip-delay** command, the system uses the global default delay set by the **ipx default-triggered-rip-delay** command for triggered RIP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the "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 interface FDDI 0:

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

Related Commands

Command	Description
ipx default-output-rip-delay	Sets the default interpacket delay for RIP updates sent on all interfaces.
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-holddown

To set the amount of time for which an IPX Routing Information Protocol (RIP) process will wait before sending flashes about RIP changes, use the **ipx triggered-rip-holddown** command in interface configuration mode. To remove the RIP hold-down, use the **no** form of this command.

ipx triggered-rip-holddown *milliseconds*

no ipx triggered-rip-holddown *milliseconds*

Syntax Description

milliseconds	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To set a default hold-down used for all interfaces, use the **ipx default-triggered-rip-holddown** command in global configuration mode.

Examples

The following example shows a hold-down time of 100 milliseconds:

```
interface ether 0
 ipx triggered-rip-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 default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-sap-holddown	Sets an amount of time a SAP process will wait before sending flashes about SAP changes.

ipx triggered-sap-delay

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

ipx triggered-sap-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

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

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

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

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

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

When you use the **no** form of the **ipx triggered-sap-delay** command, the system uses the global default delay set by the **ipx default-triggered-sap-delay** command for triggered SAP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the "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 interface FDDI 0:

```
interface FDDI 0
 ipx 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 default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx triggered-sap-holddown

To set the amount of time for which a Service Advertising Protocol (SAP) process will wait before sending flashes about SAP changes, use the **ipx triggered-sap-holddown** command in interface configuration mode. To remove the SAP hold-down, use the **no** form of this command.

ipx triggered-sap-holddown *milliseconds*

no ipx triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To set a default hold-down used for all interfaces, use the **ipx default-triggered-sap-holddown** command in global configuration mode.

Examples

The following example shows a hold-down time of 100 milliseconds:

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

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

ipx type-20-helpered

no ipx type-20-helpered

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

Use of the **ipx type-20-helpered** command does not comply with the Novell IPX router specification; however, you may need to use this command if you have a mixed internetwork that contains routers running Software Release 9.1 and routers running later versions of Cisco IOS software.

Examples

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

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

Related Commands

Command	Description
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.

ipx type-20-input-checks

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

ipx type-20-input-checks

no ipx type-20-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

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

Examples

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

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

Related Commands

Command	Description
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-output-checks

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

ipx type-20-output-checks

no ipx type-20-output-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

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

Examples

The following example imposes restrictions on outgoing type 20 broadcasts:

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

Related Commands

Command	Description
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-propagation

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

ipx type-20-propagation

no ipx type-20-propagation

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

Command	Description
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.

ipx update interval

To adjust the Routing Information Protocol (RIP) or Service Advertising Protocol (SAP) update interval, use the **ipx update interval** command in interface configuration mode. To restore the default values, use the **no** form of this command.

ipx update interval {**rip** | **sap**} {*value* | **changes-only**}

no ipx update interval {**rip** | **sap**}

Syntax Description

rip	Adjusts the interval at which RIP updates are sent. The minimum interval is 10 seconds.
sap	Adjusts the interval at which SAP updates are sent. The minimum interval is 10 seconds.
value	The interval specified in seconds.
changes-only	Specifies the sending of a SAP or RIP update when the link comes up, when the link is downed administratively, or when service information changes. This parameter is supported for both SAP and RIP updates.

Defaults

The default interval is 60 seconds for both IPX routing updates and SAP updates.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command replaces two commands found in previous releases of Cisco IOS software: **ipx sap-interval** and **ipx update-time**.

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

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

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

- IPX routes are marked invalid if no routing updates are heard within three times the value of the update interval and are advertised with a metric of infinity.
- IPX routes are removed from the routing table if no routing updates are heard within four times the value of the update interval.

Setting the interval at which SAP updates are sent is most useful on limited-bandwidth links, such as slower-speed serial interfaces.

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

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

You can set the router to send an update only when changes have occurred. Using the **changes-only** keyword specifies the sending of a SAP update only when the link comes up, when the link is downed administratively, or when the databases change. The **changes-only** keyword causes the router to do the following:

- Send a single, full broadcast update when the link comes up.
- Send appropriate triggered updates when the link is shut down.
- Send appropriate triggered updates when specific service information changes.

Examples

The following example configures the update timers for RIP updates on two interfaces in a router:

```
interface serial 0
 ipx update interval rip 40

interface ethernet 0
 ipx update interval rip 20
```

The following example configures SAP updates to be sent (and expected) on serial interface 0 every 300 seconds (5 minutes) to reduce periodic update overhead on a slow-speed link:

```
interface serial 0
 ipx update interval sap 300
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx update sap-after-rip

To configure the router to send a Service Advertising Protocol (SAP) update immediately following a Routing Information Protocol (RIP) broadcast, use the **ipx update sap-after-rip** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx update sap-after-rip

no ipx update sap-after-rip

Syntax Description

This command has no arguments or keywords.

Defaults

RIP and SAP updates are sent every 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **ipx update sap-after-rip** command causes the router to issue a SAP update immediately following a RIP broadcast. This ensures that the SAP update follows the RIP broadcast, and that the SAP update is sent using the RIP update interval. It also ensures that the receiving router has learned the route to the service interface via RIP prior to getting the SAP broadcast.

Examples

The following example configures the router to issue a SAP broadcast immediately following a RIP broadcast on serial interface 0.

```
interface serial 0
 ipx update sap-after-rip
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx update interval	Adjusts the RIP or SAP update interval.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx watchdog

To enable watchdog, use the **ipx watchdog** command in interface configuration mode. To specify filtering, spoofing, or how long spoofing is to be enabled or disabled, use arguments and keywords. To disable filtering or spoofing, use the **no** form of this command.

ipx watchdog {**filter** | **spoof** [*enable-time-hours disable-time-minutes*]}

no ipx watchdog {**filter** | **spoof**}

Syntax Description

filter	Discards IPX server watchdog packets when a DDR link is not connected.
spoof	Answers IPX server watchdog packets when a DDR link is not connected.
enable-time-hours	(Optional) Number of consecutive hours spoofing is to stay enabled. Values are 1 through 24.
disable-time-minutes	(Optional) Number of consecutive minutes spoofing is to stay disabled. Values are 18 through 1440.

Defaults

There is no watchdog processing.

Command Modes

Interface configuration

Command History

Release	Modification
11.2(9.1)	This command was introduced. This command replaces the **ipx watchdog-spoof** command.

Usage Guidelines

Use the **ipx watchdog** command when you want to enable watchdog processing. Use this command only on a serial interface with dial-on-demand (DDR) routing enabled.

Using the **filter** keyword when the DDR link is not connected will cause IPX server watchdog packets to be discarded, preventing them from bringing the DDR link up again.

Using the **spoof** keyword will allow IPX server watchdog packets to be answered when the DDR link is not connected. You can control how long spoofing is to be enabled or disabled by using the *enable-time-hours* and *disable-time-minutes* arguments.

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.

ipx watchdog-spoof

The **ipx watchdog-spoof** command is replaced by the **ipx watchdog** command. See the description of the **ipx watchdog** command in this chapter for more information.

log-adjacency-changes (IPX)

To generate a log message when an NetWare Link-Services Protocol (NLSP) adjacency changes state (up or down), use the **log-adjacency-changes** command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

Defaults

Adjacency changes are not logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command allows the monitoring of NLSP adjacency state changes. Adjacency state monitoring can be very useful when monitoring large networks. Messages are logged using the system error message facility. Messages are of the form:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

Messages regarding the use of NLSP multicast and broadcast addressing are also logged. For example, if broadcast addressing is in use on Ethernet interface 1.2, and the last neighbor requiring broadcasts goes down, the following messages will be logged:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Down, hold time expired
%CLNS-5-MULTICAST: NLSP: Multicast address in use on Ethernet1.2
```

If multicast addressing is in use and a new neighbor that supports only broadcast addressing comes up, the following messages will be logged:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Up, new adjacency
%CLNS-5-MULTICAST: NLSP Broadcast address is in use on Ethernet1.2
```

Examples

The following example instructs the router to log adjacency changes for the NLSP process area1:

```
ipx router nlsp area1
 log-adjacency-changes
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

log-neighbor-changes (EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **log-neighbor-changes** command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

No adjacency changes are logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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

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

where the arguments have the following meanings:

as-number	Autonomous system number
address (interface)	Neighbor address
state	Up or down
reason	Reason for change

Examples

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

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

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

lsp-gen-interval (IPX)

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

lsp-gen-interval *seconds*

no lsp-gen-interval *seconds*

Syntax Description

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

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

lsp-mtu (IPX)

To set the maximum size of a link-state packet (LSP) generated by Cisco IOS software, use the **lsp-mtu** command in router configuration mode. To restore the default Maximum Transmission Unit (MTU) size, use the **no** form of this command.

lsp-mtu *bytes*

no lsp-mtu *bytes*

Syntax Description

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

Defaults

512 bytes

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

```
lsp-mtu 1500
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

lsp-refresh-interval (IPX)

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

lsp-refresh-interval *seconds*

no lsp-refresh-interval *seconds*

Syntax Description

seconds	Refresh interval, in seconds. It can be a value in the range 1 to 50,000 seconds. The default is 7200 seconds (2 hours).

Defaults

7200 seconds (2 hours)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

Examples

The following example changes the LSP refresh interval to 10,800 seconds (3 hours):

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

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
max-lsp-lifetime (IPX)	Sets the maximum time that LSPs persist without being refreshed.

max-lsp-lifetime (IPX)

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

max-lsp-lifetime [**hours**] *value*

no max-lsp-lifetime

Syntax Description

hours	(Optional) If specified, the lifetime of the LSP is set in hours. If not specified, the lifetime is set in seconds.
value	Lifetime of LSP, in hours or seconds. It can be a number in the range 1 to 32,767. The default is 7500 seconds.

Defaults

7500 seconds (2 hours, 5 minutes)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **hours** keyword enables the router to interpret the maximum lifetime field in hours, allowing the router to keep LSPs for a much longer time. Keeping LSPs longer reduces overhead on slower-speed serial links and keeps ISDN links from becoming active unnecessarily.

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

Examples

The following example sets the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

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

The following example sets the maximum time that the LSP persists to 15 hours:

```
max-lsp-lifetime hours 15
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
lsp-refresh-interval (IPX)	Sets the LSP refresh interval.

multicast

To configure the router to use multicast addressing, use the **multicast** command in router configuration mode. To configure the router to use broadcast addressing, use the **no** form of this command.

multicast

no multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast addressing is enabled.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command allows the router to use NetWare Link-Services Protocol (NLSP) multicast addressing. If an adjacent neighbor does not support NLSP multicast addressing, the router will revert to using broadcasts on the affected interface.

The router will also revert to using broadcasts on any interface where multicast addressing is not supported by the hardware or driver.

Examples

The following example disables multicast addressing on the router:

```
ipx router nlsp
 no multicast
```

netbios access-list (IPX)

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

netbios access-list host *name* {**deny** | **permit**} *string*

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

netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

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

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
name	Name of the access list being defined. The name can be an alphanumeric string.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
string	Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument *string* can include the following wildcard characters: • *—Matches one or more characters. You can use this wildcard character only at the end of a string. • ?—Matches any single character.
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.
offset	Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.
byte-pattern	Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument *byte-pattern* can include the double asterisk (**) wildcard character to match any digits for that byte.

Defaults

No filters are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Keep the following points in mind when configuring IPX NetBIOS access control:

- Host (node) names are case-sensitive.
- Host and byte access lists can have the same names. They are independent of each other.
- When filtering by node name for IPX NetBIOS, the names in the access lists are compared with the destination name field for IPX NetBIOS "find name" requests.
- When filtering by byte offset, note that these access filters can have a significant impact on the packets' transmission rate across the bridge because each packet must be examined. You should use these access lists only when absolutely necessary.
- If a node name is not found in an access list, the default action is to deny access.

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

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

no netbios access-list {**host** | **bytes**} *name*

To delete a single entry from the list, use the following command:

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

Examples

The following example defines the IPX NetBIOS access list engineering:

```
netbios access-list host engineering permit eng-ws1 eng-ws2 eng-ws3
```

The following example removes a single entry from the engineering access list:

```
netbios access-list host engineering deny eng-ws3
```

The following example removes the entire engineering NetBIOS access list:

```
no netbios access-list host engineering
```

Related Commands

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

network (IPX Enhanced IGRP)

To enable Enhanced Interior Gateway Routing Protocol (EIGRP), use the **network** (IPX Enhanced IGRP) command in router configuration mode. To disable Enhanced IGRP, use the **no** form of this command.

network {*network-number* | **all**}

no network {*network-number* | **all**}

Syntax Description

network-number	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use the **network** (IPX Enhanced IGRP) command to enable the routing protocol specified in the **ipx router** command on each network.

Examples

The following commands disable RIP on network 10 and enable Enhanced IGRP on networks 10 and 20:

```
ipx router rip
 no network 10

ipx router eigrp 12
 network 10
 network 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

permit (IPX extended)

To set conditions for a named IPX extended access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the keyword **any** to match all protocol types.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.
source-socket	Socket name or number (hexadecimal) from which the packet is being sent. You can also use the word **all** to match all sockets.

destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

There is no specific condition under which a packet passes the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX protocol names and numbers, and IPX socket names and numbers, see the **access-list** (IPX extended) command.

Examples

The following example creates an extended access list named *sal* that denies all SPX packets and permits all others:

```
ipx access-list extended sal
 deny spx any all any all log
 permit any
```

The following example provides a time range to permit access:

```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (IPX standard)

To set conditions for a named IPX access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

no permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

Syntax Description

source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples

The following example creates a standard access list named *fred*. It permits communication with only IPX network number 5678.

```
ipx access-list standard fred
 permit 5678 any
 deny any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (NLSP)

To allow explicit route redistribution in a named NetWare Link-Services Protocol (NLSP) route aggregation access list, use the **permit** command in access-list configuration mode. To remove a permit condition, use the **no** form of this command.

permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

no permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description

network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary, expressed as an eight-digit hexadecimal number. The high-order bits specified for the *network-mask* argument must be contiguous 1s, while the low-order bits must be contiguous zeros (0). An arbitrary mix of 1s and 0s is not permitted.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which networks that are permitted by the access list entry can be redistributed as explicit networks, without summarization.

For additional information on creating access lists that deny or permit area addresses that summarize routes, see the **access-list** (NLSP route aggregation summarization) command.

Examples

The following example allows networks 12345600 and 12345601 to be redistributed explicitly. Other routes in the range 12345600 to 123456FF are summarized into a single aggregated route. All other routes will be redistributed as explicit routes.

```
ipx access-list summary finance
 permit 12345600
 permit 12345601
 deny 12345600 ffffff00
 permit -1
```

Related Commands

Command	Description
access-list (NLSP)	Defines an access list that denies or permits area addresses that summarize routes.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (SAP filtering)

To set conditions for a named IPX Service Advertising Protocol (SAP) filtering access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no permit *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

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

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX SAP service types, see the **access-list** (SAP filtering) command.

Examples

The following example creates a SAP access list named MyServer that allows only MyServer to be sent in SAP advertisements:

```
ipx access-list sap MyServer
 permit 1234 4 MyServer
```

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-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

prc-interval (IPX)

To control the hold-down period between partial route calculations, use the **prc-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds*

no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between partial route calculations, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **prc-interval** command controls how often Cisco IOS software can performs a partial route (PRC) calculation. The PRC calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially on slower router models. Increasing the PRC interval reduces the processor load of the router, but potentially slows down the rate of convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first calculations.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
prc-interval 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

redistribute (IPX)

To redistribute from one routing domain into another, and vice versa, use one of the following **redistribute** commands in router configuration mode. To disable this feature, use the **no** form of these commands.

For Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **nlsp** [*tag*] | **rip** | **static**}

no redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **nlsp** [*tag*] | **rip** | **static**}

For NetWare Link-Services Protocol (NLSP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute {**eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip** | **static**} [**access-list** {*access-list-number* | *name*}]

no redistribute {**eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip** | **static**} [**access-list** {*access-list-number* | *name*}]

Syntax Description

connected	Specifies connected routes.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.
nlsp [*tag*]	Specifies the NLSP protocol and, optionally, names the NLSP process (*tag*). The *tag* can be any combination of printable characters.
rip	Specifies the RIP protocol. You can configure only one RIP process on the router. Thus, you cannot redistribute RIP into RIP.
static	Specifies static routes.
access-list *access-list-number*	(Optional) Specifies an NLSP route summary access list. The *access-list-number* is a number from 1200 to 1299.
access-list *name*	(Optional) 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

Redistribution is enabled between all routing domains except between separate Enhanced IGRP processes.

Redistribution of floating static routes is disabled.

Redistribution between NLSP and Enhanced IGRP is disabled.

Command Modes Router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines Redistribution provides for routing information generated by one protocol to be advertised in another.

The only connected routes affected by this redistribute command are the routes not specified by the **network** command.

If you have enabled floating static routes by specifying the **floating** keyword in the **ipx route** global configuration command and you redistribute floating static routes into a dynamic IPX routing protocol, any nonhierarchical topology causes the floating static destination to be redistributed immediately via a dynamic protocol back to the originating router, causing a routing loop. This occurs because dynamic protocol information overrides floating static routes. For this reason, automatic redistribution of floating static routes is off by default. If you redistribute floating static routes, you should specify filters to eliminate routing loops.

For NLSP environments, you can use the NLSP **redistribute** command to configure IPX route aggregation with customized route summarization. Configure IPX route aggregation with customized route summarization in the following:

- Enhanced IGRP and NLSP version 1.1 environments
- RIP and NLSP version 1.1 environments

Note NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

An NLSP *process* is a router's databases working together to manage route information about an area. NLSP version 1.0 routers are always in the same area. Each router has its own adjacencies, link-state, and forwarding databases. These databases operate collectively as a single *process* to discover, select, and maintain route information about the area. NLSP version 1.1 routers that exist within a single area also use a single process.

NLSP version 1.1 routers that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These routers manage an adjacencies, link-state, and area address database for each area to which they attach. Collectively, these databases are still referred to as a *process*. The forwarding database is shared among processes within a router. The sharing of entries in the forwarding database is automatic when all processes interconnect NLSP version 1.1 areas.

Examples The following example does not redistributes RIP routing information:

```
ipx router eigrp 222
 no redistribute rip
```

The following example redistributes Enhanced IGRP routes from autonomous system 100 into Enhanced IGRP autonomous system 300:

```
ipx router eigrp 300
 redistribute eigrp 100
```

The following example redistributes Enhanced IGRP routes from autonomous system 300 into NLSP process area3:

```
ipx router nlsp area3
 redistribute eigrp 300
```

The following example enables route summarization and redistributes routes learned from one NLSP instance to another. Any routes learned via NLSP a1 that are subsumed by route summary aaaa0000 ffff0000 are not redistributed into NLSP a2. Instead, an aggregated route is generated. Likewise, any routes learned via NLSP a2 that are subsumed by route summary bbbb0000 ffff0000 are not redistributed into NLSP a1—an aggregated route is generated.

```
ipx routing
ipx internal-network 2000
!
interface ethernet 1
 ipx network 1001
 ipx nlsp a1 enable
!
interface ethernet 2
 ipx network 2001
 ipx nlsp a2 enable
!
access-list 1200 deny aaaa0000 ffff0000
access-list 1200 permit -1
access-list 1201 deny bbbb0000 ffff0000
access-list 1201 permit -1
!
ipx router nlsp a1
 area-address 1000 fffff000
 route-aggregation
 redistribute nlsp a2 access-list 1201
!
ipx router nlsp a2
 area-address 2000 fffff000
 route-aggregation
 redistribute nlsp a1 access-list 1200
```

Related Commands

Command	Description
access-list (NLSP)	Defines an access list that denies or permits area addresses that summarize routes.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-list	Defines an IPX access list by name.
ipx router	Specifies the routing protocol to use.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.

route-aggregation (NLSP)

To enable the generation of aggregated routes in an NetWare Link-Services Protocol (NLSP) area, use the **route-aggregation** command in router configuration mode. To disable generation, use the **no** form of this command.

route-aggregation

no route-aggregation

Syntax Description

This command has no arguments or keywords.

Defaults

Route summarization is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

When route summarization is disabled, all routes redistributed into an NLSP area will be explicit routes.

When route summarization is enabled, the router uses the access list associated with the **redistribute** command (if one exists) for the routing process associated with each route as a template for route summarization. Explicit routes that match a range denied by the access list trigger generation of an aggregated route instead. Routes permitted by the access list are redistributed as explicit routes.

If no access list exists, the router instead uses the area address (if one exists) of the routing process associated with each route as a template for route summarization. Explicit routes that match the area address trigger generation of an aggregated route instead.

Note Because an Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) routing process cannot have an area address, it is not possible to generate aggregated routes without the use of an access list.

Examples

The following example enables route summarization between two NLSP areas. Route summarization is based on the area addresses configured for each area.

```
ipx routing
ipx internal-network 123
!
interface ethernet 1
 ipx nlsp area1 enable
!
interface ethernet 2
 ipx nlsp area2 enable
```

```
!
ipx router nlsp area1
 area-address 1000 fffff000
 route-aggregation
!
ipx router nlsp area2
 area-address 2000 fffff000
 route-aggregation
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
redistribute (IPX)	Redistributes from one routing domain into another.

show ipx access-list

To display the contents of all current IPX access lists, use the **show ipx access-list** command in EXEC mode.

show ipx access-list [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the IPX access list to display. This is a number from 800 to 899, 900 to 999, 1000 to 1099, or 1200 to 1299.
name	(Optional) Name of the IPX access list to display.

Defaults

Displays all standard, extended, Service Advertising Protocol (SAP), and NetWare Link-Services Protocol (NLSP) route aggregation summary IPX access lists.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **show ipx access-list** command provides output identical to the **show access-lists** command, except that it is IPX specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ipx access-list** command when all access lists are requested:

```
Router# show ipx access-list

IPX extended access list 900
 deny any 1
IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

The following is sample output from the **show ipx access-list** command when the name of a specific access list is requested:

```
Router# show ipx access-list London

IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

show ipx accounting

To display the active or checkpoint accounting database, use the **show ipx accounting** command in EXEC mode.

show ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Displays entries in the checkpoint database.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show ipx accounting

Source                  Destination               Packets            Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72             2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14              624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62             3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20             1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20             1470

Accounting data age is     6
```

Table 50 describes the fields shown in the display.

Table 50 show ipx accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets transmitted from the source address to the destination address.
Bytes	Number of bytes transmitted from the source address to the destination address.
Accounting data age is ...	Time since the accounting database has been cleared. It can be in one of the following formats: *mm*, *hh*:*mm*, *dd*:*hh*, and *ww*:*dd*, where *m* is minutes, *h* is hours, *d* is days, and *w* is weeks.

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.