Cisco IOS Novell IPX Commands

Novell Internet Packet Exchange (IPX) is derived from the Xerox Network Systems (XNS) Internet Datagram Protocol (IDP). One major difference between the IPX and XNS protocols is that they do not always use the same Ethernet encapsulation format. A second difference is that IPX uses Novell's proprietary Service Advertising Protocol (SAP) to advertise special network services.

Our implementation of Novell's IPX protocol has been certified as providing full IPX device functionality.

Use the commands in this book to configure and monitor Novell IPX networks. For IPX configuration information and examples, see the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*, Release 12.2.

Note For all commands that previously used the keyword **novell**, this keyword has been changed to **ipx**. You can still use the keyword **novell** in all commands.

access-list (IPX extended)

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

To define an extended Novell IPX access list, use the extended version of the **access-list** command in global configuration mode. To remove an extended access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[*.source-node*] *source-node-mask*] | [*.source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[*.destination-node*] *destination-node-mask*] | [*.destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[*.source-node*] *source-node-mask*] | [*.source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[*.destination-node*] *destination-node-mask*] | [*.destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

access-list-number	Number of the access list. This is a number from 900 to 999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. Table 8 in the "Usage Guidelines" section lists some IPX protocol names and numbers.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.

source-socket	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. Table 9 in the "Usage Guidelines" section lists some IPX socket names and numbers.
destination.network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent. Table 9 in the "Usage Guidelines" section lists some IPX socket names and numbers.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

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

Release	Modification
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

Extended IPX access lists filter on protocol type. All other parameters are optional.

If a network mask is used, all other fields are required.

Use the **dipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface. The access list filters all outgoing packets on the interface.

Note For some versions of NetWare, the protocol type field is not a reliable indicator of the type of packet encapsulated by the IPX header. In these cases, use the source and destination socket fields to make this determination. For additional information, contact Novell.

Table 8 lists some IPX protocol names and numbers. Table 9 lists some IPX socket names and numbers. For additional information about IPX protocol numbers and socket numbers, contact Novell.

Table 8 Some IPX Protocol Names and Numbers

IPX Protocol Number (Decimal)	IPX Protocol Name	Protocol (Packet Type)
-1	any	Wildcard; matches any packet type in 900 lists.
0		Undefined; refer to the socket number to determine the packet type.
1	rip	Routing Information Protocol (RIP).
4	sap	Service Advertising Protocol (SAP).
5	spx	Sequenced Packet Exchange (SPX).
17	ncp	NetWare Core Protocol (NCP).
20	netbios	IPX NetBIOS.

Table 9 Some IPX Socket Names and Numbers

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
0	all	Wildcard used to match all sockets.
2	cping	Cisco IPX ping packet.

Table 9 Some IPX Socket Names and Numbers (continued)

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
451	ncp	NetWare Core Protocol (NCP) process.
452	sap	Service Advertising Protocol (SAP) process.
453	rip	Routing Information Protocol (RIP) process.
455	netbios	Novell NetBIOS process.
456	diagnostic	Novell diagnostic packet.
457		Novell serialization socket.
4000-7FFF		Dynamic sockets; used by workstations for interaction with file servers and other network servers.
8000-FFFF		Sockets as assigned by Novell, Inc.
85BE	eigrp	IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP).
9086	nping	Novell standard ping packet.

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

no access-list *access-list-number*

To delete the access list for a specific protocol, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *protocol*

Examples

The following example denies access to all RIP packets from the RIP process socket on source network 1 that are destined for the RIP process socket on network 2. It permits all other traffic. This example uses protocol and socket names rather than hexadecimal numbers.

```
access-list  900  deny  -1 1 rip 2 rip
access-list  900  permit  -1
```

The following example permits type 2 packets from any socket from host 10.0000.0C01.5234 to access any sockets on any node on networks 1000 through 100F. It denies all other traffic (with an implicit deny all):

Note This type is chosen only as an example. The actual type to use depends on the specific application.

```
access-list 910 permit 2 10.0000.0C01.5234 0000.0000.0000 0
  1000.0000.0000.0000 F.FFFF.FFFF.FFFF 0
```

The following example provides a time range to the access list:

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

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
cdeny (extended)	Sets conditions for a named IPX extended access list.
dipx access-group	Applies generic input and output filters to an interface.
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	Controls which servers are included in the GNS responses sent by the Cisco IOS software.
ipx router-filter	Filters the devices from which packets are accepted.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list (IPX standard)

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

To define a standard IPX access list, use the standard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source-network*[*.source-node*[*source-node-mask*]] [*destination-network*[*.destination-node* [*destination-node-mask*]]]

no access-list *access-list-number* {**deny** | **permit**} *source-network*[*.source-node*[*source-node-mask*]] [*destination-network*[*.destination-node* [*destination-node-mask*]]]

Syntax Description

access-list-number	Number of the access list. This is a number from 800 to 899.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are predefined.

Command Modes Global configuration

Command History

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

Usage Guidelines Standard IPX access lists filter on the source network. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. The access list filters all outgoing packets on the interface.

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

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *source-network*

Examples The following example denies access to traffic from all IPX networks (-1) to destination network 2:

```
access-list 800 deny -1 2
```

The following example denies access to all traffic from IPX address 1.0000.0c00.1111:

```
access-list 800 deny 1.0000.0c00.1111
```

The following example denies access from all nodes on network 1 that have a source address beginning with 0000.0c:

```
access-list 800 deny 1.0000.0c00.0000 0000.00ff.ffff
```

The following example denies access from source address 1111.1111.1111 on network 1 to destination address 2222.2222.2222 on network 2:

```
access-list 800 deny 1.1111.1111.1111 0000.0000.0000 2.2222.2222.2222 0000.0000.0000
```

or

```
access-list 800 deny 1.1111.1111.1111 2.2222.2222.2222
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
dipx access-group	Applies generic input and output filters to an interface.
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	Controls the list of networks included in routing updates sent out an interface.
ipx router-filter	Filters the devices from which packets are accepted.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list (NLSP)

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

To define an access list that denies or permits area addresses that summarize routes, use the NetWare Link-Services Protocol (NLSP) route aggregation version of the **access-list** command in global configuration mode. To remove an NLSP route aggregation access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

no access-list *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description

access-list-number	Number of the access list. This is a number from 1200 to 1299.
deny	Denies redistribution of explicit routes if the conditions are matched. If you have enabled route summarization with route-aggregation command, the device redistributes an aggregated route instead.
permit	Permits redistribution of explicit routes if the conditions are matched.
network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary. 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.
interface	(Optional) Interface on which the access list should be applied to incoming updates.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults No access lists are predefined.

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0	The *interface* argument 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 in12.2S-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 the NLSP route aggregation access list in the following situations:

- When redistributing from an Enhanced IGRP or RIP area into a new NLSP area.

  Use the access list to instruct the device to redistribute an aggregated route instead of the explicit route. The access list also contains a "permit all" statement that instructs the device to redistribute explicit routes that are not subsumed by a route summary.

- When redistributing from an NLSP version 1.0 area into an NLSP version 1.1 area, and vice versa.

  From an NLSP version 1.0 area into an NLSP version 1.1 area, use the access list to instruct the device to redistribute an aggregated route instead of an explicit route and to redistribute explicit routes that are not subsumed by a route summary.

  From an NLSP version 1.1 area into an NLSP version 1.0 area, use the access list to instruct the device to filter aggregated routes from passing into the NLSP version 1.0 areas and to redistribute explicit routes instead.

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

Examples

The following example uses NLSP route aggregation access lists to redistribute routes learned from RIP to NLSP area1. Routes learned via RIP are redistributed into NLSP area1. Any routes learned via RIP that are subsumed by aaaa0000 ffff0000 are not redistributed. An address summary is generated instead.

```
ipx routing
ipx internal-network 2000

interface ethernet 1
 ipx network 1001
 ipx nlsp area1 enable

interface ethernet 2
 ipx network 2001
```

```
access-list 1200 deny aaaa0000 ffff0000
access-list 1200 permit -1

ipx router nlsp area
 area-address 1000 fffff000
 route-aggregation
 redistribute rip access-list 1200
```

Related Commands

Command	Description
area-address (NLSP)	Defines a set of network numbers to be part of the current NLSP area.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-list	Defines an IPX access list by name.
ipx nlsp enable	Configures the interval between the transmission of hello packets.
ipx router	Specifies the routing protocol to use.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.
prc-interval	Controls the hold-down period between partial route calculations.
redistribute (IPX)	Redistributes from one routing domain into another.

access-list (SAP filtering)

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

To define an access list for filtering Service Advertising Protocol (SAP) requests, use the SAP filtering form of the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

access-list-number	Number of the SAP access list. This is a number from 1000 to 1099.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	(Optional) Node specified on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.node-mask	(Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. Table 10 in the "Usage Guidelines" section lists examples of service types.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (" ") to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Table 10 lists some sample IPX SAP types. For more information about SAP types, contact Novell. Note that in the filter (specified by the *service-type* argument), we define a value of 0 to filter all SAP services. If, however, you receive a SAP packet with a SAP type of 0, this indicates an unknown service.

Table 10 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
1	User
2	User group
3	Print server queue
4	File server
5	Job server
7	Print server
9	Archive server
A	Queue for job servers
21	Network Application Support Systems Network Architecture (NAS SNA) gateway
2D	Time Synchronization value-added process (VAP)
2E	Dynamic SAP
47	Advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES—NetWare for Virtual Memory System (VMS)
98	NetWare access server
9A	Named Pipes server
9E	Portable NetWare—UNIX

Table 10 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
107	RCONSOLE
111	Test server
166	NetWare management (Novell's Network Management Station [NMS])
26A	NetWare management (NMS console)

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

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *network*

Examples

The following access list blocks all access to a file server (service Type 4) on the directly attached network by resources on other Novell networks, but allows access to all other available services on the interface:

```
access-list 1001 deny -1 4
access-list 1001 permit -1
```

Related Commands

Command	Description
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-gns-filter	Controls which servers are included in the GNS 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 device.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

area-address (NLSP)

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

To define a set of network numbers to be part of the current NetWare Link-Services Protocol (NLSP) area, use the **area-address** command in device configuration mode. To remove a set of network numbers from the current NLSP area, use the **no** form of this command.

area-address *address mask*

no area-address *address mask*

Syntax Description

address	Network number prefix. This is a 32-bit hexadecimal number.
mask	Mask that defines the length of the network number prefix. This is a 32-bit hexadecimal number.

Defaults

No area address is defined by default.

Command Modes

Device 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

You must configure at least one area address before NLSP will operate.

The **area-address** command defines a prefix that includes all networks in the area. This prefix allows a single route to an area address to substitute for a longer list of networks.

All networks on which NLSP is enabled must fall under the area address prefix. This configuration is for future compatibility. When Level 2 NLSP becomes available, the only route advertised for the area will be the area address prefix (the prefix represents all networks within the area).

All devices in an NLSP area must be configured with a common area address, or they will form separate areas. You can configure up to three area addresses on the device.

The area address must have zero bits in all bit positions where the mask has zero bits. The mask must consist of only left-justified contiguous one bits.

Examples

The following example defines an area address that includes networks AAAABBC0 through AAAABBDF:

```
area-address AAAABBC0 FFFFFFE0
```

The following example defines an area address that includes all networks:

```
area-address 0 0
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

clear ipx accounting

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

To delete all entries in the accounting database when IPX accounting is enabled, use the **clear ipx accounting** command in EXEC mode.

clear ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Clears the checkpoint database.

Command Modes

EXEC

Command History

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

Usage Guidelines

Specifying the **clear ipx accounting** command with no keywords copies the active database to the checkpoint database and clears all entries in the active database. When cleared, active database entries and static entries, such as those set by the **ipx accounting-list** command, are reset to zero. Dynamically found entries are deleted.

Any traffic that traverses the device after you issue the **clear ipx accounting** command is saved in the active database. Accounting information in the checkpoint database at that time reflects traffic prior to the most recent **clear ipx accounting** command.

You can also delete all entries in the active and checkpoint database by issuing the **clear ipx accounting** command twice in succession.

Examples

The following example first displays the contents of the active database before the contents are cleared. Then, the **clear ipx accounting** command clears all entries in the active database. As a result, the **show ipx accounting** command shows that there is no accounting information in the active database. Lastly, the **show ipx accounting checkpoint** command shows that the contents of the active database were copied to the checkpoint database when the **clear ipx accounting** command was issued.

```
Device# show ipx accounting

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

Accounting data age is      6

Device# clear ipx accounting
Device# show ipx accounting

Source                  Destination               Packets           Bytes

Accounting data age is      0

Device# show ipx accounting checkpoint

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

Accounting data age is      6
```

Related Commands

Command	Description
ipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

clear ipx cache

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

To delete entries from the IPX fast-switching cache, use the **clear ipx cache** command in EXEC mode.

clear ipx cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

The **clear ipx cache** command clears entries used for fast switching and autonomous switching.

Examples

The following example deletes all entries from the IPX fast-switching cache:

```
clear ipx cache
```

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
show ipx cache	Displays the contents of the IPX fast-switching cache.

clear ipx nhrp

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

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ipx nhrp** command in EXEC mode.

clear ipx nhrp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1v	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 does not clear any static (configured) IPX-to-NBMA address mappings from the NHRP cache.

Examples

The following example clears all dynamic entries from the NHRP cache for the interface:

```
clear ipx nhrp
```

Related Commands

Command	Description
show ipx nhrp	Displays the NHRP cache.

clear ipx nlsp neighbors

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

To delete all NetWare Link Services Protocol (NLSP) adjacencies from the adjacency database of Cisco IOS software, use the **clear ipx nlsp neighbors** command in EXEC mode.

clear ipx nlsp [*tag*] **neighbors**

Syntax Description

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

Command Modes EXEC

Command History

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

Usage Guidelines Deleting all entries from the adjacency database forces all devices in the area to perform the shortest path first (SPF) calculation.

When you specify an NLSP tag, the device clears all NLSP adjacencies discovered by that NLSP process. An NLSP process is a device's databases working together to manage route information about an area. NLSP version 1.0 devices are always in the same area. Each device 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 devices that exist within a single area also use a single process.

NLSP version 1.1 devices that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These devices 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 device. 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 device interconnects multiple NLSP areas.

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

Examples

The following example deletes all NLSP adjacencies from the adjacency database:

```
clear ipx nlsp neighbors
```

The following example deletes the NLSP adjacencies for process area2:

```
clear ipx nlsp area2 neighbors
```

Related Commands

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

clear ipx route

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

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

clear ipx route {*network* [*network-mask*] | **default** | *****}

Syntax Description

network	Number of the network whose routing table entry you want to delete. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to 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 an NLSP route summary to clear. The high-order bits specified for the *network-mask* argument 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	Deletes the default route from the routing table.
*	Deletes all routes in the routing table.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keyword and argument were added: • *network-mask* • **default**
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.

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

Usage Guidelines

After you use the **clear ipx route** command, RIP/SAP general requests are issued on all IPX interfaces.

For devices configured for NLSP route aggregation, use this command to clear an aggregated route from the routing table.

Examples

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

```
clear ipx route 3
```

The following example clears a route summary entry from the IPX routing table:

```
clear ipx route ccc00000 fff00000
```

Related Commands

Command	Description
show ipx route	Displays the contents of the IPX routing table.

clear ipx sap

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

To clear IPX SAP entries from the IPX routing table, use the **clear ipx sap** command in EXEC mode.

clear ipx sap {***** | *sap-type* | *sap-name*}

Syntax Description

*****	Clears all IPX SAP service entries by marking them invalid.
sap-type	Specifies the type of services that you want to clear by marking as invalid. This is an four-digit hexadecimal number that uniquely identifies a service type. It can be a number in the range 1 to FFFF. You do not need to specify leading zeros in the service number. For example, for the service number 00AA, you can enter AA.
sap-name	Specifies a certain name of service so that you can clear IPX SAP service entries that begin with the specified name. The name can be any contiguous string of printable ASCII characters. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters. For example, to clear all services that begin with the name "accounting," enter the command clear ipx sap accounting* to clear all services that begin with the name "accounting". Use double quotation marks (“ ”) to enclose strings containing embedded spaces.

Command Modes

EXEC

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

You can use the **clear ipx sap** command to research problems with the service table.

Examples

The following example clears all service entries from the IPX routing table:

```
clear ipx sap *
```

clear ipx traffic

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

To clear IPX protocol and NetWare Link Services Protocol (NLSP) traffic counters, use the **clear ipx traffic** command in privileged EXEC mode.

clear ipx [**nlsp**] **traffic**

Syntax Description

nlsp	(Optional) Clears only the NLSP traffic counters and leaves other IPX traffic counters intact.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(1)T	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 the **show ipx traffic since bootup** command to recall traffic statistics that have been previously cleared.

Examples The following example clears all IPX traffic statistics:

```
clear ipx traffic
```

Related Commands

Command	Description
show ipx traffic	Displays information about the number and type of IPX packets sent and received.

deny (extended)

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

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

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

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

Syntax Description

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

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

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

Usage Guidelines

Use this command following the **ipx accounting** command to specify conditions under which a packet cannot pass the named access list.

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

Examples

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

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

The following example provides a time range to deny access :

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

Related Commands

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

deny (NLSP)

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

To filter explicit routes and generate an aggregated route for a named NetWare Link Services Protocol (NLSP) route aggregation access list, use the **deny** command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

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

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

Syntax Description

network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary, expressed as an 8-digit hexadecimal number. The high-order bits of *network-mask* must be contiguous 1s, while the low-order bits must be contiguous zeros (0). An arbitrary mix of 1s and 0s is not permitted.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

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

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

Usage Guidelines

Use this command following the **ipx access-list** command to prevent the redistribution of explicit networks that are denied by the access list entry and, instead, generate an appropriate aggregated (summary) route.

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

Examples

The following example from a configuration file defines the access list named *finance* for NLSP route aggregation. This access list prevents redistribution of explicit routes in the range 12345600 to 123456FF and, instead, summarizes these routes into a single aggregated route. The access list allows explicit route redistribution of all other routes.

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

Related Commands

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

deny (SAP filtering)

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

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

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

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

Syntax Description

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

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

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

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

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet cannot pass the named access list.

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

Examples

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

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

Related Commands

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

deny (standard)

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

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

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

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

Syntax Description

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

Defaults No access lists are defined.

Command Modes Access-list configuration

Command History

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

Usage Guidelines Use this command following the **ipx access-list** command to specify conditions under which a packet cannot pass the named access list.

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

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

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

Related Commands

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

distribute-list in

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

To filter networks received in updates, use the **distribute-list in** command in device configuration mode. To change or cancel the filter, use the **no** form of this command.

distribute-list {*access-list-number* | *name*} **in** [*interface-name*]

no distribute-list {*access-list-number* | *name*} **in** [*interface-name*]

Syntax Description

access-list-number	Standard IPX access list number in the range 800 to 899 or NLSP access list number in the range 1200 to 1299. The list explicitly specifies which networks are to be received and which are to be suppressed.
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.
in	Applies the access list to incoming routing updates.
interface-name	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

Defaults

Disabled

Command Modes

Device configuration

Command History

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

Examples

The following example causes only two networks—network 2 and network 3—to be accepted by an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process:

```
access-list 800 permit 2
access-list 800 permit 3
access-list 800 deny -1
!
ipx router eigrp 100
 network 3
 distribute-list 800 in
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
access-list (NLSP)	Defines an access list that denies or permits area addresses that summarize routes.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
deny (standard)	Sets conditions for a named IPX access list.
distribute-list out	Suppresses networks from being advertised in updates.
ipx access-list	Defines an IPX access list by name.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.
prc-interval	Sets conditions for a named IPX access list.
redistribute (IPX)	Redistributes from one routing domain into another.

distribute-list out

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

To suppress networks from being advertised in updates, use the **distribute-list out** command in device configuration mode. To cancel this function, use the **no** form of this command.

distribute-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

no distribute-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

Syntax Description

access-list-number	Standard IPX access list number in the range 800 to 899 or NLSP access list number in the range 1200 to 1299. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
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.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates. **Note** When you use the **distribute-list out** command after entering the **ipx router eigrp** command to enable the Enhanced Interior Gateway Routing Protocol (EIGRP), you must use the *interface-name* argument. If you do not specify an interface, the devices will not exchange any routes or SAPs with their neighbors.
routing-process	(Optional) Name of a particular routing process as follows: • **eigrp** *autonomous-system-number* • **rip** • **nlsp** [*tag*]

Defaults Disabled

Command Modes Device configuration

Command History

Release	Modification
10.0	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.
12.2(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 redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list out** command. This causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list out** command without a process name argument is applied. Addresses not specified in the **distribute-list out** command are not advertised in outgoing routing updates.

Examples

The following example causes only one network—network 3—to be advertised by an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process:

```
access-list 800 permit 3
access-list 800 deny -1
!
ipx router eigrp 100
 network 3
 distribute-list 800 out
```

Related Commands

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

Command	Description
prc-interval	Sets conditions for a named IPX access list.
redistribute (IPX)	Redistributes from one routing domain into another.

distribute-sap-list in

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

To filter services received in updates, use the **distribute-sap-list in** command in device configuration mode. To change or cancel the filter, use the **no** form of this command.

distribute-sap-list {*access-list-number* | *name*} **in** [*interface-name*]

no distribute-sap-list {*access-list-number* | *name*} **in** [*interface-name*]

Syntax Description

access-list-number	SAP access list number in the range 1000 to 1099. The list explicitly specifies which services are to be received and which are to be suppressed.
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.
interface-name	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

Defaults

Disabled

Command Modes

Device 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.

Examples

In the following example, the device redistributes Enhanced Interior Gateway Routing Protocol (EIGRP) into NetWare Link Services Protocol (NLSP) area 1. Only services for network 2 and 3 are accepted by the NLSP routing process.

```
access-list 1000 permit 2
access-list 1000 permit 3
access-list 1000 deny -1
!
ipx router nlsp area1
 redistribute eigrp
 distribute-sap-list 1000 in
```

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.
distribute-list out	Suppresses networks from being advertised in updates.
ipx access-list	Defines an IPX access list by name.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
redistribute (IPX)	Redistributes from one routing domain into another.

distribute-sap-list out

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

To suppress services from being advertised in SAP updates, use the **distribute-sap-list out** command in device configuration mode. To cancel this function, use the **no** form of this command.

distribute-sap-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

no distribute-sap-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

Syntax Description

access-list-number	SAP access list number in the range 1000 to 1099. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
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.
interface-name	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates. **Note** When you use the **distribute-sap-list out** command after entering the **ipx router eigrp** command to enable the Enhanced Interior Gateway Routing Protocol (EIGRP), you must use the *interface-name* argument. If you do not specify an interface, the devices will not exchange any routes or SAPs with their neighbors.
routing-process	(Optional) Name of a particular routing process as follows: • **eigrp** *autonomous-system-number* • **nlsp** [*tag*] • **rip**

Defaults Disabled

Command Modes Device 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 redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-sap-list out** command. This causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-sap-list out** command without a process name argument is applied. Addresses not specified in the **distribute-sap-list out** command are not advertised in outgoing routing updates.

Examples

The following example causes only services from network 3 to be advertised by an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process:

```
access-list 1010 permit 3
access-list 1010 deny -1
!
ipx router eigrp 100
 network 3
 distribute-sap-list 1010 out
```

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.
distribute-sap-list in	Filters services received in updates.
ipx access-list	Defines an IPX access list by name.
ipx router	Specifies the routing protocol to use.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
redistribute (IPX)	Redistributes from one routing domain into another.

ipx access-group

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

To apply generic input and output filters to an interface, use the **ipx access-group** command in interface configuration mode. To remove filters, use the **no** form of this command.

ipx access-group {*access-list-number* | *name*} [**in** | **out**]

no ipx access-group {*access-list-number* | *name*} [**in** | **out**]

Syntax Description

access-list-number	Number of the access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, the value for the *access-list-number* argument 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.
in	(Optional) Filters inbound packets. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list.
out	(Optional) Filters outbound packets. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. This is the default when you do not specify an input (**in**) or output (**out**) keyword in the command line.

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

Generic filters control which data packets an interface receives or sends out based on the packet source and destination addresses, IPX protocol type, and source and destination socket numbers. You use the standard **access-list** and extended **access-list** commands to specify the filtering conditions.

You can apply only one input filter and one output filter per interface or subinterface.

When you do not specify an input (**in**) or output (**out**) filter in the command line, the default is an output filter.

You cannot configure an output filter on an interface where autonomous switching is already configured. Similarly, you cannot configure autonomous switching on an interface where an output filter is already present. You cannot configure an input filter on an interface if autonomous switching is already configured on *any* interface. Likewise, you cannot configure input filters if autonomous switching is already enabled on *any* interface.

Examples

The following example applies access list 801 to Ethernet interface 1. Because the command line does not specify an input filter or output filter with the keywords **in** or **out**, the software assumes that it is an output filter.

```
interface ethernet 1
 ipx access-group 801
```

The following example applies access list 901 to Ethernet interface 0. The access list is an input filter access list as specified by the keyword **in**.

```
interface ethernet 0
 ipx access-group 901 in
```

To remove the input access list filter in the previous example, you must specify the **in** keyword when you use the **no** form of the command. The following example correctly removes the access list:

```
interface ethernet 0
 no ipx access-group 901 in
```

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 accounting	Defines an IPX access list by name.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

ipx access-list

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

To define an IPX access list by name, use the **ipx access-list** command in global configuration mode. To remove a named IPX access list, use the **no** form of this command.

ipx access-list {**standard** | **extended** | **sap** | **summary**} *name*

no ipx access-list {**standard** | **extended** | **sap** | **summary**} *name*

Syntax Description

standard	Specifies a standard IPX access list.
extended	Specifies an extended IPX access list.
sap	Specifies a SAP access list.
summary	Specifies area addresses that summarize routes using NLSP route aggregation filtering.
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

There is no default named IPX access list.

Command Modes

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

Usage Guidelines

Use this command to configure a named IPX access list as opposed to a numbered IPX access list. This command will take you into access-list configuration mode, where you must define the denied or permitted access conditions with the **deny** and **permit** commands.

Specifying **standard**, **extended**, **sap**, or **summary** with the **ipx access-list** command determines the prompt you get when you enter access-list configuration mode.

Caution Named access lists will not be recognized by any software release before Cisco IOS Release 11.3.

Examples

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

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

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

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

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

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

The following example creates a summary access list named finance that allows the redistribution of all explicit routes every 64 ticks:

```
ipx access-list summary finance
 permit -1 ticks 64
```

The following example provides a time range to an access list:

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

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
access-list (NLSP)	Defines an access list that denies or permits area addresses that summarize routes.
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
deny (standard)	Sets conditions for a named IPX access list.

Command	Description
permit (IPX extended)	Sets conditions for a named IPX extended access list.
permit (IPX standard)	Sets conditions for a named IPX access list.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
prc-interval	Controls the hold-down period between partial route calculations.
show ipx access-list	Displays the contents of all current IPX access lists.

ipx accounting

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

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

ipx accounting

no ipx accounting

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

IPX accounting allows you to collect information about IPX packets and the number of bytes that are switched through the Cisco IOS software. You collect information based on the source and destination IPX address. IPX accounting tracks only IPX traffic that is routed out an interface on which IPX accounting is configured; it does not track traffic generated by or terminated at the device itself.

The Cisco IOS software maintains two accounting databases: an active database and a checkpoint database. The active database contains accounting data tracked until the database is cleared. When the active database is cleared, its contents are copied to the checkpoint database. Using these two databases together allows you to monitor both current traffic and traffic that has previously traversed the device.

IPX accounting statistics will be accurate even if IPX access lists are being used or if IPX fast switching is enabled. Enabling IPX accounting significantly decreases performance of a fast switched interface.

IPX accounting does not keep statistics if autonomous switching is enabled. In fact, IPX accounting is disabled if autonomous or SSE switching is enabled.

Examples

The following example enables IPX accounting on Ethernet interface 0:

```
interface ethernet 0
 ipx accounting
```

Related Commands

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

ipx accounting-list

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

To filter networks for which IPX accounting information is kept, use the **ipx accounting-list** command in global configuration mode. To remove the filter, use the **no** form of this command.

ipx accounting-list *number mask*

no ipx accounting-list *number mask*

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The source and destination addresses of each IPX packet traversing the device are compared with the network numbers in the filter. If there is a match, accounting information about the IPX packet is entered into the active accounting database. If there is no match, the IPX packet is considered to be a transit packet and may be counted, depending on the setting of the **ipx accounting-transits** global configuration command.

Examples

The following example adds all networks with IPX network numbers beginning with 1 to the list of networks for which accounting information is kept:

```
ipx accounting-list 1 0000.0000.0000
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting	Enables IPX accounting.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

ipx accounting-threshold

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

To set the maximum number of accounting database entries, use the **ipx accounting-threshold** command in global configuration mode. To restore the default, use the **no** form of this command.

ipx accounting-threshold *threshold*

no ipx accounting-threshold *threshold*

Syntax Description

threshold	Maximum number of entries (source and destination address pairs) that the Cisco IOS software can accumulate.

Defaults

512 entries

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

The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates. The threshold is designed to prevent IPX accounting from consuming all available free memory. This level of memory consumption could occur in a device that is switching traffic for many hosts. To determine whether overflows have occurred, use the **show ipx accounting** EXEC command.

Examples

The following example sets the IPX accounting database threshold to 500 entries:

```
ipx accounting-threshold 500
```

Related Commands

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

ipx accounting-transits

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

To set the maximum number of transit entries that will be stored in the IPX accounting database, use the **ipx accounting-transits** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx accounting-transits *count*

no ipx accounting-transits

Syntax Description

count	Number of transit entries that will be stored in the IPX accounting database.

Defaults

0 entries

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.
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

Transit entries are those that do not match any of the networks specified by **ipx accounting-list** global configuration commands. If you have not defined networks with **ipx accounting-list** commands, IPX accounting tracks all traffic through the interface (all transit entries) up to the accounting threshold limit.

Examples

The following example specifies a maximum of 100 transit records to be stored in the IPX accounting database:

```
ipx accounting-transits 100
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
show ipx accounting	Displays the active or checkpoint accounting database.

ipx advertise-default-route-only (RIP)

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

To advertise only the default RIP route via the specified network, use the **ipx advertise-default-route-only** command in interface configuration mode. To advertise all known RIP routes out the interface, use the **no** form of this command.

ipx advertise-default-route-only *network*

no ipx advertise-default-route-only *network*

Syntax Description

network	Number of the network through which to advertise the default route.

Defaults

All known routes are advertised out the interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

If you specify the **ipx advertise-default-route-only** command, only a known default RIP route is advertised out the interface; no other networks will be advertised. If you have a large number of routes in the routing table, for example, on the order of 1000 routes, none of them will be advertised out the interface. However, if the default route is known, it will be advertised. Nodes on the interface can still reach any of the 1000 networks via the default route.

Specifying the **ipx advertise-default-route-only** command results in a significant reduction in CPU processing overhead when there are many routes and many interfaces. It also reduces the load on downstream devices.

This command applies only to RIP. Enhanced IGRP is not affected when you enable this command. It continues to advertise all routes that it knows about.

Note Not all devices recognize and support the default route. Use this command with caution if you are not sure if all devices in your network support the default route.

Examples

The following example enables the advertising of the default route only:

```
interface ethernet 1
 ipx network 1234
 ipx advertise-default-route-only 1234
```

Related Commands

Command	Description
ipx default-route	Forwards to the default network all packets for which a route to the destination network is unknown.

ipx advertise-to-lost-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 advertise-to-lost-route** command is not supported in Cisco IOS software.

To enable the sending of lost route mechanism packets, use the **ipx advertise-to-lost-route** command in global configuration mode. To disable the flooding of network down notifications that are not part of the Novell lost route algorithm, use the **no** form of this command.

ipx advertise-to-lost-route

no ipx advertise-to-lost-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

You may reduce congestion on slow WAN links when there are many changes in an unstable network by turning off part of the Novell lost route algorithm. To turn off part of the Novell lost route algorithm, use the **no ipx advertise-to-lost-route** command.

Note The side effect of disabling the Novell lost route algorithm is longer convergence times in networks with multiple paths to networks.

Examples The following example enables the Novell lost route algorithm:

```
ipx advertise-to-lost-route
```

ipx backup-server-query-interval (EIGRP)

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

To change the time between successive queries of each Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor's backup server table, use the **ipx backup-server-query-interval** command in global configuration mode. To restore the default time, use the **no** form of this command.

ipx backup-server-query-interval *interval*

no ipx backup-server-query-interval

Syntax Description

interval	Minimum time, in seconds, between successive queries of each Enhanced IGRP neighbor's backup server table. The default is 15 seconds.

Defaults

15 seconds

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

A lower interval may use more CPU resources, but may cause lost server information to be retrieved from other servers' tables sooner.

Examples

The following example changes the server query time to 5 seconds:

```
ipx backup-server-query-interval 5
```

ipx bandwidth-percent eigrp

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

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ipx bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx bandwidth-percent eigrp *as-number percent*

no ipx bandwidth-percent eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that Enhanced IGRP may use.

Defaults

50 percent

Command Modes

Interface 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.

Usage Guidelines

Enhanced IGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured; this may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows Enhanced IGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
interface serial 0
 bandwidth 56
 ipx bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipx router	Specifies the routing protocol to use.

ipx broadcast-fastswitching

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

To enable the device to fast switch IPX directed broadcast packets, use the **ipx broadcast-fastswitching** command in global configuration mode. To disable fast switching of IPX directed broadcast packets, use the **no** form of this command.

ipx broadcast-fastswitching

no ipx broadcast-fastswitching

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

The default behavior is to process switch directed broadcast packets.

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

A directed broadcast is one with a network layer destination address of the form net.ffff.ffff.ffff. The **ipx broadcast-fastswitching** command permits the device to fast switch IPX directed broadcast packets. This may be useful in certain broadcast-based applications that rely on helpering.

Note that the device never uses autonomous switching for eligible directed broadcast packets, even if autonomous switching is enabled on the output interface. Also note that routing and service updates are always exempt from this treatment.

Examples

The following example enables the device to fast switch IPX directed broadcast packets:

```
ipx broadcast-fastswitching
```

ipx default-output-rip-delay

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

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

ipx default-output-rip-delay *delay*

no ipx default-output-rip-delay

Syntax Description

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

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
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 default-output-rip-delay** command sets a default interpacket delay for all interfaces.

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

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

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

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

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

Examples

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

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

Related Commands

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

ipx default-output-sap-delay

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

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

ipx default-output-sap-delay *delay*

no ipx default-output-sap-delay

Syntax Description

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

Defaults

55 ms

Command Modes

Global configuration

Command History

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ipx default-route

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

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

ipx default-route

no ipx default-route

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
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 **no ipx default-route** command, Cisco IOS software no longer uses -2 as the default network. Instead, the software interprets -2 as a regular network and packets for which a route to the destination network is unknown are dropped.

Examples

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

```
no ipx default-route
```

Related Commands

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

ipx default-triggered-rip-delay

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

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

ipx default-triggered-rip-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ipx default-triggered-rip-holddown

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

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

ipx default-triggered-rip-holddown *milliseconds*

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

Syntax Description

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

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

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

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

Examples

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

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

Related Commands

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

ipx default-triggered-sap-delay

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

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

ipx default-triggered-sap-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

Global configuration

Command History

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ipx default-triggered-sap-holddown

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

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

ipx default-triggered-sap-holddown *milliseconds*

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

Syntax Description

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

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

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

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

Examples

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

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

Related Commands

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

ipx delay

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

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

ipx delay *ticks*

no ipx delay

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 delay** command sets the count used in the IPX RIP delay field, which is also known as the *ticks* field.

IPXWAN links determine their delay dynamically. If you do not specify the **ipx delay** command on an interface and you have not changed the interface delays with the **interface delay** interface configuration command, all LAN interfaces have a delay of 1 and all WAN interfaces have a delay of 6. The preferred

method of adjusting delays is to use the **ipx delay** command, not the **interface delay** command. The **show ipx interface** EXEC command display only the delay value configured with the **ipx delay** command.

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

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

Examples

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

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

Related Commands

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

ipx down

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

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

ipx down *network*

no ipx down

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

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

Examples

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

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

ipx eigrp-sap-split-horizon

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

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

ipx eigrp-sap-split-horizon

no ipx eigrp-sap-split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled on LANs and disabled on WANs.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

The following example disables split horizon on the device:

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

Related Commands

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

ipx encapsulation

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

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

ipx encapsulation *encapsulation-type*

no ipx encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	(Required) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 11.

Defaults

novell-etherZX

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

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

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

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

Table 11 describes the types of encapsulation available for specific interfaces.

Table 11 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell's Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0. For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header. For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
snap	For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header. For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

Examples

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

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

Related Commands

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

ipx flooding-unthrottled (NLSP)

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

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

ipx flooding-unthrottled

no ipx flooding-unthrottled

Syntax Description

This command has no arguments or keywords.

Defaults

Unthrottled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
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

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

Examples

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

```
ipx flooding-unthrottled
```

ipx gns-reply-disable

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

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

ipx gns-reply-disable

no ipx gns-reply-disable

Syntax Description

This command has no arguments or keywords.

Defaults

Replies are sent to IPX GNS queries.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

ipx gns-response-delay

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

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

ipx gns-response-delay [*milliseconds*]

no ipx gns-response-delay

Syntax Description

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

Defaults

0 (no delay)

Command Modes

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

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

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

It is desirable to have these end-host server systems get their reply to the client before the device does because the client typically takes the first response, not the best response. In this case the best response is the one from the local server.

NetWare 2.*x* has a problem with dual-connected servers in parallel with a device. If you are using this version of NetWare, you should set a GNS delay. A value of 500 ms is recommended.

In situations in which servers are always located across devices from their clients, there is no need for a delay to be imposed.

Examples

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

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

Related Commands

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

ipx gns-round-robin

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

To rotate using a round-robin selection method through a set of eligible servers when responding to Get Nearest Server (GNS) requests, use the **ipx gns-round-robin** command in global configuration mode. To use the most recently learned server, use the **no** form of this command.

ipx gns-round-robin

no ipx gns-round-robin

Syntax Description

This command has no arguments or keywords.

Defaults

The most recently learned eligible server is used.

Command Modes

Global configuration

Command History

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

Usage Guidelines

In the normal server selection process, requests for service are responded to with the most recently learned, closest server. If you enable the round-robin method, the Cisco IOS software maintains a list of the nearest servers eligible to provide specific services. It uses this list when responding to GNS requests. Responses to requests are distributed in a round-robin fashion across all active IPX interfaces on the device.

Eligible servers are those that satisfy the “nearest” requirement for a given request and that are not filtered either by a SAP filter or by a GNS filter.

Examples

The following example responds to GNS requests using a round-robin selection method from a list of eligible nearest servers:

```
ipx gns-round-robin
```

Related Commands

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

ipx hello-interval eigrp

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Examples

The following example changes the hello interval to 10 seconds:

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

Related Commands

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

ipx helper-address

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

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

ipx helper-address *network.node*

no ipx helper-address *network.node*

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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

Devices normally block all broadcast requests and do not forward them to other network segments. This is done to prevent the degradation of performance over the entire network. The **ipx helper-address** command allows broadcasts to be forwarded to other networks. This is useful when a network segment does not have an end-host capable of servicing a particular type of broadcast request. This command lets you forward the broadcasts to a server, network, or networks that can process them. Incoming unrecognized broadcast packets that match the access list created with the **ipx helper-list** command, if it is present, are forwarded.

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

The Cisco IOS software supports all-networks flooded broadcasts (sometimes referred to as *all-nets flooding*). These are broadcast messages that are forwarded to all networks. To configure the all-nets flooding, define the IPX helper address for an interface as follows:

```
ipx helper-address -1.FFFF.FFFF.FFFF
```

On systems configured for IPX routing, this helper address is displayed as follows (via the **show ipx interface** command):

```
FFFFFFFF.FFFF.FFFF.FFFF
```

Although our software takes care to keep broadcast traffic to a minimum, some duplication is unavoidable. When loops exist, all-nets flooding can propagate bursts of excess traffic that will eventually age out when the hop count reaches its limit (16 hops). Use all-nets flooding carefully and only when necessary. Note that you can apply additional restrictions by defining a helper list.

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

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

Examples

The following example forwards all-nets broadcasts on Ethernet interface 0 (except type 20 propagation packets) are forwarded to IPX server 00b4.23cd.110a on network bb:

```
interface ethernet 0
 ipx helper-address bb.00b4.23cd.110a
```

Related Commands

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

ipx helper-list

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

To assign an access list to an interface to control broadcast traffic (including type 20 propagation packets), use the **ipx helper-list** command in interface configuration mode. To remove the access list from an interface, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No access list is preassigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 helper-list** command specifies an access list to use in forwarding broadcast packets. One use of this command is to prevent client nodes from discovering services they should not use.

Because the destination address of a broadcast packet is by definition the broadcast address, this command is useful only for filtering based on the source address of the broadcast packet.

The helper list, if present, is applied to both all-nets broadcast packets and type 20 propagation packets.

The helper list on the input interface is applied to packets before they are output via either the helper address or type 20 propagation packet mechanism.

Examples

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

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

Related Commands

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

ipx hold-down eigrp

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

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

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

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

Syntax Description

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

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 an Enhanced IGRP route is lost, it is placed into a hold-down state for a period of time. The purpose of the hold-down state is to ensure the validity of any new routes for the same destination.

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

Examples

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

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

ipx hold-time eigrp

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
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 the current value for the hold time is less than two times the interval between hello packets, the hold time will be reset to three times the hello interval.

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

Increasing the hold time delays route convergence across the network.

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

Examples

The following example changes the hold time to 45 seconds:

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

Related Commands

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