ipx input-network-filter (RIP)

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

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

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

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

Syntax Description

access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the value for the *access-list-number* argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 input-network-filter** command controls which networks are added to the routing table based on the networks learned in incoming IPX routing updates (RIP updates) on the interface.

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

Examples

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

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

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

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

Related Commands

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

ipx input-sap-filter

✎

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

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

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

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

Syntax Description

access-list-number	Number of the SAP access list. All incoming packets are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 input-sap-filter** command filters all incoming service advertisements received by the router. This is done prior to accepting information about a service.

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

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

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

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

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

ipx internal-network

✎

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

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

ipx internal-network *network-number*

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

Syntax Description

network-number	Number of the internal network.

Defaults   No internal network number is set.

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.
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.

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

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

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

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

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

Related Commands

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

ipx ipxwan

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

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

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

   no ipx ipxwan

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

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

Command Modes	Interface configuration

Command History

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

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

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

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

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

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

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

Examples   The following example enables IPXWAN on serial interface 0:

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

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

On the local access server (CHICAGO-AS):

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

On the remote router (NYC-AS):

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

Related Commands

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

ipx ipxwan error

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

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

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

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

Syntax Description

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

Defaults The link is reset.

Command Modes Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
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 ipxwan error** command to define what action to take if the IPXWAN startup negotiation fails.

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

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

Related Commands

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

ipx ipxwan static

✎

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

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

ipx ipxwan static

no ipx ipxwan static

Syntax Description   This command has no arguments or keywords.

Defaults   Static routing is disabled.

Command Modes   Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
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 specify the **ipx ipxwan static** command, the interface negotiates static routing on the link. If the router at the other side of the link is not configured to negotiate for static routing, the link will not initialize.

Examples   The following example enables static routing with IPXWAN:

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

```
ipx ipxwan static
```

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

ipx link-delay

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

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

ipx link-delay *microseconds*

no ipx link-delay *microseconds*

Syntax Description

microseconds	Delay, in microseconds.

Defaults No link delay (delay of 0).

Command Modes Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
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 link delay you specify replaces the default value or overrides the value measured by IPXWAN when it starts.

Examples The following example sets the link delay to 20 microseconds:

```
ipx link-delay 20
```

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

ipx linkup-request (RIP)

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

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

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

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

Syntax Description

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

Defaults General RIP and SAP queries are sent.

Command Modes Interface configuration

Command History

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

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

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

Related Commands

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

ipx maximum-hops (RIP)

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

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

ipx maximum-hops *hops*

no ipx maximum-hops *hops*

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

Defaults 16 hops

Command Modes Global configuration

Command History

Release	Modification
10.3	This command was introduced.
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 Packets whose hop count is equal to or greater than that specified by the **ipx maximum-hops** command are dropped.

In periodic RIP updates, the Cisco IOS software never advertises any network with a hop count greater than 15. However, using protocols other than RIP, the software might learn routes that are farther away than 15 hops. The **ipx maximum-hops** command defines the maximum number of hops that the software

will accept as reachable, as well as the maximum number of hops that an IPX packet can traverse before it is dropped by the software. Also, the software will respond to a specific RIP request for a network that is reachable at a distance of greater than 15 hops.

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

```
ipx maximum-hops 64
```

ipx maximum-paths

✎

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

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

ipx maximum-paths *paths*

no ipx maximum-paths

Syntax Description

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

Defaults 1 path

Command Modes Global configuration

Command History

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

When per-host load sharing is disabled, IPX performs load sharing on a packet-by-packet basis in round-robin fashion, regardless of whether you are using fast switching or process switching. That is, the first packet is sent along the first path, the second packet along the second path, and so on. When the final path is reached, the next packet is sent to the first path, the next to the second path, and so on.

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

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

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

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

```
ipx maximum-paths 3
```

Related Commands

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

ipx nasi-server enable

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

To enable NetWare Asynchronous Services Interface (NASI) clients to connect to asynchronous devices attached to your router, use the **ipx nasi-server enable** command in global configuration mode. To prevent NASI clients from connecting to asynchronous devices through a router, use the **no** form of this command.

ipx nasi-server enable

no ipx nasi-server enable

Syntax Description   This command has no arguments or keywords.

Command Default   NASI is not enabled.

Command Modes   Global configuration

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.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines   When you enter this command, NASI clients can connect to any port on the router, other than the console port, to access network resources. When the user on the NASI client uses the Windows or DOS application to connect to the router, a list of available tty and vty lines appear, beginning with tty1. The user can select the desired outgoing tty or vty port.

To to enable a username and password prompt for authentication, authorization, and accounting purposes, you can configure TACACS+ security on the router, after the user on the NASI client selects a tty or vty port.

Examples   The following example shows a minimum configuration to enable NASI clients dial-in access with
TACACS+ authentication:

```
ipx routing
ipx internal-network ncs001
interface ethernet 0
  ipx network 1
ipx nasi-server enable
! enable TACACS+ authentication for NASI clients using the list name swami
aaa authentication nasi swami tacacs+
line 1 8
  modem inout
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters.

ipx netbios input-access-filter

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

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

> **ipx netbios input-access-filter** {**host** | **bytes**} *name*

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

Syntax Description

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

Defaults   No filters are predefined.

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 issue only one **ipx netbios input-access-filter host** and one **ipx netbios input-access-filter bytes** command on each interface.

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

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

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

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

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

ipx netbios output-access-filter

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

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

ipx netbios output-access-filter {**host** | **bytes**} *name*

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

Syntax Description

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

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 issue only one **ipx netbios output-access-filter host** and one **ipx netbios output-access-filter bytes** command on each interface.

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

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

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

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

Related Commands

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

ipx netbios-socket-input-checks

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

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

ipx netbios-socket-input-checks

no ipx netbios-socket-input-checks

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History

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

■ **Novell IPX**

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

Examples The following example enables the additional checks on NetBIOS packets:

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

Related Commands

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

ipx network

✎

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

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

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

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

Syntax Description		
network	Network number. This is an 8-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD.	
	You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.	
encapsulation *encapsulation-type*	(Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 12.	
secondary	(Optional) Indicates an additional (secondary) network configured after the first (primary) network.	

Defaults IPX routing is disabled.

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

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

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(1)T	This command was modified to support the FDDI interface.
	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.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **ipx network** command allows you to configure a single logical network on a physical network or more than one logical network on the same physical network (network cable segment). Each network on a given interface must have a different encapsulation type.

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

The first network you configure on an interface is considered to be the primary network. Any additional networks are considered to be secondary networks; these must include the **secondary** keyword.

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

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

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

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

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

Caution The maximum size of the IPX packets that can be sent via the secondary networks depends on the encapsulation of the primary network and the maximum transfer unit (MTU) of the interface where these networks are configured. Otherwise, packet loss may occur. Subinterfaces, when used instead of secondary networks, do not impose primary network-based packet size restrictions. Some of the maximum IPX packet sizes supported for the supported encapsulation types are shown in the examples.

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

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

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

no ipx network

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

no ipx network *number*

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

no ipx network *number*

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

Novell's FDDI_RAW encapsulation is common in bridged or switched environments that connect Ethernet-based Novell end hosts via a FDDI backbone. Packets with FDDI_RAW encapsulation are classified as Novell packets and are not automatically bridged when you enable both bridging and IPX routing. Additionally, you cannot configure FDDI_RAW encapsulation on an interface configured for IPX autonomous or silicon switching engine (SSE) switching. Similarly, you cannot enable IPX autonomous or SSE switching on an interface configured with FDDI_RAW encapsulation.

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

Table 12 describes the types of encapsulation available for specific interfaces.

Table 12   Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell's Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.

Table 12   *Encapsulation Types (continued)*

Encapsulation Type	Description
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0.
	For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.
	For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
snap	For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header.
	For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

Examples

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

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

interface ethernet 0.1
 ipx network 2 encapsulation snap

interface ethernet 0.2
 ipx network 3 encapsulation arpa

interface ethernet 0
 ipx network 4 encapsulation sap
```

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

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

The following example provides information about maximum supported packet sizes described in the "Caution." If the primary network is configured with SAP encapsulation, IPX packets greater than 1497 are dropped because one of the following situations exists:

- The size of a datagram is rounded off from an odd number of bytes to an even number of bytes, which may increase the IPX packet length by 1; in this example, from 1497 bytes to 1498 bytes.

• A secondary network on the same interface is configured with Novell-Ethernet encapsulation, although this encapsulation supports an MTU of 1500 bytes.

The following data compares some maximum sizes of IPX datagrams:

Novell-Ethernet is 1518 - 12 -2 (length) -4 (CRC) = 1500

SAP is 1518 - 12 -2 (length) -3 (SAP header) -4 (CRC) = 1497

SNAP is 1518 - 12 -2 (length) -8 (SNAP header) -4 (CRC) = 1492

ARPA is 1518 -12 -2 (length) -2 (type) -4 (CRC) =1500

Twelve bytes represents the source address and destination address in the Ethernet frame.

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

```
ipx routing

interface fddi 0.2 enc sde 2
 ipx network f02 encapsulation snap

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

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

ipx nhrp authentication

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

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

ipx nhrp authentication *string*

no ipx nhrp authentication [*string*]

Syntax Description

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

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

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

```
ipx nhrp authentication specialxx
```

ipx nhrp holdtime

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

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

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

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

Syntax Description

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

Defaults 7200 seconds (2 hours) for both arguments.

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

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

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

```
ipx nhrp holdtime 3600
```

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

```
ipx nhrp holdtime 7200 3600
```

ipx nhrp interest

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

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

ipx nhrp interest *access-list-number*

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

Syntax Description

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

Defaults   All non-NHRP packets can trigger NHRP requests.

Command Modes   Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

```
ipx nhrp interest 901
```

```
access-list 901 permit 20
```

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

ipx nhrp map

✎

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

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

ipx nhrp map *ipx-address nbma-address*

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

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

Defaults No static IPX-to-NBMA cache entries exist.

Command Modes Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.
	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.

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

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

```
interface serial 0
 ipx nhrp nhs 1.0000.0c14.59ef
 ipx nhrp nhs 1.0000.0c14.59d0
```

```
ipx nhrp map 1.0000.0c14.59ef c141.0001.0001
ipx nhrp map 1.0000.0c14.59d0 c141.0001.0002
```

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

ipx nhrp max-send

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

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

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

no ipx nhrp max-send

Syntax Description

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

Defaults
pkt-count = 5 packets
interval = 10 seconds

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

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

Related Commands

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

ipx nhrp network-id

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

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

ipx nhrp network-id *number*

no ipx nhrp network-id

Syntax Description

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

Defaults NHRP is disabled on the interface.

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

Examples The following example enables NHRP on the interface:

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

ipx nhrp nhs

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

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

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

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

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

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

Command Modes　Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.
	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.

■ Novell IPX

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

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

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

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

ipx nhrp record

✎

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

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

   ipx nhrp record

   no ipx nhrp record

Syntax Description This command has no arguments or keywords.

Defaults Forward record and reverse record options are enabled by default.

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

Examples The following example suppresses forward record and reverse record options:

```
no ipx nhrp record
```

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

ipx nhrp responder

✎

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

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

ipx nhrp responder *type number*

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

Syntax Description

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

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

Command Modes Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

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

```
ipx nhrp responder serial 0
```

ipx nhrp use

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

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

ipx nhrp use *usage-count*

no ipx nhrp use *usage-count*

Syntax Description

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

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

Command Modes
Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
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.

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

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

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

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

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

```
ipx nhrp use 5
```

Related Commands

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

ipx nlsp csnp-interval

✎

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

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

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

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

Syntax Description

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

Defaults 30 seconds

Command Modes Interface configuration

Command History

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

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

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

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

Related Commands

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

ipx nlsp enable

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

To enable NetWare Link-Services Protocol (NLSP) routing on the primary network configured on this interface or subinterface, use the **ipx nlsp enable** command in interface configuration mode. To disable NLSP routing on the primary network configured on this interface or subinterface, use the **no** form of this command.

ipx nlsp [*tag*] **enable**

no ipx nlsp [*tag*] **enable**

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

Defaults NLSP is disabled on all interfaces.

Command Modes Interface configuration

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

When you specify an NLSP *tag*, the router enables NLSP on the specified 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.

Examples   The following example enables NLSP routing on Ethernet interface 0:

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

The following example enables NLSP routing on serial interface 0:

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

The following example enables NLSP routing for process area3 on Ethernet interface 0:

```
interface ethernet 0
 ipx nlsp area3 enable
```

Related Commands

Command	Description
ipx nlsp rip	Configures RIP compatibility when NLSP is enabled.
ipx output-ggs-filter	Configures SAP compatibility when NLSP in enabled.

ipx nlsp hello-interval

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

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

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

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

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
seconds	Time, in seconds, between the transmission of hello packets on the interface. It can be a number in the range 1 to 1600. The default is 10 seconds for the designated router and 20 seconds for nondesignated routers.

Defaults

10 seconds for the designated router.
20 seconds for nondesignated routers.

Command Modes

Interface configuration

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

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

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

You may also use this command to reduce link overhead on very slow links by raising the hello interval. This will reduce the traffic on the link at the cost of increasing the time required to detect a failed router or link.

Examples

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

```
interface serial 0
 ipx ipxwan 2442 unnumbered local1
 ipx nlsp enable
 ipx nlsp hello-interval 30
```

Related Commands

Command	Description
ipx nlsp csnp-interval	Configures the NLSP CSNP interval.
ipx nlsp hello-multiplier	Configures the time delay between successive NLSP LSP transmissions.
ipx nlsp retransmit-interval	Configures RIP compatibility when NLSP is enabled.

ipx nlsp hello-multiplier

✎

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

To specify the hello multiplier used on an interface, use the **ipx nlsp hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nlsp [*tag*] **hello-multiplier** *multiplier*

no ipx nlsp [*tag*] **hello-multiplier**

Syntax Description	*tag*	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	multiplier	Value by which to multiply the hello interval. It can be a number in the range 3 to 1000. The default is 3.

Defaults   The default multiplier is 3.

Command Modes   Interface 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   You use the hello modifier in conjunction with the hello interval to determine the holding time value sent in a hello packet. The holding time is equal to the hello interval multiplied by the hello multiplier.

The holding time tells the neighboring router how long to wait for another hello packet from the sending router. If the neighboring router does not receive another hello packet in the specified time, then the neighboring router declares that the sending router is down.

You can use this method of determining the holding time when hello packets are lost with some frequency and NLSP adjacencies are failing unnecessarily. You raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

Examples   In the following example, serial interface 0 will advertise hello packets every 15 seconds. The multiplier is 5. These values determine that the hello packet holding time is 75 seconds.

```
interface serial 0
 ipx nlsp hello-interval 15
 ipx nlsp hello-multiplier 5
```

Related Commands

Command	Description
ipx nlsp hello-interval	Specifies the hello multiplier used on an interface.

ipx nlsp lsp-interval

✎

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

To configure the time delay between successive NetWare Link-Services Protocol (NLSP) link-state packet (LSP) transmissions, use the **ipx nlsp lsp-interval** command in interface configuration mode. To restore the default time delay, use the **no** form of this command.

ipx nlsp [*tag*] **lsp-interval** *interval*

no ipx nlsp [*tag*] **lsp-interval**

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
interval	Time, in milliseconds, between successive LSP transmissions. The interval can be a number in the range 55 and 5000. The default interval is 55 milliseconds (ms).

Defaults   55 milliseconds

Command Modes   Interface 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 you to control how fast LSPs can be flooded out an interface.

In topologies with a large number of NLSP neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows you to reduce the LSP transmission rate (and by implication the reception rate of other systems).

Examples

The following example causes the system to transmit LSPs every 100 ms (10 packets per second) on Ethernet interface 0:

```
interface Ethernet 0
 ipx nlsp lsp-interval 100
```

Related Commands

Command	Description
ipx nlsp retransmit-interval	Configures RIP compatibility when NLSP is enabled.

ipx nlsp metric

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

To configure the NetWare Link-Services Protocol (NLSP) cost for an interface, use the **ipx nlsp metric** command in interface configuration mode. To restore the default cost, use the **no** form of this command.

ipx nlsp [*tag*] **metric** *metric-number*

no ipx nlsp [*tag*] **metric** *metric-number*

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
metric-number	Metric value for the interface. It can be a number from 0 to 63.

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

Command Modes Interface configuration

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

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

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

```
interface serial 0
 ipx network 107
 ipx nlsp enable
 ipx nlsp metric 10
```

Related Commands

Command	Description
ipx nlsp enable	Configures the interval between the transmission of hello packets.

ipx nlsp multicast

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

To configure an interface to use multicast addressing, use the **ipx nlsp multicast** command in interface configuration mode. To configure the interface to use broadcast addressing, use the **no** form of this command.

> **ipx nlsp** [*tag*] **multicast**

> **no ipx nlsp** [*tag*] **multicast**

Syntax Description

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

Defaults   Multicast addressing is enabled.

Command Modes   Interface 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.
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 interface to use 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 if multicast addressing is not supported by the hardware or driver.

Examples   The following example disables multicast addressing on Ethernet interface 0:

```
interface ethernet 0
 no ipx nlsp multicast
```

ipx nlsp priority

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

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

ipx nlsp [*tag*] **priority** *priority-number*

no ipx nlsp [*tag*] **priority** *priority-number*

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
priority-number	Election priority of the designated router for the specified interface. This can be a number in the range 0 to 127. This value is unitless. The default is 44.

Defaults 44

Command Modes Interface configuration

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

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

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

```
interface ethernet 0
 ipx network 101
 ipx nlsp enable
 ipx nlsp priority 65
```

ipx nlsp retransmit-interval

✎

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

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

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

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

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
seconds	LSP retransmission interval, in seconds. This can be a number in the range 1 to 30. The default is 5 seconds.

Defaults 5 seconds

Command Modes Interface configuration

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 This command sets the maximum amount of time that can pass before an LSP will be sent again (retransmitted) on a WAN link, if no acknowledgment is received.

Reducing the retransmission interval can improve the convergence rate of the network in the face of lost WAN links. The cost of reducing the retransmission interval is the potential increase in link utilization.

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

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

Related Commands

Command	Description
ipx nlsp csnp-interval	Configures the NLSP CSNP interval.
ipx nlsp hello-interval	Specifies the hello multiplier used on an interface.

ipx nlsp rip

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

To configure RIP compatibility when NetWare Link-Services Protocol (NLSP) is enabled, use the **ipx nlsp rip** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx nlsp [*tag*] **rip** [**on** | **off** | **auto**]

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

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
on	(Optional) Always generates and sends RIP periodic traffic.
off	(Optional) Never generates and sends RIP periodic traffic.
auto	(Optional) Sends RIP periodic traffic only if another RIP router in sending periodic RIP traffic. This is the default.

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

Command Modes Interface configuration

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

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

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

Related Commands

Command	Description
ipx nlsp enable	Configures the interval between the transmission of hello packets.
ipx output-ggs-filter	Configures SAP compatibility when NLSP in enabled.

ipx nlsp sap

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

To configure SAP compatibility when NetWare Link-Services Protocol (NLSP) in enabled, use the **ipx nlsp sap** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx nlsp [*tag*] **sap** [**on** | **off** | **auto**]

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

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
on	(Optional) Always generates and sends SAP periodic traffic.
off	(Optional) Never generates and sends SAP periodic traffic.
auto	(Optional) Sends SAP periodic traffic only if another SAP router in sending periodic SAP traffic. This is the default.

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

Command Modes Interface configuration

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

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

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

Related Commands

Command	Description
ipx nlsp enable	Configures the interval between the transmission of hello packets.
ipx nlsp rip	Configures RIP compatibility when NLSP is enabled.

ipx output-ggs-filter

✎

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

To control which servers are included in the Get General Service (GGS) responses sent by Cisco IOS software, use the **ipx output-ggs-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-ggs-filter {*access-list-number* | *name*}

no ipx output-ggs-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the Service Advertising Protocol (SAP) access list. All outgoing GGS packets are filtered by the entries in this list. The *access-list number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent their being confused with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
12.0(1)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 You can issue only one **ipx output-ggs-filter** command on each interface.

Note Because GGS SAP response filters are applied ahead of output SAP filters, a SAP entry permitted to pass through the GGS SAP response filter can still be filtered by the output SAP filter.

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

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-ggs-filter 1000
```

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

ipx output-gns-filter

✎

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

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

ipx output-gns-filter {*access-list-number | name*}

no ipx output-gns-filter {*access-list-number | name*}

Syntax Description

access-list-number	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults   No filters are predefined.

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 issue only one **ipx output-gns-filter** command on each interface.

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

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-gns-filter 1000
```

	Command	Description
Related Commands	**access-list (SAP filtering)**	Defines an access list for filtering SAP requests.
	deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
	ipx access-list	Defines an IPX access list by name.
	ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
	permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx output-network-filter (RIP)

> ✎
>
> **Note** Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx output-network-filter (RIP)** command is not supported in Cisco IOS software.

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

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

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

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 output-network-filter** command controls which networks the Cisco IOS software advertises in its IPX routing updates (RIP updates).

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

■ **Novell IPX**

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

```
access-list 896 permit 2b

interface serial 1
 ipx output-network-filter 896
```

Related Commands	Command	Description
	access-list (IPX extended)	Defines an extended Novell IPX access list.
	access-list (IPX standard)	Defines a standard IPX access list.
	deny (extended)	Sets conditions for a named IPX extended access list.
	deny (standard)	Sets conditions for a named IPX access list.
	ipx access-list	Defines an IPX access list by name.
	ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
	ipx router-filter	Filters the routers from which packets are accepted.
	permit (IPX extended)	Sets conditions for a named IPX extended access list.
	prc-interval	Sets conditions for a named IPX access list.

ipx output-rip-delay

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

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

ipx output-rip-delay *delay*

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

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

Defaults   55 ms

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

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

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

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

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

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

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

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

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

Related 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 triggered-rip-delay	Sets the interpacket delay for triggered RIP 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 output-sap-delay

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

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

ipx output-sap-delay *delay*

no ipx output-sap-delay

Syntax Description

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

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

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

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

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

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

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

Examples

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

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

Related 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 triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx output-sap-filter

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

To control which services are included in Service Advertising Protocol (SAP) updates sent by Cisco IOS software, use the **ipx output-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

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

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

Syntax Description

access-list-number	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 Cisco IOS software applies output SAP filters prior to sending SAP packets.

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

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

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

```
access-list 1000 deny aa.0000.0000.0001
access-list 1000 permit -1

interface ethernet 0
 ipx network 3c

interface ethernet 1
 ipx network 4d
 ipx output-sap-filter 1000

interface serial 0
 ipx network 2b
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx pad-process-switched-packets

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

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

ipx pad-process-switched-packets

no ipx pad-process-switched-packets

Syntax Description This command has no arguments or keywords.

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

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

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

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

Examples   The following example configures the Cisco IOS software to pad odd-length packets so that they are sent as even-length packets on FDDI interface 1.

```
interface fddi 1
 ipx network 2A
 no ipx route-cache
 ipx pad-process-switched-packets
```

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.

ipx per-host-load-share

✎

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

To enable per-host load sharing, use the **ipx per-host-load-share** command in global configuration mode. To disable per-host load sharing, use the **no** form of this command.

> **ipx per-host-load-share**

> **no ipx per-host-load-share**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command Modes   Global 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.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines   Use this command to enable per-host load sharing. Per-host load sharing transmits traffic across multiple, equal-cost paths while guaranteeing that packets for a given end host always take the same path.

When you do not enable per-host load sharing, the software uses a round-robin algorithm to accomplish load sharing. Round-robin load sharing transmits successive packets over alternate, equal-cost paths, regardless of the destination host. With round-robin load sharing, successive packets destined for the

same end host might take different paths. Thus, round-robin load sharing increases the possibility that successive packets to a given end host might arrive out of order or be dropped, but ensures true load balancing of a given workload across multiple links.

In contrast, per-host load sharing decreases the possibility that successive packets to a given end host will arrive out of order; but, there is a potential decrease in true load balancing across multiple links. True load sharing occurs only when different end hosts utilize different paths; equal link utilization cannot be guaranteed.

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

Examples   The following command globally enables per-host load sharing:

```
ipx per-host-load share
```

Related Commands

Command	Description
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.

ipx ping-default

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

To select the ping type that Cisco IOS software transmits, use the **ipx ping-default** command in global configuration mode. To return to the default ping type, use the **no** form of this command.

ipx ping-default {**cisco** | **novell** | **diagnostic**}

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

Syntax Description	cisco	Transmits Cisco pings.
	novell	Transmits standard Novell pings.
	diagnostic	Transmits diagnostic request/response for IPX pings.

Defaults Cisco pings

Command Modes Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0	The **diagnostic** keyword was added.
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.

Usage Guidelines This command can transmit Cisco pings, standard Novell pings as defined in the NLSP specification, and IPX diagnostic pings.

The IPX diagnostic ping feature addresses diagnostic related issues by accepting and processing unicast or broadcast diagnostic packets. It makes enhancements to the current IPX ping command to ping other stations using the diagnostic packets and display the configuration information in the response packet.

> **Note** When a ping is sent from one station to another, the response is expected to come back immediately; when **ipx ping-default** is set to diagnostics, the response could consist of more than one packet and each node is expected to respond within 0.5 seconds of receipt of the request. Due to the absence of an end-of-message flag, there is a delay and the requester must wait for all responses to arrive. Therefore, in verbose mode there may be a brief delay of 0.5 seconds before the response data is displayed.

> The **ipx ping-default** command using the **diagnostic** keyword can be used to conduct a reachability test and should not be used to measure accurate roundtrip delay.

Examples   The following is sample output from the **ipx ping-default** command when the **diagnostic** keyword is enabled:

```
Router# ipx ping-default diagnostic

Protocol [ip]: ipx
Target IPX address: 20.0000.0000.0001
Verbose [n]: y
Timeout in seconds [2]: 1
Type escape sequence to abort.
Sending 1, 31-byte IPX Diagnostic Echoes to 20.0000.0000.0001, timeout is 1 seconds:

Diagnostic Response from 20.0000.0000.0001 in 4 ms
Major Version: 1
Minor Version: 0
SPX Diagnostic Socket: 4002
Number of components: 3
Component ID: 0 (IPX / SPX)
Component ID: 1 (Router Driver)
Component ID: 5 (Router)
Number of Local Networks: 2
 Local Network Type: 0 (LAN Board)
  Network Address1 20
  Node Address1 0000.0000.0001
 Local Network Type: 0 (LAN Board)
  Network Address2 30
  Node Address2 0060.70cc.bc65
```

> **Note** Verbose mode must be enabled to get diagnostic information.

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.
trace (privileged)	Discovers the specified protocol's routes that packets will actually take when traveling to their destination.

ipx potential-pseudonode (NLSP)

✎

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

To enable NetWare Link Services Protocol (NLSP) to keep backup router and service information for potential pseudonode, use the **ipx potential-pseudonode** command in global configuration mode. To disable the feature so that NLSP does not keep backup router and service information for potential pseudonode, use the **no** form of this command.

ipx potential-pseudonode

no ipx potential-pseudonode

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History

Release	Modification
11.0	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 The potential pseudonode is NLSP-specified service information that a router keeps in anticipation of possibly becoming a designated router. Designated routers are required to produce an actual pseudonode.

Examples   The following example enables NLSP to keep backup router and service information for potential pseudonode:

```
ipx potential-pseudonode
```

ipx rip-max-packetsize

✎

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

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

   ipx rip-max-packetsize *bytes*

   no ipx rip-max-packetsize *bytes*

Syntax Description

bytes	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each, plus 32 bytes of IPX network and RIP header information.

Defaults   432 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 RIP header information.

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

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

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

■ **Novell IPX**

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

ipx rip-multiplier

✎

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

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

ipx rip-multiplier *multiplier*

no ipx rip-multiplier *multiplier*

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

Defaults   Three times the RIP 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 RIP updates are sent once every 2 minutes, the interval at which RIP entries age out is set to 10 minutes:

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

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

ipx rip-queue-maximum

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

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

ipx rip-queue-maximum *milliseconds*

no ipx rip-queue-maximum *milliseconds*

Syntax Description

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

Defaults No queue limit is set.

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

Examples The following example sets a RIP queue maximum of 500 milliseconds:

```
ipx rip-queue-maximum 500
```

Related Commands	Command	Description
	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 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 rip-response-delay

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

To change the delay when responding to Routing Information Protocol (RIP) requests, use the **ipx rip-response-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx rip-response-delay *ms*

no ipx rip-response-delay

Syntax Description

ms	Delay time, in milliseconds, for RIP responses.

Defaults   No delay in answering (0 ms).

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 slows down the Cisco router and allows another router to answer first and become the router of choice. A delay in responding to RIP requests can be imposed so that, in certain topologies, any local Novell IPX router or any third-party IPX router can respond to the RIP requests before the Cisco router responds.

Optimal delay time is the same as or slightly longer than the time it takes the other router to answer.

Examples   The following example sets the delay in responding to RIP requests to 55 ms (0.055 seconds):

```
ipx rip-response-delay 55
```

Related Commands	Command	Description
	ipx gns-response-delay	Changes the delay when responding to GNS requests.
	ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
	ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.

ipx rip-update-queue-maximum

✎

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

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

> **ipx rip-update-queue-maximum** *queue-maximum*

> **no ipx rip-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 rip-update-queue-maximum** command to control how many incoming RIP update packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming RIP update packets are dropped.

✎

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

Novell IPX

Examples   The following example sets a RIP update queue maximum of 500:

```
ipx rip-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 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 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 route

✎

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

To add a static route or static NetWare Link Services Protocol (NLSP) route summary to the routing table, use the **ipx route** command in global configuration mode. To remove a route from the routing table, use the **no** form of this command.

ipx route {*network* [*network-mask*] | **default**} {*network.node* | *interface*} [*ticks*] [*hops*] [**floating-static**]

no ipx route

Syntax Description		
network	Network to which you want to establish a static route.	
	This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.	
network-mask	(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the *network* argument, it specifies the static route summary.	
	The high-order bits of *network-mask* must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.	
default	Creates a static entry for the "default route." The router forwards all nonlocal packets for which no explicit route is known via the specified next hop address (*network.node*) or interface.	
network.node	Router to which to forward packets destined for the specified network.	
	The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading 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 router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).	
interface	Network interface to which to forward packets destined for the specified network. Interface is serial 0 or serial 0.2. Specifying an interface instead of a network node is intended for use on IPXWAN unnumbered interfaces. The specified interface can be a null interface.	

ticks	(Optional) Number of IBM clock ticks of delay to the network for which you are establishing a static route. One clock tick is 1/18 of a second (approximately 55 ms). Valid values are 1 through 65,534.
hops	(Optional) Number of hops to the network for which you are establishing a static route. Valid values are 1 through 254.
floating-static	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.

Defaults   No static routes are predefined.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following arguments and keywords were added: • *network-mask* • **default** • *interface* • **floating-static**
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.

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

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

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

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

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

Examples

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

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

The following example defines a static NLSP route summary:

```
ipx routing
ipx route aaaa0000 ffff0000
```

Related Commands

Command	Description
ipx default-route	Forwards to the default network all packets for which a route to the destination network is unknown.
show ipx route	Displays the contents of the IPX routing table.

ipx route-cache

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

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

ipx route-cache

no ipx route-cache

Syntax Description   This command has no arguments or keywords.

Defaults   Fast switching is 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   Fast switching allows higher throughput by switching packets using a cache created by previous transit packets. Fast switching is enabled by default on all interfaces that support fast switching, including Token Ring, Frame Relay, PPP, Switched Multimegabit Data Service (SMDS), and ATM.

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

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

> **Note** CiscoBus (Cbus) switching of IPX packets is not supported on the MultiChannel Interface Processor (MIP) interface.

Examples The following example enables fast switching on an interface:

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

The following example disables fast switching on an interface:

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

Related Commands	**Command**	**Description**
	clear ipx cache	Deletes entries from the IPX fast-switching cache.
	ipx watchdog	Causes the Cisco IOS software to respond to the watchdog packets of a server on behalf of a remote client.
	show ipx cache	Displays the contents of the IPX fast-switching cache.
	show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx route-cache inactivity-timeout

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

To adjust the period and rate of route cache invalidation because of inactivity, use the **ipx route-cache inactivity-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

   ipx route-cache inactivity-timeout *period* [*rate*]

   no ipx route-cache inactivity-timeout

Syntax Description

period	Number of minutes that a valid cache entry may be inactive before it is invalidated. Valid values are 0 through 65,535. A value of zero disables this feature.
rate	(Optional) Maximum number of inactive entries that may be invalidated per minute. Valid values are 0 through 65,535. A value of zero means no limit.

Defaults   The default period is 2 minutes. The default rate is 0 (cache entries do not age).

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   IPX fast-switch cache entries that are not in use may be invalidated after a configurable period of time. If no new activity occurs, these entries will be purged from the route cache after one additional minute.

Cache entries that have been uploaded to the switch processor when autonomous switching is configured are always exempt from this treatment.

This command has no effect if silicon switching is configured.

Examples   The following example sets the inactivity period to 5 minutes, and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache inactivity-timeout 5 10
```

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
ipx route-cache	Enables IPX fast switching.
ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache max-size

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

To set a maximum limit on the number of entries in the IPX route cache, use the **ipx route-cache max-size** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipx route-cache max-size *size*

no ipx route-cache max-size

Syntax Description	*size*	Maximum number of entries allowed in the IPX route cache.

Defaults   The default setting is no limit on the number of entries.

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   On large networks, storing too many entries in the route cache can use a significant amount of router memory, causing router processing to slow. This situation is most common on large networks that run network management applications for NetWare. If the network management station is responsible for managing all clients and servers in a very large (greater than 50,000 nodes) Novell network, the routers on the local segment can become inundated with route cache entries. The **ipx route-cache max-size** command allows you to set a maximum number of entries for the route cache.

If the route cache already has more entries than the specified limit, the extra entries are not deleted. However, all route cache entries are subject to being removed via the parameter set for route cache aging via the **ipx route-cache inactivity-timeout** command.

Examples The following example sets the maximum route cache size to 10,000 entries.

```
ipx route-cache max-size 10000
```

Related Commands	Command	Description
	ipx route-cache	Enables IPX fast switching.
	ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
	ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
	show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache update-timeout

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

To adjust the period and rate of route cache invalidation because of aging, use the **ipx route-cache update-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache update-timeout *period* [*rate*]

no ipx route-cache update-timeout

Syntax Description

period	Number of minutes since a valid cache entry was created before it may be invalidated. A value of zero disables this feature.
rate	(Optional) Maximum number of aged entries that may be invalidated per minute. A value of zero means no limit.

Defaults The default setting is 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 IPX fast-switch cache entries that exceed a minimum age may be invalidated after a configurable period of time. Invalidation occurs unless the cache entry was marked as active during the last minute. Following invalidation, if no new activity occurs, these entries will be purged from the route cache after one additional minute.

This capability is primarily useful when autonomous switching or silicon switching is enabled. In both cases, activity is not recorded for entries in the route cache, because data is being switched by the Switch Processor (SP) or Silicon Switch Processor (SSP). In this case, it may be desirable to periodically invalidate a limited number of older cache entries each minute.

If the end hosts have become inactive, the cache entries will be purged after one additional minute. If the end hosts are still active, the route cache and autonomous or SSP cache entries will be revalidated instead of being purged.

Examples

The following example sets the update timeout period to 5 minutes and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache update-timeout 5 10
```

Related Commands	Command	Description
	clear ipx cache	Deletes entries from the IPX fast-switching cache.
	iipx route-cache	Enables IPX fast switching.
	ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
	show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx router

✎

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

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

> **ipx router** {**eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip**}

> **no ipx router** {**eigrp** *autonomous-system-number* | **nlsp** [*tag*] | **rip**}

Syntax Description

eigrp *autonomous-system-number*	Enables the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol. The argument *autonomous-system-number* is the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
nlsp [*tag*]	Enables the NetWare Link Services Protocol (NLSP) routing protocol. The optional argument *tag* names the NLSP process to which you are assigning the NLSP protocol. If the router has only one process, defining a *tag* is optional. A maximum of three NLSP processes may be configured on the router at the same time. The *tag* can be any combination of printable characters.
rip	Enables the Routing Information Protocol (RIP) routing protocol. It is on by default.

Defaults RIP is enabled.

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The following keyword and argument were added: • **nlsp** • *tag*
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.

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

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

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.

When you specify an NLSP *tag*, you configure the NLSP routing protocol for a particular 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.

Examples   The following example enables Enhanced IGRP:

```
ipx router eigrp 4
```

The following example enables NLSP on process area1. This process handles routing for NLSP area 1.

```
ipx router nlsp area1
```

Related Commands

Command	Description
network	Enables Enhanced IGRP.
redistribute (IPX)	Redistributes from one routing domain into another.

ipx router-filter

✎

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

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

ipx router-filter {*access-list-number* | *name*}

no ipx router-filter

Syntax Description		
access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	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.
	15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

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

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

```
access-list 866 permit 3c.0000.00c0.047d

interface ethernet 0
 ipx router-filter 866
```

Related Commands	Command	Description
	access-list (IPX extended)	Defines an extended Novell IPX access list.
	access-list (IPX standard)	Defines a standard IPX access list.
	deny (extended)	Sets conditions for a named IPX extended access list.
	deny (standard)	Sets conditions for a named IPX access list.
	ipx access-list	Defines an IPX access list by name.
	ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
	ipx output-network-filter (RIP)	Controls the list of networks included in routing updates sent out an interface.
	permit (IPX extended)	Sets conditions for a named IPX extended access list.
	prc-interval	Sets conditions for a named IPX access list.

ipx router-sap-filter

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

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

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

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

Syntax Description

access-list-number	Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults No filters are predefined.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 issue only one **ipx router-sap-filter** command on each interface.

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

```
access-list 1000 permit aa.0207.0104.0874
access-list 1000 deny -1

interface ethernet 0
 ipx router-sap-filter 1000
```

Related Commands	Command	Description
	access-list (SAP filtering)	Defines an access list for filtering SAP requests.
	deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
	ipx access-list	Defines an IPX access list by name.
	ipx 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 sap	Specifies static SAP entries.
	permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
	show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx routing

✎

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

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

ipx routing [*node*]

no ipx routing

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

Defaults Disabled

Command Modes Global configuration

Command Historyi	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.

internal-network 1

Usage Guidelines The **ipx routing** command enables IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) services.

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

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

Examples   The following example enables IPX routing:

```
ipx routing
```

Novell IPX ■

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