ipx sap

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap** command is not supported in Cisco IOS software.

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

ipx sap *service-type name network.node socket hop-count*

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

Syntax Description

service-type	SAP service-type number. See the **access-list** (SAP filtering) command earlier in this chapter for a table of some IPX SAP services.
name	Name of the server that provides the service.
network.node	Network number and node address of the server. The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA. The argument *node* is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
socket	Socket number for this service. See access-list (IPX extended) command earlier in this chapter for a table of some IPX socket numbers.
hop-count	Number of hops to the server.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.

Release	Modification
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
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.
show ipx servers	Lists the IPX servers discovered through SAP advertisements.

ipx sap follow-route-path

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx sap follow-route-path** command is not supported in Cisco IOS software.

To enable a router to accept IPX Service Advertising Protocol (SAP) entries from SAP updates received on an interface only if that interface is one of the best paths to reach the destination networks of those SAPs, use the **ipx sap follow-route-path** command in global configuration mode. To disable this router function, use **no** form of this command.

ipx sap follow-route-path

no ipx sap follow-route-path

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

In redundantly connected networks that use IPX-Enhanced IGRP routing in which multiple IPX paths exist, IPX SAP services can be learned on nonoptimal interfaces, causing SAP loops, also known as phantom SAPs, when those services become obsolete. Use the **ipx sap follow-route-path** command to prevent the occurrence of SAP loops.

When the **ipx sap follow-route-path** command is used, the router screens individual services (SAPs) in SAP updates. The router looks at the destination network number of each SAP entry's . If the receiving interface is one of the best interfaces to reach the destination network of the SAP, that SAP entry is accepted. Otherwise, the SAP entry is discarded.

Caution When the **ipx sap follow-route-path** command is globally enabled in conjunction with SAP input filters on interfaces that are considered the best paths to reach the destination networks, the SAPs that are being filtered will no longer be learned by the router, even if other less optimal interfaces are capable of receiving those SAP updates.

Examples

The following example enables the router to accept only the IPX SAP entries from SAP updates received on an interface deemed to be one of the best paths to the destination address of those SAPs:

```
ipx sap follow-route-path
```

Related Commands

Command	Description
ipx server-split-horizon-on-server-paths	Controls whether Service Information split horizon checking should be based on RIP or SAP.

ipx sap-helper

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-helper** command is not supported in Cisco IOS software.

To set an address, which should be another Cisco router that is adjacent to the router being configured, to which all Service Advertising Protocol (SAP) request packets are received, use the **ipx sap-helper** command in interface configuration mode. To remove the address and stop forwarding SAP request packets, use the **no** form of this command.

ipx sap-helper *network.node*

no ipx sap-helper *network.node*

Syntax Description

network.node	The argument *network* is the network on which the SAP helper router resides. This eight-digit hexadecimal number uniquely identifies a network cable segment. It can be a number in the range from 1 to FFFFFFFD. You do not need to specify the leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. The argument *node* is the node number of the SAP helper router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

Defaults

No helper address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use this command to redirect SAP packet requests that are sent to a remote router that has a limited memory size, CPU speed, and often a slow WAN link joining it to the main corporate backbone. The SAP helper target is usually much a much larger router that has a much larger routing table and a complete SAP table.

Examples

The following example assigns a router with the address 1000.0000.0c00.1234 as the SAP helper:

```
interface ethernet 0
 ipx sap-helper 1000.0000.0c00.1234
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.

ipx sap-incremental (EIGRP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-incremental (EIGRP)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-incremental split-horizon** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-max-packetsize** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-multipler** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx sap-queue-maximum** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx sap-update-queue-maximum** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, and 15.1(1)SY, the **ipx server-split-horizon-on-server-paths** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx split-horizon eigrp** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx spx-idle-time** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx spx-spoof** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx throughput** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The value you specify with the **ipx throughput** command overrides the value measured by IPXWAN when it starts.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx triggered-rip-delay** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx triggered-rip-holddown** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx triggered-sap-delay** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx triggered-sap-holddown** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-helpered** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-input-checks** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-output-checks** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx type-20-propagation** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx update interval** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx update sap-after-rip** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx watchdog** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-adjaceny-changes (IPX)** command is not supported in Cisco IOS software.

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.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-neighbor-changes (EIGRP)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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 EIGRP process 209:

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

log-neighbor-warnings

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-neighbor-warnings** command is not supported in Cisco IOS software.

Note Effective with Cisco IOS Release 15.0(1)M, 12.2(33)SRE and Cisco IOS XE Release 2.5, the **log-neighbor-warnings** command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

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

log-neighbor-warnings [*seconds*]

no log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 through 65535.

Command Default Neighbor warning messages are logged.

Command Modes Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
12.2(33)SRE	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
Cisco IOS XE Release 2.5	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With the **log-neighbor-warnings** command, you can disable and enable the logging of neighbor warning messages and configure the interval between repeated neighbor warning messages.

Examples

The following example shows that neighbor warning messages will be logged for EIGRP process 1 and warning messages will be repeated in 5-minute (300 seconds) intervals:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# log-neighbor-warnings 300
```

Related Commands

Command	Description
log-neighbor-changes	Enables the logging of changes in EIGRP neighbor adjacencies.

lsp-gen-interval (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-gen-interval (IPX)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-mtu (IPX)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-refresh-interval (IPX)** command is not supported in Cisco IOS software.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **max-lsp-lifetime (IPX)** command is not supported in Cisco IOS software.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **multicast** command is not supported in Cisco IOS software.

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.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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
```

nasi authentication

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **nasi authentication** command is not supported in Cisco IOS software.

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

nasi authentication {**default** | *list-name*}

no nasi authentication {**default** | *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication nasi** command.
list-name	Uses the list created with the **aaa authentication nasi** command.

Defaults

Uses the default set with the **aaa authentication nasi** command.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi** command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1* be used on line 7:

```
line 7
 nasi authentication list1
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

netbios access-list (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **netbios access-list (IPX)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **network (IPX Enhanced IGRP)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (IPX extended)** command is not supported in Cisco IOS software.

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*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (IPX standard)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (NLSP)** command is not supported in Cisco IOS software.

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.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (SAP filtering)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **prc-interval (IPX)** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **redistribute (IPX)** command is not supported in Cisco IOS software.

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** | **rip** | **static**}

no redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

Syntax Description

connected	Specifies connected routes.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a 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.
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 *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.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	The **access-list** keyword and *access-list-number* argument have been removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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.

- Enhanced IGRP version 1.1 environments
- RIP version 1.1 environments

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
```

Related Commands

Command	Description
ipx access-list	Defines an IPX access list by name.
ipx router	Specifies the routing protocol to use.

route-aggregation (NLSP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **route-aggregation (NLSP)** command is not supported in Cisco IOS software.

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.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx access-list** command is not supported in Cisco IOS software.

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, and Service Advertising Protocol (SAP) IPX access lists.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx accounting** command is not supported in Cisco IOS software.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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 13 describes the fields shown in the display.

Table 13 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.

show ipx cache

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx cache** command is not supported in Cisco IOS software.

To display the contents of the IPX fast-switching cache, use the **show ipx cache** command in EXEC mode.

show ipx cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx cache

Novell routing cache version is 9
Destination          Interface              MAC Header
*1006A               Ethernet 0             00000C0062E600000C003EB0064
*14BB                Ethernet 1             00000C003E2A00000C003EB0064
```

Table 14 describes the fields shown in the display.

Table 14 show ipx cache Field Descriptions

Field	Description
Novell routing cache version is ...	Number identifying the version of the fast-switching cache table. It increments each time the table changes.
Destination	Destination network for this packet. Valid entries are marked by an asterisk (*).
Interface	Route interface through which this packet is transmitted.
MAC Header	Contents of this packet's MAC header.

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
ipx route-cache	Enables IPX fast switching.

show ipx eigrp interfaces

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp interfaces** command is not supported in Cisco IOS software.

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp interfaces** command in EXEC mode.

show ipx eigrp interfaces [*type number*] [*as-number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
as-number	(Optional) Autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **show ipx eigrp interfaces** command to determine on which interfaces Enhanced IGRP is active and to find out information about Enhanced IGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which Enhanced IGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all Enhanced IGRP processes are displayed.

Examples

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

```
Router> show ipx eigrp interfaces

IPX EIGRP interfaces for process 109
```

```
                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

Table 15 describes the fields shown in the display.

Table 15 show ipx eigrp interfaces Field Descriptions

Field	Description
process 109	Autonomous system number of the process.
Interface	Interface name.
Peers	Number of neighbors on the interface.
Xmit Queue	Count of unreliable and reliable packets queued for transmission.
Mean SRTT	Average round-trip time for all neighbors on the interface.
Pacing Time	Number of milliseconds to wait after transmitting unreliable and reliable packets.
Multicast Flow Timer	Number of milliseconds to wait for acknowledgment of a multicast packet by all neighbors before transmitting the next multicast packet.
Pending Routes	Number of routes still to be transmitted on this interface.

Related Commands

Command	Description
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

show ipx eigrp neighbors

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp neighbors** command is not supported in Cisco IOS software.

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipx eigrp neighbors [**servers**] [**detail** | *interface interface-number*] [**regexp** *name*]

Syntax Description

servers	(Optional) Displays the server list advertised by each neighbor. This list is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
detail	(Optional) Displays detailed peer information.
interface	(Optional) Specifies the type of interface.
interface-number	(Optional) Specifies the interface number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The following keyword and argument were added: • **regexp** • *name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **regexp** and **servers** keywords were removed. The *name* argument was removed.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use **show ipx eigrp neighbors** command to display the neighbors discovered by EIGRP.

Examples

The following are sample outputs of **show ipx eigrp neighbors** commands:

```
Router# show ipx eigrp neighbors

EIGRP-IPX Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.aabb.cc00.0e00       Et0/0             12 00:01:17  166   996  0  4
0   10.aabb.cc00.0a00       Et0/0             12 00:01:19  173  1038  0  9

Router# show ipx eigrp neighbors detail

EIGRP-IPX Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.aabb.cc00.0e00       Et0/0             14 00:01:20  166   996  0  4
   Version 5.0/3.0, Retrans: 0, Retries: 0, Prefixes: 1
   Topology-ids from peer - 0
0   10.aabb.cc00.0a00       Et0/0             14 00:01:22  173  1038  0  9
   Version 5.0/3.0, Retrans: 0, Retries: 0, Prefixes: 1
   Topology-ids from peer - 0
```

Table 16 describes the fields shown in the display.

Table 16 show ipx eigrp neighbors Field Descriptions

Field	Description
AS()	Autonomous system number specified in the **ipx router** configuration command.
H	Handle. An arbitrary and unique number inside this router that identifies the neighbor.
Address	IPX address of the Enhanced IGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time, in seconds, that Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.
Uptime	Elapsed time (in hours, minutes, and seconds) since the local router first heard from this neighbor.

Table 16 show ipx eigrp neighbors Field Descriptions (continued)

Field	Description
Q Cnt	Number of IPX Enhanced IGRP packets (Update, Query, and Reply) that Cisco IOS software is waiting to send.
Seq Num	Sequence number of the last Update, Query, or Reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds it takes for an IPX Enhanced IGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. This is the amount of time Cisco IOS software waits before retransmitting a packet from the retransmission queue to a neighbor.
Type	Contains codes from the Codes field to indicates how service was learned.

Related Commands

Command	Description
ipx sap-incremental	Sends SAP updates only when a change occurs in the SAP table.

show ipx eigrp topology

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp topology** command is not supported in Cisco IOS software.

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show ipx eigrp topology** command in user EXEC mode or privileged EXEC mode.

show ipx eigrp topology [*network-number* [*ipx-network-mask*] | **active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors** | **base** [*network-number* [*ipx-network-mask*] | **active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors** | **accounting** | **events** [[**errmsg** | **sia**] [*start-event-number end-event-number*] | **type**]]]

Syntax Description

network-number	(Optional) Specifies the IPX network number whose topology table entry is displayed. Specifies the base IPX network number of the topology table when used with the **base** keyword.
ipx-network-mask	(Optional) Specifies the IPX network mask. Specifies the base IPX network mask when used with the **base** keyword.
active	(Optional) Displays only the active topology entries. Displays active base topology entries when used with the **base** keyword.
all-links	(Optional) Displays summary information of all entries in the EIGRP topology table. Displays the base summary information of all entries in the EIGRP topology table when used with the **base** keyword.
detail-links	(Optional) Displays detailed information about all entries in the EIGRP topology table. Displays detailed base information about all entries in the EIGRP topology table when used with the **base** keyword.
pending	(Optional) Displays all entries in the EIGRP topology table that are eiher waiting for an update from a neighbor or waiting to reply to a neighbor. Displays the base events pending for transmission when used with the **base** keyword.
summary	(Optional) Displays a summary of the EIGRP topology table. Displays the base summary of the EIGRP topology table when used with the **base** keyword.
zero-successors	(Optional) Displays available routes in the EIGRP topology table. Displays the available base routes in the EIGRP topology table when used with the **base** keyword.
base	(Optional) Specifies the base topology.
accounting	(Optional) Specifies the accounting prefix of the base topology.
events	(Optional) Specifies the base topology logged events.
start-event-number	(Optional) Specifies the starting event number.

errmsg	(Optional) Displays the logged error messages.
end-event-number	Specifies the ending event number.
sia	(Optional) Displays the stuck in active (sia) logged events.
type	(Optional) Displays the type of the logged events.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE. This command was modified. The **accounting**, **base**, **errmsg**, **events, sia**, and **type** keywords were removed. The *start-event-number* and *end-event-number* arguments were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output of **show ipx eigrp topology** command:

```
Router# show ipx eigrp topology

IPX EIGRP Topology Table for process 109
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 42, 1 successors, FD is 0
   via 160.0000.0c00.8ea9 (345088/319488), Ethernet0
P 160, 1 successor via Connected, Ethernet
   via 160.0000.0c00.8ea9 (307200/281600), Ethernet0
P 165, 1 successors, FD is 307200
   via Redistributed (287744/0)
   via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
P 164, 1 successors, flags: U, FD is 200
   via 160.0000.0c00.8ea9 (307200/281600), Ethernet1
   via 160.0000.0c01.2b71 (332800/307200), Ethernet1
P A112, 1 successors, FD is 0
   via Connected, Ethernet2
   via 160.0000.0c00.8ea9 (332800/307200), Ethernet0
P AAABBB, 1 successors, FD is 10003
   via Redistributed (287744/0),
   via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
A A112, 0 successors, 1 replies, state: 0, FD is 0
   via 160.0000.0c01.2b71 (307200/281600), Ethernet1
   via 160.0000.0c00.8ea9 (332800/307200), r, Ethernet1
```

Table 17 describes the fields shown in the display.

Table 17 show ipx eigrp topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the Enhanced IGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No Enhanced IGRP computations are being performed for this destination.
A – Active	Enhanced IGRP computations are being performed for this destination.
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set after Cisco IOS software has sent a query and is waiting for a reply.
42, 160, and so on	Destination IPX network number.
successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
FD	Feasible distance. This value is used in the feasibility condition check. If the neighbor's reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the router determines it has a feasible successor, it does not have to send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
via	IPX address of the peer who told Cisco IOS software about this destination. The first *n* of these entries, where *n* is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(345088/319488)	The first number is the Enhanced IGRP metric that represents the cost to the destination. The second number is the Enhanced IGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.

The following are sample outputs from the **show ipx eigrp topology** command when an IPX network number is specified:

Internal EIGRP IPX Network: Example

```
Router# show ipx eigrp topology BB

EIGRP-IPX Topology Entry for AS(2)/ID(0.aabb.cc01.f600) for BB
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
  Descriptor Blocks:
  AA.aabb.cc01.f500 (Ethernet0/0), from AA.aabb.cc01.f500, Send flag is 0x0
      Composite metric is (409600/128256), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

External EIGRP IPX Network: Example

```
Router# show ipx eigrp topology CC

EIGRP-IPX Topology Entry for AS(2)/ID(0.aabb.cc01.f600) for CC
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
  Descriptor Blocks:
  AA.aabb.cc01.f500 (Ethernet0/0), from AA.aabb.cc01.f500, Send flag is 0x0
      Composite metric is (409600/128256), route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is  aabb.cc01.f500
        AS number of route is 0
        External protocol is RIP, external metric is 1
        Administrator tag is 0 (0x00000000)
```

Table 18 describes the fields shown in the display.

Table 18 show ipx eigrp topology Field Descriptions—Specific Network

Field	Description
BB, CC	IPX network number of the destination.
State is ...	State of this entry. It can be either Passive or Active. Passive means that no Enhanced IGRP computations are being performed for this destination, and Active means that they are being performed.
Query origin flag	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
Successor(s)	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
Ethernet0	Interface from which this information was learned.

Table 18 show ipx eigrp topology Field Descriptions—Specific Network (continued)

Field	Description
from	Peer from whom the information was learned. For connected and redistributed routers, this is 0.0000.0000.0000. For information learned via Enhanced IGRP, this is the peer's address. Currently, for information learned via Enhanced IGRP, the peer's IPX address always matches the address in the "Next hop is" field.
Composite metric is	Enhanced IGRP composite metric. The first number is this device's metric to the destination, and the second is the peer's metric to the destination.
Send flag	Numeric representation of the "flags" field described in Table 16. It is 0 when nothing is being sent, 1 when an Update is being sent, 3 when a Query is being sent, and 4 when a Reply is being sent. Currently, 2 is not used.
Route is ...	Type of router. It can be either internal or external. Internal routes are those that originated in an Enhanced IGRP autonomous system, and external are routes that did not. Routes learned through RIP are always external.
This is an ignored route	Indicates that this path is being ignored because of filtering.
Vector metric:	This section describes the components of the Enhanced IGRP metric.
Minimum bandwidth	Minimum bandwidth of the network used to reach the next hop.
Total delay	Delay time to reach the next hop.
Reliability	Reliability value used to reach the next hop.
Load	Load value used to reach the next hop.
Minimum MTU	Minimum MTU size of the network used to reach the next hop.
Hop count	Number of hops to the next hop.
External data:	This section describes the original protocol from which this route was redistributed. It appears only for external routes.
Originating router	Network address of the router that first distributed this route into Enhanced IGRP.
External protocol..metric..delay	External protocol from which this route was learned. The metric will match the external hop count displayed by the **show ipx route** command for this destination. The delay is the external delay.
Administrator tag	Not currently used.
Flag	Not currently used.

show ipx eigrp traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp traffic** command is not supported in Cisco IOS software.

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received, use the **show ipx eigrp traffic** command in privileged EXEC mode.

show ipx eigrp *autonomous-system-number* **traffic**

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx eigrp 2 traffic

EIGRP-IPX Traffic Statistics for AS(2)
  Hellos sent/received: 7454/2507
  Updates sent/received: 20/20
  Queries sent/received: 1/17
  Replies sent/received: 9/1
  Acks sent/received: 22/27
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 199
  PDM Process ID: 171
  Socket Queue: 0 (current)
  Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

Table 19 describes the significant fields shown in the display.

Table 19 show ipx eigrp traffic Field Descriptions

Field	Description
AS	Autonomous system number specified in the **ip router** command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

show ipx interface

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx interface** command is not supported in Cisco IOS software.

To display the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show ipx interface** command in EXEC mode.

show ipx interface [*type number*]

Syntax Description

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to add Get General Service (GGS) filters and some counters per interface.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx interface serial 2/0

Serial2/0 is up, line protocol is up
  IPX address is 123.00e0.1efc.0b01 [up]
  Delay of this IPX network, in ticks is 6 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 60 seconds
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is 900
  Outgoing access list is not set
  IPX helper access list is not set
```

```
SAP GGS output filter list is 1000
SAP GNS processing enabled, delay 0 ms, output filter list is not set
SAP Input filter list is not set
SAP Output filter list is not set
SAP Router filter list is not set
Input filter list is not set
Output filter list is not set
Router filter list is not set
Netbios Input host access list is not set
Netbios Input bytes access list is not set
Netbios Output host access list is not set
Netbios Output bytes access list is not set
Updates each 60 seconds aging multiples RIP:3 SAP:3
SAP interpacket delay is 55 ms, maximum size is 480 bytes
RIP interpacket delay is 55 ms, maximum size is 432 bytes
RIP response delay is not set
 Watchdog spoofing is currently enabled
      On duration 1 hour(s), 00:24:50 remaining
      Off duration 18 minute(s), 00:00:00 remaining
 SPX spoofing is disabled, idle time 60
 IPX accounting is disabled
 IPX fast switching is configured (enabled)
 RIP packets received 0, RIP packets sent 906, 0 Throttled
 RIP specific requests received 0, RIP specific replies sent 0
 RIP general requests received 0, 0 ignored, RIP general replies sent 0
 SAP packets received 0, SAP packets sent 25, 0 Throttled
 SAP GNS packets received 0,k SAP GNS replies sent 0
 SAP GGS packets received 0, 0 ignored, SAP GGS replies sent 0
```

Table 20 describes the fields shown in the display.

Table 20 show ipx interface Field Descriptions

Field	Description
Serial is ..., line protocol is...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
IPX address is ...	Network and node address of the local router interface, followed by the type of encapsulation configured on the interface and the status of the interface. See the **ipx network** command for a list of possible values.
[up]	Indicates whether IPX routing is enabled (up) or disabled (down) on the interface.
NOVELL-ETHER	Type of encapsulation being used on the interface, if any.
Delay of this IPX network, in ticks ...	Value of the ticks field (configured with the **ipx delay** command).
throughput	Throughput of the interface (configured with the **ipx spx-idle-time** interface configuration command).
link delay	Link delay of the interface (configured with the **ipx link-delay** interface configuration command).
IPXWAN processing...	Indicates whether IPXWAN processing has been enabled on this interface with the **ipx ipxwan** command.

Table 20 show ipx interface Field Descriptions (continued)

Field	Description
IPX SAP update interval	Indicates the frequency of outgoing Service Advertising Protocol (SAP) updates (configured with the **ipx update interval** command).
IPX type 20 propagation packet forwarding...	Indicates whether forwarding of IPX type 20 propagation packets (used by NetBIOS) is enabled or disabled on this interface, as configured with the **ipx type-20-propagation** command.
Incoming access list	Indicates whether an incoming access list has been configured on this interface.
Outgoing access list	Indicates whether an access list has been enabled with the **ipx access-group** command.
IPX helper access list	Number of the broadcast helper list applied to the interface with the **ipx helper-list** command.
SAP GGS output filter list	Number of the Get General Server (GGS) response filter applied to the interface with the **ipx output-ggs-filter** command.
SAP GNS processing ...	Indicates if GNS processing is enabled, what the response delay set is, and if there is any GNS output access-list configured
delay	Indicates the delay of this ipx network, represented in metric ticks for routers on this interface using the IPX RIP routing protocol.
output filter list	Number of the Get Nearest Server (GNS) response filter applied to the interface with the **ipx output-gns-filter** command.
SAP Input filter list	Number of the input SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Output filter list	Number of the output SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Router filter list	Number of the router SAP filter applied to the interface with the **ipx router-sap-filter** command.
Input filter list	Number of the input filter applied to the interface with the **ipx input-network-filter** command.
Output filter list	Number of the output filter applied to the interface with the **ipx output-network-filter** command.
Router filter list	Number of the router entry filter applied to the interface with the **ipx router-filter** command.
Netbios Input host access list	Name of the IPX NetBIOS input host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Input bytes access list	Name of the IPX NetBIOS input bytes filter applied to the **ipx netbios input-access-filter** interface with the **ipx netbios input-access-filter bytes** command.

Table 20 show ipx interface Field Descriptions (continued)

Field	Description
Netbios Output host access list	Name of the IPX NetBIOS output host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Output bytes access list	Name of the IPX NetBIOS output bytes filter applied to the interface with the **input netbios input-access-filter bytes** command.
Updates each ...	How often Cisco IOS software sends Routing Information Protocol (RIP) updates, as configured with the **ipx update sap-after-rip** command.
SAP interpacket delay	Interpacket delay for SAP updates.
RIP interpacket delay	Interpacket delay for RIP updates.
RIP response delay	Delay for RIP responses.
Watchdog spoofing ...	Indicates whether watchdog spoofing is enabled or disabled for this interface, as configured with the **ipx watchdog spoof** command. This information is displayed only on serial interfaces.
SPX spoofing ...	Indicates whether SPX spoofing is enabled or disabled for this interface.
IPX accounting	Indicates whether IPX accounting has been enabled with the **ipx accounting** command.
IPX fast switching IPX autonomous switching	Indicates whether IPX fast switching is enabled (default) or disabled for this interface, as configured with the **ipx route-cache** command. (If IPX autonomous switching is enabled, it is configured with the **ipx route-cache cbus** command.)
RIP packets received, RIP packets sent, Throttled	Number of RIP packets received, sent, or dropped.
RIP specific requests received, RIP specific replies sent,	Number of RIP specific requests received and the number of RIP specific replies sent.
RIP general requests received, ignored, RIP general replies sent	Number of RIP general requests received and ignored. Number of RIP general replies sent.
SAP GNS packets received, SAP GNS packets sent, Throttled	Number of SAP Get Nearest Server (GNS) packets received, sent, or dropped.
SAP GGS packets received, SAP GGS packets sent, Throttled	Number of SAP Get General Server (GGS) packets received, sent, or dropped.
SAP packets received, SAP packets sent, Throttled	Number of SAP packets received, sent, or dropped.

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
access-list (IPX standard)	Defines a standard IPX access list.
ipx accounting	Enables IPX accounting.

Command	Description
ipx default-output-rip delay	Sets the default interpacket delay for RIP updates sent on all interfaces.
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx delay	Sets the tick count.
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
ipx netbios output-access-filter	Controls outgoing IPX NetBIOS FindName messages.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-network-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx output-sap-filter	Controls which services are included in SAP updates sent by Cisco IOS software.
ipx route-cache	Enables IPX fast switching.
ipx router-filter	Filters the routers from which packets are accepted.
ipx router-sap-filter	Filters SAP messages received from a particular router.
ipx routing	Enables IPX routing.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
ipx watchdog	Enables watchdog processing.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.

show ipx nasi connections

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nasi connections** command is not supported in Cisco IOS software.

To display the status of NetWare Asynchronous Services Interface (NASI) connections, use the **show ipx nasi connections** command in EXEC mode.

show ipx nasi connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **show ipx nasi connections** command to view the addresses of remote NASI clients local connection addresses and status bits. If the connection is associated with a tty port then the `Connected to` line field appears in the **show ipx nasi connections** output.

Examples

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

```
Router# show ipx nasi connections

NASI Remote: A001500::0020.afe5.3ec5:626C   Local: ACBB::0000.0000.0001:2010
  flags 0

NASI Remote: A001500::0020.afe5.3ec5:6E6C   Local: ACBB::0000.0000.0001:20D0
  flags 0
   Connected to line 2  incount 0  outcount 0  OVF 0
```

The following sample display shows an incoming NASI connection on tty line 2:

```
Router# show users
```

```
    Line     User      Host(s)              Idle Location
*   0 con 0            idle                    1
    2 tty 2  chris     incoming                1 A001500.0020.afe5.3ec5
```

Table 21 describes the significant fields shown in the display.

Table 21 show ipx nasi connections Field Descriptions

Field	Description
NASI Remote	• xxxxxxx::yyyyyyyyy:zzzz is the address for the remote NASI client connected to the router. • xxxx is the Internetwork Packet Exchange (IPX) network number. • yyyyyyy is the IPX host node (MAC address) for the client. • zzzz is the SPX connection number.
Local	xxxxxxx::yyyyyyyyyy:zzzz is the local address associated with this connection on the router end of the link.
flags	A status bit that is used internally to allow and close connections.
Connected to line 2	Appears only when the connection is associated with a tty port. Indicates that this NASI connection is attached to tty 2.
incount 0	Data from the remote client.
outcount 0	Data to be sent to the remote client.
OVF 0	Refers to the number of times data could not be written to the tty line, because the buffers were full. Ideally, this counter should stay at 0.

Related Commands

Command	Description
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

show ipx nhrp

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nhrp** command is not supported in Cisco IOS software.

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ipx nhrp** command in EXEC mode.

show ipx nhrp [**dynamic** | **static**] [*type number*]

Syntax Description

dynamic	(Optional) Displays only the dynamic (learned) IPX-to-NBMA address cache entries.
static	(Optional) Displays only the static IPX-to-NBMA address entries in the cache (configured through the **ipx nhrp map** command).
type	(Optional) Interface type for which to display the NHRP cache. Valid options are **atm**, **serial**, and **tunnel**.
number	(Optional) Interface number for which to display the NHRP cache.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx nhrp

1.0000.0c35.de01, Serial1 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: c141.0001.0001
```

```
1.0000.0c35.e605, Serial1 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: c141.0001.0002
```

Table 22 describes the fields shown in the display.

Table 22 show ipx nhrp Field Descriptions

Field	Description
1.0000.0c35.de01	IPX address in the IPX-to-NBMA address cache.
Serial1 created 0:00:43	Interface type and number and how long ago it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ipx nhrp holdtime** command.
Type	Value can be one of the following: • dynamic—NBMA address was obtained from NHRP Request packet. • static—NBMA address was statically configured.
Flags	Value can be one of the following: • authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IPX address mapping for a particular destination. • implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router. • negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.
NBMA address	Nonbroadcast, multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, SMDS, multipoint tunnel).

Related Commands

Command	Description
ipx nhrp map	Statically configures the IPX-to-NBMA address mapping of IPX destinations connected to an NBMA network.

show ipx nhrp traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nhrp traffic** command is not supported in Cisco IOS software.

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ipx nhrp traffic** command in EXEC mode.

show ipx nhrp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx nhrp traffic

Tunnel0
  request packets sent: 2
  request packets received: 4
  reply packets sent: 4
  reply packets received: 2
  register packets sent: 0
  register packets received: 0
  error packets sent: 0
  error packets received: 0
```

Table 23 describes the fields shown in the display.

Table 23 show ipx nhrp traffic Field Descriptions

Field	Description
Tunnel 0	Interface type and number.
request packets sent	Number of NHRP Request packets originated from this station.
request packets received	Number of NHRP Request packets received by this station.
reply packets sent	Number of NHRP Reply packets originated from this station.
reply packets received	Number of NHRP Reply packets received by this station.
register packets sent	Number of NHRP Register packets originated from this station. Currently, our routers do not send Register packets, so this value is 0.
register packets received	Number of NHRP Register packets received by this station. Currently, our routers do not send Register packets, so this value is 0.
error packets sent	Number of NHRP Error packets originated by this station.
error packets received	Number of NHRP Error packets received by this station.

show ipx nlsp database

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp database** command is not supported in Cisco IOS software.

To display the entries in the link-state packet (LSP) database, use the **show ipx nlsp database** command in EXEC mode.

show ipx nlsp [*tag*] **database** [*lspid*] [**detail**]

Syntax Description

tag	(Optional) Names the NLSP process. The *tag* can be any combination of printable characters.
lspid	(Optional) Link-state protocol ID (LSPID). You must specify this in the format *xxxx.xxxx.xxxx.yy-zz*. The components of this argument have the following meaning: • *xxxx.xxxx.xxxx* is the system identifier. • *yy* is the pseudo identifier. • *zz* is the LSP number.
detail	(Optional) Displays the contents of the LSP database entries. If you omit this keyword, only a summary display is shown.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When you specify an NLSP *tag*, the router displays the link-state packet database entries for that NLSP process. 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.

Configure multiple NLSP processes when a router interconnects multiple NLSP areas.

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.

If you omit all options, a summary display is shown.

Examples

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

```
Router# show ipx nlsp database detail

LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.3097.00-00* 0x00000042   0xC512        699           0/0/0
0000.0C00.3097.06-00* 0x00000027   0x0C27        698           0/0/0
0000.0C02.7471.00-00  0x0000003A   0x4A0F        702           0/0/0
0000.0C02.7471.08-00  0x00000027   0x0AF0        702           0/0/0
0000.0C02.7471.0A-00  0x00000027   0xC589        702           0/0/0
0000.0C02.747D.00-00  0x0000002E   0xC489        715           0/0/0
0000.0C02.747D.06-00  0x00000027   0xEEFE        716           0/0/0
0000.0C02.747D.0A-00  0x00000027   0xFE38        716           0/0/0
0000.0C02.74AB.00-00  0x00000035   0xE4AF        1059          0/0/0
0000.0C02.74AB.0A-00  0x00000027   0x34A4        705           0/0/0
0000.0C06.FBEE.00-00  0x00000038   0x3838        1056          0/0/0
0000.0C06.FBEE.0D-00  0x0000002C   0xD248        1056          0/0/0
0000.0C06.FBEE.0E-00  0x0000002D   0x7DD2        1056          0/0/0
0000.0C06.FBEE.17-00  0x00000029   0x32FB        1056          0/0/0

0000.0C00.AECC.00-00* 0x000000B6   0x62A8        7497          0/0/0
  IPX Area Address: 00000000 00000000
  IPX Mgmt Info 87.0000.0000.0001  Ver 1  Name oscar
  Metric: 45 Lnk 0000.0C00.AECC.06  MTU 1500  Dly 8000  Thru 64K  PPP
  Metric: 20 Lnk 0000.0C00.AECC.02  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
  Metric: 20 Lnk 0000.0C01.EF90.0C  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
0000.0C00.AECC.02-00* 0x00000002   0xDA74        3118          0/0/0
  IPX Mgmt Info E0.0000.0c00.aecc  Ver 1  Name Ethernet0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  802.3 Raw
0000.0C00.AECC.06-00* 0x00000002   0x5DB9        7494          0/0/0
  IPX Mgmt Info 0.0000.0000.0000  Ver 1  Name Serial0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  PPP
  Metric: 1  IPX Ext D001  Ticks 0
  Metric: 1  IPX SVC Second-floor-printer  D001.0000.0000.0001  Sock 1  Type 4
```

Table 24 describes the fields shown in the display.

Table 24 show ipx nlsp database Field Descriptions

Field	Description
LSPID	System ID (network number), pseudonode circuit identifier, and fragment number.
LSP Seq Num	Sequence number of this LSP.
LSP Checksum	Checksum of this LSP.
LSP Holdtime	Time until this LSP expires, in hours or seconds.
ATT/P/OL	Indicates which of three bits are set. A "1" means the bit is set, and a "0" means it is not set. ATT is the L2-attached bit. OL is the overload bit. P is the partition repair bit. This bit is not used in NLSP.
IPX Area Address:	Area address of the router advertising the LSP.
IPX Mgmt Info	Management information. For nonpseudonode LSPs, the internal network number is advertised in this field. For pseudonode LSPs, the network number of the associated interface is advertised.
Ver	NLSP version running on the advertising router.
Name	For nonpseudonode LSPs, the name of the router. For pseudonode LSPs, the name (or description, if configured) of the associated interface.
Link Information	Information about the link.
Metric:	NLSP metric (cost) for the link. Links from a pseudonode to real nodes have a cost of 0 so that this link cost is not counted twice.
Lnk	System ID of the adjacent node.
MTU	MTU of the link in bytes. For pseudonode LSPs, the value in this field is always 0.
Dly	Delay of the link in microseconds. For pseudonode LSPs, the value in this field is always 0.
Thru	Throughput of the link in bits per second. For pseudonode LSPs, the value in this field is always 0.
802.3 Raw, Generic LAN	Link media type.
External (RIP) Networks	Information about an external (RIP) network.
Metric:	Received RIP hop count.
IPX Ext	IPX network number.
Ticks	Received RIP tick count.

Table 24 show ipx nlsp database Field Descriptions (continued)

Field	Description
SAP Services	Information about SAP services.
Metric:	Received SAP hop count.
IPX SVC	Name of the IPX service.
D001.000.0000.0001	IPX address of the server advertising this service.
Sock	Socket number of the service.
Type	Type of service.

show ipx nlsp neighbors

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp neighbors** command is not supported in Cisco IOS software.

To display NetWare Link Services Protocol (NLSP) neighbors and their states, use the **show ipx nlsp neighbors** command in EXEC mode.

show ipx nlsp [*tag*] **neighbors** [*interface*] [**detail**]

Syntax Description

tag	(Optional) Names the NLSP process. The value of the *tag* argument can be any combination of printable characters.
interface	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about the neighbor. If you omit this keyword, only a summary display is shown.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When you specify an NLSP *tag* value, the router displays the NLSP neighbors for that NLSP process. An NLSP process is a router's databases working together to manage route information about an area. NLSP version 1.0 routers must be in a single 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 adjacencies, link-state, and area address databases 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.

You must configure multiple NLSP processes when a router interconnects multiple NLSP areas.

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.

If you omit the keyword **detail**, a summary display is shown.

Examples

The following command output from the **show ipx nlsp neighbors** command shows a summary display of three adjacencies on two circuits:

```
Router# show ipx nlsp neighbors

System Id  Interface  State  Holdtime  Priority  Cir  Adj  Circuit Id
dtp-37     Et1.2      Up     21        64        mc   mc   dtp-37.03
dtp-37     Et1.1      Up     58        44        bc   mc   dtp-17.02
dtp-17     ET1.1      Up     27        64        bc   bc   dtp-17.02
```

This display indicates the following information about the first circuit (Circuit Id = dtp-37.03):

- Multicast addressing is in use (Cir = mc).
- The neighbor supports multicast addressing (Adj = mc).

This display indicates the following information about the second circuit (Circuit Id = dtp-17.02):

- The broadcast address is in use (Cir = bc).
- The first neighbor (System Id = dtp-37) supports multicast addressing (Adj = mc).
- The second neighbor (System Id = dtp-17) does not support multicast addressing (Adj = bc). This adjacency explains why the broadcast address is in use on the second circuit.

The following is sample output from the **show ipx nlsp neighbors detail** command:

```
Router# show ipx nlsp neighbors detail

System Id       Interface  State  Holdtime  Priority  Cir  Adj  Circuit Id
0000.0C01.EF90  Ethernet1  Up     25        64        mc   mc   0000.0C01.EF90.0C
  IPX Address: E1.0000.0c01.ef91
  IPX Areas:  00000000/00000000
  Uptime: 2:59:11
```

Table 25 describes the fields shown in the display.

Table 25 show ipx nlsp neighbors Field Descriptions

Field	Description
System Id	System ID of the neighbor.
Interface	Interface on which the neighbor was discovered.
State	State of the neighbor adjacency.
Holdtime	Remaining time before the router assumes that the neighbor has failed.
Priority	Designated router election priority.

Table 25 show ipx nlsp neighbors Field Descriptions (continued)

Field	Description
Cir	NLSP addressing state (multicast or broadcast) of the interface.
Adj	NSLP addressing state (multicast or broadcast) of the adjacent neighbor.
Circuit Id	Neighbor's internal identifier for the circuit.
IPX Address:	IPX address on this network of the neighbor.
IPX Areas:	IPX area addresses configured on the neighbor.
Uptime:	Time since the router discovered the neighbor. Time is formatted in *hh*:*mm*:*ss*.

show ipx nlsp spf-log

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp spf-log** command is not supported in Cisco IOS software.

To display a history of the shortest path first (SPF) calculations for NetWare Link Services Protocol (NLSP), use the **show ipx nlsp spf-log** command in EXEC mode.

show ipx nlsp [*tag*] **spf-log**

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx nlsp spf-log** command:

```
Router# show ipx nlsp spf-log

    Level 1 SPF log
  When   Duration  Nodes  Count  Triggers
0:30:59     1028     84      1  TLVCONTENT
0:27:09     1016     84      1  TLVCONTENT
0:26:30     1136     84      1  TLVCONTENT
0:23:11     1244     84      1  TLVCONTENT
0:22:39      924     84      2  TLVCONTENT
0:22:08     1036     84      1  TLVCONTENT
0:20:02     1096     84      1  TLVCONTENT
0:19:31     1140     84      1  TLVCONTENT
0:17:25      964     84      2  PERIODIC TLVCONTENT
0:16:54      996     84      1  TLVCONTENT
```

```
0:16:23      984     84      1  TLVCONTENT
0:15:52     1052     84      1  TLVCONTENT
0:14:34     1112     84      1  TLVCONTENT
0:13:37      992     84      1  TLVCONTENT
0:13:06     1036     84      1  TLVCONTENT
0:12:35     1008     84      1  TLVCONTENT
0:02:52     1032     84      1  TLVCONTENT
0:02:16     1032     84      1  PERIODIC
0:01:44     1000     84      3  TLVCONTENT
```

Table 26 describes the fields shown in the display.

Table 26 show ipx nlsp spf-log Field Descriptions

Field	Descriptions
When	Amount of time since the SPF calculation took place.
Duration	Amount of time (in milliseconds) that the calculation required.
Nodes	Number of link state packets (LSPs) encountered during the calculation.
Count	Number of times that the SPF calculation was triggered before it actually took place. An SPF calculation is normally delayed for a short time after the event that triggers it.
Triggers	List of the types of triggers that were recorded before the SPF calculation occurred (more than one type may be displayed): • PERIODIC—Periodic SPF calculation (every 15 minutes). • NEWSYSID—New system ID was assigned. • NEWAREA—New area address was configured. • RTCLEARED—IPX routing table was manually cleared. • NEWMETRIC—Link metric of an interface was reconfigured. • ATTACHFLAG—Level 2 router has become attached or unattached from the rest of the level 2 topology. • LSPEXPIRED—LSP has expired. • NEWLSP—New LSP has been received. • LSPHEADER—LSP with changed header fields was received. • TLVCODE—LSP with a changed (Type-Length-Value) TLV code field was received. • TLVCONTENT—LSP with changed TLV contents was received. • AREASET—Calculated area address set has changed. • NEWADJ—New neighbor adjacency came up. • DBCHANGED—NLSP link state database was manually cleared.

show ipx route

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **show ipx route** command is not supported in Cisco IOS software.

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

show ipx route [*network*] [**default**] [**detailed**]

Syntax Description

network	(Optional) Number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
default	(Optional) Displays the default route. This is equivalent to specifying a value of FFFFFFFE for the argument *network*.
detailed	(Optional) Displays detailed route information.

Command Modes EXEC

Command History

Release	Modification
10.0	This command was introduced. The following keywords were added: • **default** • **detailed**
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

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

```
Router# show ipx route

Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

8 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D40 is the internal network
C        100 (NOVELL-ETHER), Et1
C       7000 (TUNNEL),        Tu1
S        200 via     7000.0000.0c05.6023,        Tu1
R        300 [02/01] via      100.0260.8c8d.e748,   19s, Et1
S       2008 via     7000.0000.0c05.6023,        Tu1
R     CC0001 [02/01] via      100.0260.8c8d.e748,   19s, Et1
```

Table 27 describes the fields shown in the display.

Table 27 show ipx route Field Descriptions

Field	Description
Codes	Codes defining how the route was learned.
L - Local	Internal network number.
C - Connected primary network	Directly connected primary network.
c - connected secondary network	Directly connected secondary network.
S - Static	Statically defined route via the **ipx route** command.
R - RIP	Route learned from a RIP update.
E - EIGRP	Route learned from an Enhanced IGRP (EIGRP) update.
W - IPXWAN	Directly connected route determined via IPXWAN.
8 Total IPX routes	Number of routes in the IPX routing table.
No parallel paths allowed	Maximum number of parallel paths for which the Cisco IOS software has been configured with the **ipx maximum-paths** command.
Novell routing algorithm variant in use	Indicates whether Cisco IOS software is using the IPX-compliant routing algorithms (default).
Net 1	Network to which the route goes.
[3/2]	Delay/Metric. Delay is the number of IBM clock ticks (each tick is 1/18 seconds) reported to the destination network. Metric is the number of hops reported to the same network. Delay is used as the primary routing metric, and the metric (hop count) is used as a tie breaker.
via *network.node*	Address of a router that is the next hop to the remote network.

Table 27 show ipx route Field Descriptions (continued)

Field	Description
age	Amount of time (in hours, minutes, and seconds) that has elapsed since information about this network was last received.
uses	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
Ethernet0	Interface through which packets to the remote network will be sent.
(NOVELL-ETHER)	Encapsulation (frame) type. This is shown only for directly connected networks.
is directly connected	Indicates that the network is directly connected to the router.

When Cisco IOS software generates an aggregated route, the **show ipx route** command displays a line item similar to the following:

```
NA      1000 FFFFF000 [**][**/06] via        0.0000.0000.0000,  163s, Nu0
```

In the following example, the router that sends the aggregated route also generates the aggregated route line item in its table. But the entry in the table points to the null interface (*Nu0*), indicating that if this aggregated route is the most-specific route when a packet is being forwarded, the router drops the packet instead.

```
Router# show ipx route

Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

13 Total IPX routes. Up to 4 parallel paths and 16 hops allowed.

No default route known.

NA      1000 FFFFF000 [**][**/06] via        0.0000.0000.0000,  163s, Nu0
L       2008 is the internal network
C          1 (NOVELL-ETHER),  Et0
C         89 (SAP),           To0
C         91 (SAP),           To1
C        100 (NOVELL-ETHER),  Et1
N          2 [19][01/01]          via       91.0000.30a0.51cd,  317s, To1
N          3 [19][01/01]          via       91.0000.30a0.51cd,  327s, To1
N         20 [20][01/01]          via        1.0000.0c05.8b24, 2024s, Et0
N        101 [19][01/01]          via       91.0000.30a0.51cd,  327s, To1
NX      1000 [20][02/02][01/01]   via        1.0000.0c05.8b24, 2024s, Et0
N       2010 [20][02/01]          via        1.0000.0c05.8b24, 2025s, Et0
N       2011 [19][02/01]          via       91.0000.30a0.51cd,  328s, To1
```

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

```
Router# show ipx route detailed
```

```
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, s - seconds, u - uses

9 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D35 is the internal network
C       E001 (SAP),           Et0
C      D35E2 (NOVELL-ETHER),  Et2
R        D34 [02/01]
          -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
N        D36 [20][02/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                10000000:1000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
NX       D40 [20][03/02][02/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
R      D34E1 [01/01]
          -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
NX     D40E1 [20][02/02][01/01]
          -- via    D35E2.0000.0c02.8cfc, 704s,     3u, Et2
                10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
N     D36E02 [20][01/01]
          -- via    D35E2.0000.0c02.8cfc, 705s,     2u, Et2
                10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
```

Table 28 describes the additional fields shown in the display.

Table 28 show ipx route detailed Field Descriptions

Field	Description
1u	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
10000000	(NLSP only) Throughput (end to end).
3000	(NLSP only) Link delay (end to end).
1500	(NLSP only) MTU (end to end).
0000.0c02.8cfb	(NLSP only) System ID of the next-hop router.
6	(NLSP only) Local circuit ID.
0000.0c02.8cfc	(NLSP only) MAC address of the next-hop router.

Related Commands

Command	Description
clear ipx route	Deletes routes from the IPX routing table.
ipx maximum-paths	Sets the maximum number of equal-cost paths Cisco IOS software uses when forwarding packets.
ipx nlsp metric	Configures an interface to use multicast addressing.
ipx route	Adds a static route or static NLSP route summary to the routing table.

show ipx servers

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx servers** command is not supported in Cisco IOS software.

To list the IPX servers discovered through Service Advertising Protocol (SAP) advertisements, use the **show ipx servers** command in EXEC mode.

show ipx servers [**detailed**] [**network** *network-number*] [**type** *service-type-number*] [**unsorted** | [**sorted** [**name** | **network** | **type**]]] [**regexp** *name*]

Syntax Description

detailed	(Optional) Displays comprehensive information including path details.
network	(Optional) Displays IPX SAP services on a specified network.
network-number	(Optional) IPX network number. 1 to FFFFFFFF.
type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.
service-type-number	(Optional) IPX service type number. 1 to FFFF. When used with the **network** keyword, displays a list of all SAPs known to a particular network number.
unsorted	(Optional) Does not sort entries when displaying IPX servers.
sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
network	(Optional) Displays the IPX servers numerically by network number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Defaults

IPX servers are displayed numerically by SAP service type.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **unsorted** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.

Release	Modification
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following example uses a regular expression to display SAP table entries corresponding to a particular group of servers in the accounting department of a company:

```
Router# show ipx servers regexp ACCT\_SERV.+

Codes: S - Static, P - Periodic, E - EIGRP, H - Holddown, + = detail
9 Total IPX Servers

Table ordering is based on routing and server info

 Type  Name            Net  Address        Port  Route  Hops Itf
S 108  ACCT_SERV_1     7001.0000.0000.0001:0001   1/01   2   Et0
S 108  ACCT_SERV_2     7001.0000.0000.0001:0001   1/01   2   Et0
S 108  ACCT_SERV_3     7001.0000.0000.0001:0001   1/01   2   Et0
```

For more information on regular expressions, refer to the “Regular Expressions” appendix in *Cisco IOS Dial Technologies Command Reference*.

Related Commands

Command	Description
ipx sap	Specifies static SAP entries.

show ipx spx-spoof

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx spx-spoof** command is not supported in Cisco IOS software.

To display the table of Sequenced Packet Exchange (SPX) connections through interfaces for which SPX spoofing is enabled, use the **show ipx spx-spoof** command in EXEC mode.

show ipx spx-spoof

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx spx-spoof** command:

```
Router# show ipx spx-spoof

Local SPX Network.Host:sock Cid  Remote SPX Network.Host:sock Cid   Seq  Ack  Idle
CC0001.0000.0000.0001:8104  0D08 200.0260.8c8d.e7c6:4017      7204  09   0021 120
CC0001.0000.0000.0001:8104  0C08 200.0260.8c8d.c558:4016      7304  07   0025 120
```

Table 29 describes the fields shown in the display.

Table 29 show ipx spx-spoof Field Descriptions

Field	Description
Local SPX Network.Host:sock	Address of the local end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the local end of the SPX connection.
Remote SPX Network.Host:sock	Address of the remote end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the remote end of the SPX connection.
Seq	Sequence number of the last data packet transferred.
Ack	Number of the last solicited acknowledge received.
Idle	Amount of time elapsed since the last data packet was transferred.

Related Commands

Command	Description
ipx spx-idle-time	Sets the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer.
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 traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx traffic** command is not supported in Cisco IOS software.

To display information about the number and type of IPX packets sent and received, use the **show ipx traffic** command in EXEC mode.

show ipx [**nlsp**] **traffic** [**since** {**bootup** | **show**}]

Syntax Description

nlsp	(Optional) Displays only NetWare Link Services Protocol (NLSP) traffic counters.
since bootup	(Optional) Displays traffic statistics since bootup.
since show	(Optional) Displays traffic statistics since last **show** command.

Defaults

Display traffic statistics since bootup or since the last **clear** command was entered.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	The following keywords were added: • **nlsp** • **since bootup** • **since show**
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

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

```
Router# show ipx traffic

System Traffic for 0.0000.0000.0001 System-Name: Router
Time since last clear: never
Rcvd:  0 total, 0 format errors, 0 checksum errors, 0 bad hop count
       0 packets pitched, 0 local destination, 0 multicast
Bcast: 0 received, 0 sent
Sent:  0 generated, 0 forwarded
       0 encapsulation failed, 0 no route
SAP:   0 Total SAP requests, 0 Total SAP replies, 1 servers
       0 SAP General Requests, 2 sent, 0 ignored, 0 replies
       0 SAP Get Nearest Server requests, 0 replies
       0 SAP Nearest Name requests, 0 replies
          0 SAP General Name requests, 0 replies
          0 SAP advertisements received, 324 sent, 0 Throttled
       0 SAP flash updates sent, 0 SAP format errors
RIP:   0 RIP requests, 0 ignored, 0 RIP replies, 3 routes
       0 RIP advertisements received, 684 sent, 0 Throttled
       0 RIP flash updates sent, 0 atlr sent
          2 RIP general requests sent
          0 RIP format errors
Echo:  Rcvd 0 requests, 0 replies
       Sent 0 requests, 0 replies
       0 unknown: 0 no socket, 0 filtered, 0 no helper
            0 SAPs throttled, freed NDB len 0
Watchdog:
       0 packets received, 0 replies spoofed
Queue lengths:
       IPX input: 0, SAP 0, RIP 0, GNS 0
       SAP throttling length: 0/(no limit), 0 nets pending lost route reply
       Delayed process creation: 0
EIGRP: Total received 0, sent 0
       Updates received 0, sent 0
       Queries received 0, sent 0
       Replies received 0, sent 0
       SAPs received 0, sent 0
NLSP:  Time since last clear: never
NLSP:  Level-1 Hellos (sent/rcvd): 0/0
       PTP Hellos    (sent/rcvd): 0/0
       Level-1 LSPs sourced (new/refresh): 1/0
       Level-1 LSPs flooded (sent/rcvd): 0/0
            LSP Retransmissions: 0
       Level-1 CSNPs (sent/rcvd): 0/0
       Level-1 PSNPs (sent/rcvd): 0/0
       Level-1 DR Elections: 0
       Level-1 SPF Calculations: 1
       Level-1 Partial Route Calculations: 0
       LSP checksum errors received: 0
Trace:  Rcvd 0 requests, 0 replies
          Sent 0 requests, 0 replies
```

Table 30 describes the fields shown in the display.

Table 30 show ipx traffic Field Descriptions

Field	Description
Time since last clear	Elapsed time since last **clear** command issued.
Rcvd:	Description of the packets received.
total	Total number of packets received.
format errors	Number of bad packets discarded (for example, packets with a corrupted header). Includes IPX packets received in an encapsulation that this interface is not configured for.
checksum errors	Number of packets containing a checksum error. This number should always be 0, because IPX rarely uses a checksum.
bad hop count	Number of packets discarded because their hop count exceeded 16.
packets pitched	Number of times the device received its own broadcast packet.
local destination	Number of packets sent to the local broadcast address or specifically to the router.
multicast	Number of packets received that were addressed to an IPX multicast address.
Bcast:	Description of broadcast packets the router received and sent.
received	Number of broadcast packets received.
sent	Number of broadcast packets sent, including those the router is either forwarding or has generated.
Sent:	Description of packets the software generated and sent and those the software received and routed to other destinations.
generated	Number of packets sent that the router generated itself.
forwarded	Number of packets sent that the router forwarded from other sources.
encapsulation failed	Number of packets the software was unable to encapsulate.
no route	Number of times the software could not locate a route to the destination in the routing table.
SAP:	Description of the Service Advertising Protocol (SAP) packets sent and received.
Total SAP requests	Cumulative sum of SAP requests received: • SAP general requests • SAP Get Nearest Server (GNS) requests
Total SAP replies	Cumulative sum of all SAP reply types: General, Get Nearest Server, Nearest Name, and General Name.
servers	Number of servers in the SAP table.
SAP General Requests, received, sent, ignored, replies	Number of general SAP requests, sent requests, ignored requests, and replies. This field applies to Cisco IOS Release 11.2 and later.
SAP Get Nearest Server, requests, replies	Number of GNS requests and replies. This field applies to Cisco IOS Release 11.2 and later.

Table 30 show ipx traffic Field Descriptions (continued)

Field	Description
SAP Nearest Name requests, replies	Number of SAP Nearest Name requests and replies. This field applies to Cisco IOS Release 11.2 and later.
SAP advertisements received and sent	Number of SAP advertisements generated and then sent as a result of a change to the routing or service tables.
Throttled	Number of SAP advertisements discarded because they exceeded buffer capacity.
SAP flash updates sent	Number of SAP flash updates generated and sent because of changes to routing or service tables.
SAP format errors	Number of incorrectly formatted SAP advertisements received.
RIP:	Description of the Routing Information Protocol (RIP) packets received and sent.
RIP requests	Number of RIP requests received.
ignored	Number of RIP requests ignored.
RIP replies	Number of RIP replies sent in response to RIP requests.
routes	Number of RIP routes in the current routing table.
RIP advertisements received	Number of RIP advertisements received from another router.
sent	Number of RIP advertisements generated and then sent.
Throttled	Number of RIP advertisements discarded because they exceeded buffer capacity.
RIP flash updates sent atlr sent	Number of RIP flash updates generated and sent and number of advertisements to lost routes sent because of changes to the routing table.
RIP general requests sent	Number of RIP general requests generated and then sent.
RIP format errors	Number of incorrectly formatted RIP packets received.
Echo:	Description of the ping replies and requests received and sent.
Rcvd requests, replies	Number of ping requests and replies received.
Sent requests, replies	Number of ping requests and replies sent.
unknown	Number of unsupported packets received on socket.
no socket, filtered, no helper	Number of packets that could not be forwarded because helper addresses were improperly configured.
SAPs throttled	Number of SAP packets discarded because they exceeded buffer capacity.
freed NDB len	Number of Network Descriptor Blocks removed from the network but still needing to be removed from the routing table of the router.
Watchdog:	Description of the watchdog packets the software handled.
packets received	Number of watchdog packets received from IPX servers on the local network.
replies spoofed	Number of times the software responded to a watchdog packet on behalf of the remote client.

Table 30 show ipx traffic Field Descriptions (continued)

Field	Description
Queue lengths	Description of outgoing packets currently in buffers waiting to be processed.
IPX input	Number of incoming packets waiting to be processed.
SAP	Number of outgoing SAP packets waiting to be processed.
RIP	Number of outgoing RIP packets waiting to be processed.
GNS	Number of outgoing GNS packets waiting to be processed.
SAP throttling length	Maximum number of outgoing SAP packets allowed in the buffer. Additional packets received are discarded.
nets pending lost reply route	Number of "downed" routes being processed by the Lost Route Algorithm.
EIGRP: Total received, sent	Description of the Enhanced Interior Gateway Protocol (IGRP) packets the router received and sent.
Updates received, sent	Number of Enhanced IGRP updates received and sent.
Queries received, sent	Number of Enhanced IGRP queries received and sent.
Replies received, sent	Number of Enhanced IGRP replies received and sent.
SAPs received, sent	Number of SAP packets received from and sent to Enhanced IGRP neighbors.
NLSP:	Description of the NetWare Link Services Protocol (NLSP) packets the router sent and received.
Time since last clear	Elapsed time since last **clear** command issued.
Level-1 Hellos (sent/rcvd)	Number of LAN hello packets sent and received.
PTP Hellos (sent/rcvd)	Number of point-to-point Hello packets sent and received.
Level-1 LSPs sourced (new/refresh)	Number of local link-state packets (LSPs) created/refreshed by this router.
Level 1-LSPs flooded (sent/rcvd)	Number of LSPs sent and received by this router.
LSP Retransmissions	Number of LSPs resent by this router.
Level-1 CSNPs (sent/rcvd)	Number of complete sequence number PDU (CSNP) packets sent and received.
Level-1 PSNPs (sent/rcvd)	Number of partial sequence number PDU (PSNP) packets sent and received.
Level-1 DR Elections	Number of times the software calculated its designated router election priority.
Level-1 SPF Calculations	Number of times the software performed the shortest path first (SPF) calculation.
Level-1 Partial Route Calculations	Number of times the software recalculated routes without running SPF.
LSP Checksum errors received	Number of LSPs rejected because of checksum errors.

Table 30 show ipx traffic Field Descriptions (continued)

Field	Description
Trace:	Description of the trace packets the router received and sent.
RCvd requests, replies	Number of trace requests and replies received.
Sent requests, replies	Number of trace requests and replies sent.

Related Commands

Command	Description
clear ipx traffic	Clears IPX protocol and NLSP traffic counters.

show sse summary

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show sse summary** command is not supported in Cisco IOS software.

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** command in EXEC mode.

show sse summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show sse summary** command:

```
Router# show sse summary

SSE utilization statistics

               Program words  Rewrite bytes  Internal nodes  Depth
Overhead                 499              1               8
IP                         0              0               0      0
IPX                        0              0               0      0
SRB                        0              0               0      0
CLNP                       0              0               0      0
IP access lists            0              0               0
Total used               499              1               8
Total free             65037         262143
Total available        65536         262144

Free program memory
  [499..65535]
Free rewrite memory
```

```
  [1..262143]

Internals
  75032 internal nodes allocated, 75024 freed
  SSE manager process enabled, microcode enabled, 0 hangs
  Longest cache computation 4ms, longest quantum 160ms at 0x53AC8
```

spf-interval

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **spf-interval** command is not supported in Cisco IOS software.

To customize Intermediate System-to-Intermediate System (IS-IS) throttling of shortest path first (SPF) calculations, use the **spf-interval** command in router configuration mode. To restore default values, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

no spf-interval

Syntax Description

level-1	(Optional) Apply intervals to Level-1 areas only.
level-2	(Optional) Apply intervals to Level-2 areas only.
spf-max-wait	Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.
spf-initial-wait	(Optional) Indicates the initial SPF calculation delay (in milliseconds) after a topology change. The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).
spf-second-wait	(Optional) Indicates the hold time between the first and second SPF calculation (in milliseconds). The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

Defaults

spf-max-wait: 10 seconds
spf-initial-wait: 5500 milliseconds
spf-second-wait: 5500 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.1	The **level-1** and **level-2** keywords were added; the *spf-max-wait*, *spf-initial-wait*, and *spf-second-wait* arguments were added. The default interval between SPF calculations was changed from 5 seconds to 10 seconds.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.

Release	Modification
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** command controls how often Cisco IOS software performs the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows down the rate of convergence.

The following description will help you determine whether to change the default values of this command:

- The *spf-initial-wait* argument indicates the initial wait time (in milliseconds) after a topology change before the first SPF calculation.
- The *spf-second-wait* argument indicates the interval (in milliseconds) between the first and second SPF calculation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *spf-max-wait* interval specified; the SPF calculations are throttled or slowed down after the initial and second intervals. Once the *spf-max-wait* interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the *spf-max-wait* interval, fast behavior is restored (the initial wait time).

SPF throttling is not a dampening mechanism; that is, SPF throttling does not prevent SPF calculations or mark any route, interface, or router as down. SPF throttling simply increases the intervals between SPF calculations.

Examples

The following example configures intervals for SPF calculations, partial route calculation (PRC), and link-state packet (LSP) generation:

```
router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100
```