Cisco IOS Novell IPX Command Reference

October 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS Novell IPX Command Reference

CONTENTS

Cisco IOS Novell IPX Commands IPX-1

- access-list (IPX extended) IPX-2
- access-list (IPX standard) IPX-7
- access-list (NLSP) IPX-10
- access-list (SAP filtering) IPX-13
- area-address (NLSP) IPX-16
- clear ipx accounting IPX-18
- clear ipx cache IPX-20
- clear ipx nhrp IPX-21
- clear ipx nlsp neighbors IPX-22
- clear ipx route IPX-24
- clear ipx sap IPX-26
- clear ipx traffic IPX-28
- deny (extended) IPX-30
- deny (NLSP) IPX-33
- deny (SAP filtering) IPX-35
- deny (standard) IPX-38
- distribute-list in IPX-40
- distribute-list out IPX-43
- distribute-sap-list in IPX-46
- distribute-sap-list out IPX-49
- ipx access-group IPX-51
- ipx access-list IPX-53
- ipx accounting IPX-56
- ipx accounting-list IPX-59
- ipx accounting-threshold IPX-62
- ipx accounting-transits IPX-64
- ipx advertise-default-route-only (RIP) IPX-66
- ipx advertise-to-lost-route IPX-69
- ipx backup-server-query-interval (EIGRP) IPX-71

ipx bandwidth-percent eigrp **IPX-73**
ipx broadcast-fastswitching **IPX-75**
ipx default-output-rip-delay **IPX-77**
ipx default-output-sap-delay **IPX-79**
ipx default-route **IPX-81**
ipx default-triggered-rip-delay **IPX-83**
ipx default-triggered-rip-holddown **IPX-85**
ipx default-triggered-sap-delay **IPX-87**
ipx default-triggered-sap-holddown **IPX-89**
ipx delay **IPX-91**
ipx down **IPX-94**
ipx eigrp-sap-split-horizon **IPX-96**
ipx encapsulation **IPX-98**
ipx flooding-unthrottled (NLSP) **IPX-101**
ipx gns-reply-disable **IPX-102**
ipx gns-response-delay **IPX-103**
ipx gns-round-robin **IPX-105**
ipx hello-interval eigrp **IPX-107**
ipx helper-address **IPX-109**
ipx helper-list **IPX-111**
ipx hold-down eigrp **IPX-114**
ipx hold-time eigrp **IPX-116**
ipx input-network-filter (RIP) **IPX-119**
ipx input-sap-filter **IPX-121**
ipx internal-network **IPX-124**
ipx ipxwan **IPX-126**
ipx ipxwan error **IPX-129**
ipx ipxwan static **IPX-131**
ipx link-delay **IPX-133**
ipx linkup-request (RIP) **IPX-135**
ipx maximum-hops (RIP) **IPX-137**
ipx maximum-paths **IPX-139**
ipx nasi-server enable **IPX-141**
ipx netbios input-access-filter **IPX-143**
ipx netbios output-access-filter **IPX-146**

ipx netbios-socket-input-checks IPX-149
ipx network IPX-151
ipx nhrp authentication IPX-156
ipx nhrp holdtime IPX-158
ipx nhrp interest IPX-160
ipx nhrp map IPX-162
ipx nhrp max-send IPX-165
ipx nhrp network-id IPX-167
ipx nhrp nhs IPX-169
ipx nhrp record IPX-171
ipx nhrp responder IPX-173
ipx nhrp use IPX-175
ipx nlsp csnp-interval IPX-177
ipx nlsp enable IPX-179
ipx nlsp hello-interval IPX-181
ipx nlsp hello-multiplier IPX-184
ipx nlsp lsp-interval IPX-187
ipx nlsp metric IPX-189
ipx nlsp multicast IPX-191
ipx nlsp priority IPX-193
ipx nlsp retransmit-interval IPX-195
ipx nlsp rip IPX-197
ipx nlsp sap IPX-199
ipx output-ggs-filter IPX-201
ipx output-gns-filter IPX-204
ipx output-network-filter (RIP) IPX-207
ipx output-rip-delay IPX-210
ipx output-sap-delay IPX-212
ipx output-sap-filter IPX-214
ipx pad-process-switched-packets IPX-217
ipx per-host-load-share IPX-219
ipx ping-default IPX-221
ipx potential-pseudonode (NLSP) IPX-223
ipx rip-max-packetsize IPX-225
ipx rip-multiplier IPX-227

ipx rip-queue-maximum IPX-229
ipx rip-response-delay IPX-231
ipx rip-update-queue-maximum IPX-233
ipx route IPX-236
ipx route-cache IPX-240
ipx route-cache inactivity-timeout IPX-243
ipx route-cache max-size IPX-246
ipx route-cache update-timeout IPX-249
ipx router IPX-252
ipx router-filter IPX-254
ipx router-sap-filter IPX-257
ipx routing IPX-260
ipx sap IPX-263
ipx sap follow-route-path IPX-265
ipx sap-helper IPX-268
ipx sap-incremental (EIGRP) IPX-270
ipx sap-incremental split-horizon IPX-272
ipx sap-max-packetsize IPX-274
ipx sap-multiplier IPX-276
ipx sap-queue-maximum IPX-278
ipx sap-update-queue-maximum IPX-281
ipx server-split-horizon-on-server-paths IPX-284
ipx split-horizon eigrp IPX-286
ipx spx-idle-time IPX-288
ipx spx-spoof IPX-291
ipx throughput IPX-293
ipx triggered-rip-delay IPX-295
ipx triggered-rip-holddown IPX-297
ipx triggered-sap-delay IPX-299
ipx triggered-sap-holddown IPX-301
ipx type-20-helpered IPX-303
ipx type-20-input-checks IPX-306
ipx type-20-output-checks IPX-308
ipx type-20-propagation IPX-310
ipx update interval IPX-312

ipx update sap-after-rip IPX-315
ipx watchdog IPX-317
ipx watchdog-spoof IPX-319
log-adjacency-changes (IPX) IPX-320
log-neighbor-changes (EIGRP) IPX-322
log-neighbor-warnings IPX-324
lsp-gen-interval (IPX) IPX-326
lsp-mtu (IPX) IPX-328
lsp-refresh-interval (IPX) IPX-330
max-lsp-lifetime (IPX) IPX-332
multicast IPX-334
nasi authentication IPX-336
netbios access-list (IPX) IPX-339
network (IPX Enhanced IGRP) IPX-342
permit (IPX extended) IPX-344
permit (IPX standard) IPX-347
permit (NLSP) IPX-349
permit (SAP filtering) IPX-351
prc-interval (IPX) IPX-353
redistribute (IPX) IPX-355
route-aggregation (NLSP) IPX-357
show ipx access-list IPX-360
show ipx accounting IPX-362
show ipx cache IPX-365
show ipx eigrp interfaces IPX-367
show ipx eigrp neighbors IPX-370
show ipx eigrp topology IPX-373
show ipx eigrp traffic IPX-378
show ipx interface IPX-380
show ipx nasi connections IPX-385
show ipx nhrp IPX-388
show ipx nhrp traffic IPX-391
show ipx nlsp database IPX-393
show ipx nlsp neighbors IPX-397
show ipx nlsp spf-log IPX-400

show ipx route **IPX-403**
show ipx servers **IPX-407**
show ipx spx-spoof **IPX-410**
show ipx traffic **IPX-413**
show sse summary **IPX-419**
spf-interval **IPX-421**

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 1 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 2 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 2 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 1 lists some IPX protocol names and numbers. Table 2 lists some IPX socket names and numbers. For additional information about IPX protocol numbers and socket numbers, contact Novell.

Table 1 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 2 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 2 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 3 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 3 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 3 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 3 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 4.

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 4 describes the types of encapsulation available for specific interfaces.

Table 4 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.

ipx input-network-filter (RIP)

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **ipx input-network-filter** command controls which networks are added to the routing table based on the networks learned in incoming IPX routing updates (RIP updates) on the interface.

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

Examples

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

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

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

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

Related Commands

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

ipx input-sap-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx internal-network

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

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

ipx internal-network *network-number*

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

Syntax Description

network-number	Number of the internal network.

Defaults

No internal network number is set.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx ipxwan

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

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

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

no ipx ipxwan

Syntax Description

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

Defaults

IPXWAN is disabled.

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keyword and argument were added: • **unnumbered** • *retry-interval*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

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

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

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

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

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

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

Examples

The following example enables IPXWAN on serial interface 0:

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

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

On the local access server (CHICAGO-AS):

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

On the remote router (NYC-AS):

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

Related Commands

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

ipx ipxwan error

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

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

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

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

Syntax Description

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

Defaults

The link is reset.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx ipxwan static

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

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

ipx ipxwan static

no ipx ipxwan static

Syntax Description

This command has no arguments or keywords.

Defaults

Static routing is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables static routing with IPXWAN:

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

```
ipx ipxwan static
```

Related Commands

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

ipx link-delay

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

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

ipx link-delay *microseconds*

no ipx link-delay *microseconds*

Syntax Description

microseconds	Delay, in microseconds.

Defaults

No link delay (delay of 0).

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The link delay you specify replaces the default value or overrides the value measured by IPXWAN when it starts.

Examples

The following example sets the link delay to 20 microseconds:

```
ipx link-delay 20
```

Related Commands

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

ipx linkup-request (RIP)

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

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

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

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

Syntax Description

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

Defaults

General RIP and SAP queries are sent.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx maximum-hops (RIP)

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

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

ipx maximum-hops *hops*

no ipx maximum-hops *hops*

Syntax Description

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

Defaults

16 hops

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
ipx maximum-hops 64
```

ipx maximum-paths

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

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

ipx maximum-paths *paths*

no ipx maximum-paths

Syntax Description

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

Defaults

1 path

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

```
ipx maximum-paths 3
```

Related Commands

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

ipx nasi-server enable

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

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

ipx nasi-server enable

no ipx nasi-server enable

Syntax Description

This command has no arguments or keywords.

Command Default

NASI is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx netbios input-access-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Related Commands

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

ipx netbios output-access-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Related Commands

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

ipx netbios-socket-input-checks

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

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

ipx netbios-socket-input-checks

no ipx netbios-socket-input-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example enables the additional checks on NetBIOS packets:

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

Related Commands

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

ipx network

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

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

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

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

Syntax Description

network	Network number. This is an 8-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
encapsulation *encapsulation-type*	(Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 5.
secondary	(Optional) Indicates an additional (secondary) network configured after the first (primary) network.

Defaults

IPX routing is disabled.

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

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to support the FDDI interface.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

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

no ipx network

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

no ipx network *number*

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

no ipx network *number*

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

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

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

Table 5 describes the types of encapsulation available for specific interfaces.

Table 5 Encapsulation Types

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

Table 5 Encapsulation Types (continued)

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

Examples

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

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

interface ethernet 0.1
 ipx network 2 encapsulation snap

interface ethernet 0.2
 ipx network 3 encapsulation arpa

interface ethernet 0
 ipx network 4 encapsulation sap
```

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

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

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

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

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

The following data compares some maximum sizes of IPX datagrams:

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

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

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

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

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

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

```
ipx routing

interface fddi 0.2 enc sde 2
 ipx network f02 encapsulation snap

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

Related Commands

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

ipx nhrp authentication

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

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

ipx nhrp authentication *string*

no ipx nhrp authentication [*string*]

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ipx nhrp authentication specialxx
```

ipx nhrp holdtime

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

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

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

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

Syntax Description

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

Defaults

7200 seconds (2 hours) for both arguments.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
ipx nhrp holdtime 3600
```

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

```
ipx nhrp holdtime 7200 3600
```

ipx nhrp interest

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

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

ipx nhrp interest *access-list-number*

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

Syntax Description

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

Defaults

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ipx nhrp interest 901
```

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

Related Commands

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

ipx nhrp map

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

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

ipx nhrp map *ipx-address nbma-address*

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

Syntax Description

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

Defaults

No static IPX-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

ipx nhrp max-send

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

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

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

no ipx nhrp max-send

Syntax Description

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

Defaults

pkt-count = 5 packets
interval = 10 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx nhrp network-id

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

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

ipx nhrp network-id *number*

no ipx nhrp network-id

Syntax Description

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

Defaults

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables NHRP on the interface:

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

ipx nhrp nhs

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

ipx nhrp record

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

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

ipx nhrp record

no ipx nhrp record

Syntax Description

This command has no arguments or keywords.

Defaults

Forward record and reverse record options are enabled by default.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example suppresses forward record and reverse record options:

```
no ipx nhrp record
```

Related Commands

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

ipx nhrp responder

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

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

ipx nhrp responder *type number*

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
ipx nhrp responder serial 0
```

ipx nhrp use

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

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

ipx nhrp use *usage-count*

no ipx nhrp use *usage-count*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
ipx nhrp use 5
```

Related Commands

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

ipx nlsp csnp-interval

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

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

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

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

Syntax Description

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

Defaults

30 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx nlsp enable

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

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

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

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

Syntax Description

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

Defaults

NLSP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

The following example enables NLSP routing on Ethernet interface 0:

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

The following example enables NLSP routing on serial interface 0:

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

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

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

Related Commands

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

ipx nlsp hello-interval

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx nlsp hello-multiplier

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

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

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

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

Syntax Description

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

Defaults

The default multiplier is 3.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx nlsp lsp-interval

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

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

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

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

Syntax Description

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

Defaults 55 milliseconds

Command Modes Interface configuration

Command History

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

Usage Guidelines This command allows you to control how fast LSPs can be flooded out an interface.

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

Examples

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

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

Related Commands

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

ipx nlsp metric

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx nlsp multicast

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

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

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

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

Syntax Description

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

Defaults

Multicast addressing is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command allows the router interface to use NLSP multicast addressing. If an adjacent neighbor does not support NLSP multicast addressing, the router will revert to using broadcasts on the affected interface.

The router will also revert to using broadcasts if multicast addressing is not supported by the hardware or driver.

Examples

The following example disables multicast addressing on Ethernet interface 0:

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

ipx nlsp priority

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

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

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

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

Syntax Description

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

Defaults

44

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

ipx nlsp retransmit-interval

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

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

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

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

Syntax Description

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

Defaults

5 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx nlsp rip

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx nlsp sap

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

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx output-ggs-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Related Commands

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

ipx output-gns-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

ipx output-network-filter (RIP)

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **ipx output-network-filter** command controls which networks the Cisco IOS software advertises in its IPX routing updates (RIP updates).

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

Examples

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

```
access-list 896 permit 2b

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

Related Commands

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

ipx output-rip-delay

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

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

ipx output-rip-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx default-output-rip-delay	Sets the default interpacket delay for RIP updates sent on all interfaces
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx output-sap-delay

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

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

ipx output-sap-delay *delay*

no ipx output-sap-delay

Syntax Description

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

Defaults

55 ms

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx output-sap-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Cisco IOS software applies output SAP filters prior to sending SAP packets.

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

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

Examples

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

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

interface ethernet 0
 ipx network 3c

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

interface serial 0
 ipx network 2b
```

Related Commands

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

ipx pad-process-switched-packets

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

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

ipx pad-process-switched-packets

no ipx pad-process-switched-packets

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.

ipx per-host-load-share

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

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

ipx per-host-load-share

no ipx per-host-load-share

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

The following command globally enables per-host load sharing:

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

Related Commands

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

ipx ping-default

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

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

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

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

Syntax Description

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

Defaults

Cisco pings

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
Router# ipx ping-default diagnostic

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

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

Note Verbose mode must be enabled to get diagnostic information.

Related Commands

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

ipx potential-pseudonode (NLSP)

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

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

ipx potential-pseudonode

no ipx potential-pseudonode

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ipx potential-pseudonode
```

ipx rip-max-packetsize

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

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

ipx rip-max-packetsize *bytes*

no ipx rip-max-packetsize *bytes*

Syntax Description

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

Defaults

432 bytes

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The maximum size is for the IPX packet including the IPX network and RIP header information.

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

Examples

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

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

Related Commands

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

ipx rip-multiplier

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

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

ipx rip-multiplier *multiplier*

no ipx rip-multiplier *multiplier*

Syntax Description

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

Defaults

Three times the RIP update interval

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

In the following example, in a configuration where RIP updates are sent once every 2 minutes, the interval at which RIP entries age out is set to 10 minutes:

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

Related Commands

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

ipx rip-queue-maximum

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

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

ipx rip-queue-maximum *milliseconds*

no ipx rip-queue-maximum *milliseconds*

Syntax Description

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

Defaults

No queue limit is set.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx rip-response-delay

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

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

ipx rip-response-delay *ms*

no ipx rip-response-delay

Syntax Description

ms	Delay time, in milliseconds, for RIP responses.

Defaults

No delay in answering (0 ms).

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx rip-update-queue-maximum

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

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

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

no ipx rip-update-queue-maximum *queue-maximum*

Syntax Description

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

Defaults

No queue limit

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Related Commands

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

ipx route

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

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

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

no ipx route

Syntax Description

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

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

Defaults

No static routes are predefined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

The following example defines a static NLSP route summary:

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

Related Commands

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

ipx route-cache

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

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

ipx route-cache

no ipx route-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Fast switching is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

The following example enables fast switching on an interface:

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

The following example disables fast switching on an interface:

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

Related Commands

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

ipx route-cache inactivity-timeout

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

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

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

no ipx route-cache inactivity-timeout

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

This command has no effect if silicon switching is configured.

Examples

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

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

Related Commands

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

ipx route-cache max-size

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

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

ipx route-cache max-size *size*

no ipx route-cache max-size

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx route-cache update-timeout

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

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

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

no ipx route-cache update-timeout

Syntax Description

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

Defaults

The default setting is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx router

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

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

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

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

Syntax Description

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

Defaults

RIP is enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The following keyword and argument were added: • **nlsp** • *tag*
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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

Usage Guidelines

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

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

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

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

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

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

Examples

The following example enables Enhanced IGRP:

```
ipx router eigrp 4
```

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

```
ipx router nlsp area1
```

Related Commands

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

ipx router-filter

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

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

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

no ipx router-filter

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

interface ethernet 0
 ipx router-filter 866
```

Related Commands

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

ipx router-sap-filter

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

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

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

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

Syntax Description

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

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx sap	Specifies static SAP entries.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx routing

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

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

ipx routing [*node*]

no ipx routing

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration

Command Historyi

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

internal-network 1

Usage Guidelines

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

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

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

Examples

The following example enables IPX routing:

```
ipx routing
```

Related Commands

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

ipx sap

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

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration

Command History

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

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
show ipx servers	Lists the IPX servers discovered through SAP advertisements.

ipx sap follow-route-path

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

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

ipx sap follow-route-path

no ipx sap follow-route-path

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx sap-helper

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

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

ipx sap-helper *network.node*

no ipx sap-helper *network.node*

Syntax Description

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

Defaults

No helper address is specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx sap-incremental (EIGRP)

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

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

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

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

Syntax Description

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

Defaults

Enabled on serial interfaces

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

ipx sap-incremental split-horizon

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

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

ipx sap-incremental split-horizon

no ipx sap-incremental split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Note IPX incremental SAP split horizon is off for WAN interfaces and subinterfaces, and on for LAN interfaces. The global default stays off. The interface setting takes precedence if the interface setting is modified or when both the global and interface settings are unmodified. The global setting is used only when global setting is modified and the interface setting is unmodified.

Examples

The following example disables split horizon on serial interface 0:

```
interface serial 0
  no ipx sap-incremental split-horizon
```

Related Commands

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

ipx sap-max-packetsize

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

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

ipx sap-max-packetsize *bytes*

no ipx sap-max-packetsize *bytes*

Syntax Description

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

Defaults

480 bytes

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipx sap-multiplier

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

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

ipx sap-multiplier *multiplier*

no ipx sap-multiplier *multiplier*

Syntax Description

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

Defaults

Three times the SAP update interval.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

```
interface ethernet 0
```

```
ipx sap-multiplier 10
```

Related Commands

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

ipx sap-queue-maximum

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

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

ipx sap-queue-maximum *queue-maximum*

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

Syntax Description

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

Defaults

No queue limit

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ipx sap-update-queue-maximum

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

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

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

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

Syntax Description

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

Defaults

No queue limit

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Related Commands

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

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

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

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

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

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

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

By default, split horizon prevents information about periodic SAPs from being advertised by a router to the same interface in which the best route to that SAP is learned. However, in an instance where the SAP may be learned from interfaces other than, or in addition to, the interface on which the best route to that SAP is learned, using the **ipx server-split-horizon-on-server-paths** command may reduce the number

of unnecessary periodic SAP updates. The reduction in the number of SAP updates occurs because each SAP will not be advertised on the interface or interfaces it was learned from. The reduction in the number of SAP updates will also prevent a potential SAP loop in the network.

Examples

The following example shows the application of split horizon blocks:

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

Related Commands

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

ipx split-horizon eigrp

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

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

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

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

Syntax Description

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

Defaults

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example disables split horizon on serial interface 0:

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

ipx spx-idle-time

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

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

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

no ipx spx-idle-time

Syntax Description

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

Defaults

60 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipx spx-spoof

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

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

The following example enables spoofing on serial interface 0:

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

Related Commands

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

ipx throughput

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

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

ipx throughput *bits-per-second*

no ipx throughput *bits-per-second*

Syntax Description

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

Defaults

Current bandwidth setting for the interface

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ipx throughput 1000000
```

Related Commands

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

ipx triggered-rip-delay

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

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

ipx triggered-rip-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on interface FDDI 0:

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

Related Commands

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

ipx triggered-rip-holddown

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

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

ipx triggered-rip-holddown *milliseconds*

no ipx triggered-rip-holddown *milliseconds*

Syntax Description

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

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

```
interface ether 0
 ipx triggered-rip-holddown 100
```

Related Commands

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

ipx triggered-sap-delay

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

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

ipx triggered-sap-delay *delay*

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

Syntax Description

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

Defaults

55 ms

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

The **ipx triggered-sap-delay** command sets the interpacket delay for triggered updates sent on a single interface. The delay value set by this command overrides the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered updates sent on the interface.

If the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command is high, then we strongly recommend a low delay value for triggered updates so that updates triggered by special events are sent in a more timely manner than periodic updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX servers.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for both periodic and triggered SAP updates.

When you use the **no** form of the **ipx triggered-sap-delay** command, the system uses the global default delay set by the **ipx default-triggered-sap-delay** command for triggered SAP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the "Defaults" section.

This command is also useful on limited bandwidth point-to-point links, or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets an interpacket delay of 55 ms for triggered SAP updates sent on interface FDDI 0:

```
interface FDDI 0
 ipx triggered-sap-delay 55
```

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx triggered-sap-holddown

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx triggered-sap-holddown** command is not supported in Cisco IOS software.

To set the amount of time for which a Service Advertising Protocol (SAP) process will wait before sending flashes about SAP changes, use the **ipx triggered-sap-holddown** command in interface configuration mode. To remove the SAP hold-down, use the **no** form of this command.

ipx triggered-sap-holddown *milliseconds*

no ipx triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

To set a default hold-down used for all interfaces, use the **ipx default-triggered-sap-holddown** command in global configuration mode.

Examples

The following example shows a hold-down time of 100 milliseconds:

```
interface ethernet 0
 ipx triggered-sap-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-rip-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-rip-holddown** command.
ipx-default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.

ipx type-20-helpered

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-helpered** command is not supported in Cisco IOS software.

To forward IPX type 20 propagation packet broadcasts to specific network segments, use the **ipx type-20-helpered** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx type-20-helpered

no ipx type-20-helpered

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **ipx type-20-helpered** command disables the input and output of type 20 propagation packets as done by the **ipx type-20-propagation** interface configuration command.

The **ipx type-20-propagation** command broadcasts type 20 packets to all nodes on the network and imposes a hop-count limit of eight routers for broadcasting these packets. These functions are in compliance with the Novell IPX router specification. In contrast, the **ipx type-20-helpered** command broadcasts type 20 packets to only those nodes indicated by the **ipx helper-address** interface configuration command and extends the hop-count limit to 16 routers.

Use of the **ipx type-20-helpered** command does not comply with the Novell IPX router specification; however, you may need to use this command if you have a mixed internetwork that contains routers running Software Release 9.1 and routers running later versions of Cisco IOS software.

Examples

The following example forwards IPX type 20 propagation packet broadcasts to specific network segments:

```
interface ethernet 0
 ipx network aa
 ipx type-20-helpered
 ipx helper-address bb.ffff.ffff.ffff
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-input-checks

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-input-checks** command is not supported in Cisco IOS software.

To restrict the acceptance of IPX type 20 propagation packet broadcasts, use the **ipx type-20-input-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-input-checks

no ipx type-20-input-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

By default, Cisco IOS software is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-input-checks** command to impose additional restrictions on the acceptance of type 20 packets. Specifically, the software will accept type 20 propagation packets only on the single network that is the primary route back to the source network. Similar packets received via other networks will be dropped. This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Examples

The following example imposes additional restrictions on incoming type 20 broadcasts:

```
ipx type-20-input-checks
```

Related Commands

Command	Description
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-output-checks

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **ipx type-20-output-checks** command is not supported in Cisco IOS software.

To restrict the forwarding of IPX type 20 propagation packet broadcasts, use the **ipx type-20-output-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-output-checks

no ipx type-20-output-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

By default, Cisco IOS software is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-output-checks** command to impose additional restrictions on outgoing type 20 packets. Specifically, the software will forward these packets only to networks that are not routes back to the source network. (The software uses the current routing table to determine routes.) This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Examples

The following example imposes restrictions on outgoing type 20 broadcasts:

```
ipx type-20-output-checks
```

Related Commands

Command	Description
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-propagation

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx type-20-propagation** command is not supported in Cisco IOS software.

To forward IPX type 20 propagation packet broadcasts to other network segments, use the **ipx type-20-propagation** command in interface configuration mode. To disable both the reception and forwarding of type 20 broadcasts on an interface, use the **no** form of this command.

ipx type-20-propagation

no ipx type-20-propagation

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Routers normally block all broadcast requests. To allow input and output of type 20 propagation packets on an interface, use the **ipx type-20-propagation** command. Note that type 20 packets are subject to loop detection and control as specified in the IPX router specification.

Additional input and output checks may be imposed by the **ipx type-20-input-checks** and **ipx type-20-output-checks** commands.

IPX type 20 propagation packet broadcasts are subject to any filtering defined by the **ipx helper-list** command.

Examples

The following example enables both the reception and forwarding of type 20 broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ipx type-20-propagation
```

The following example enables the reception and forwarding of type 20 broadcasts between networks 123 and 456, but does not enable reception and forwarding of these broadcasts to and from network 789:

```
interface ethernet 0
 ipx network 123
 ipx type-20-propagation
!
interface ethernet 1
 ipx network 456
 ipx type-20-propagation
!
interface ethernet 2
 ipx network 789
```

Related Commands

Command	Description
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.

ipx update interval

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx update interval** command is not supported in Cisco IOS software.

To adjust the Routing Information Protocol (RIP) or Service Advertising Protocol (SAP) update interval, use the **ipx update interval** command in interface configuration mode. To restore the default values, use the **no** form of this command.

ipx update interval {**rip** | **sap**} {*value* | **changes-only**}

no ipx update interval {**rip** | **sap**}

Syntax Description

rip	Adjusts the interval at which RIP updates are sent. The minimum interval is 10 seconds.
sap	Adjusts the interval at which SAP updates are sent. The minimum interval is 10 seconds.
value	The interval specified in seconds.
changes-only	Specifies the sending of a SAP or RIP update when the link comes up, when the link is downed administratively, or when service information changes. This parameter is supported for both SAP and RIP updates.

Defaults

The default interval is 60 seconds for both IPX routing updates and SAP updates.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

This command replaces two commands found in previous releases of Cisco IOS software: **ipx sap-interval** and **ipx update-time**.

Routers exchange information about routes by sending broadcast messages when they are started up and shut down, and periodically while they are running. The **ipx update interval** command enables you to modify the periodic update interval. By default, this interval is 60 seconds (this default is defined by Novell).

You should set RIP timers only in a configuration in which all routers are Cisco routers or in which all other IPX routers allow configurable timers. The timers should be the same for all devices connected to the same cable segment.

The update value you choose affects the internal IPX timers as follows:

- IPX routes are marked invalid if no routing updates are heard within three times the value of the update interval and are advertised with a metric of infinity.
- IPX routes are removed from the routing table if no routing updates are heard within four times the value of the update interval.

Setting the interval at which SAP updates are sent is most useful on limited-bandwidth links, such as slower-speed serial interfaces.

You should ensure that all IPX servers and routers on a given network have the same SAP interval. Otherwise, they may decide that a server is down when it is really up.

It is not possible to change the interval at which SAP updates are sent on most PC-based servers. This means that you should never change the interval for an Ethernet or Token Ring network that has servers on it.

You can set the router to send an update only when changes have occurred. Using the **changes-only** keyword specifies the sending of a SAP update only when the link comes up, when the link is downed administratively, or when the databases change. The **changes-only** keyword causes the router to do the following:

- Send a single, full broadcast update when the link comes up.
- Send appropriate triggered updates when the link is shut down.
- Send appropriate triggered updates when specific service information changes.

Examples

The following example configures the update timers for RIP updates on two interfaces in a router:

```
interface serial 0
 ipx update interval rip 40

interface ethernet 0
 ipx update interval rip 20
```

The following example configures SAP updates to be sent (and expected) on serial interface 0 every 300 seconds (5 minutes) to reduce periodic update overhead on a slow-speed link:

```
interface serial 0
 ipx update interval sap 300
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx update sap-after-rip

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx update sap-after-rip** command is not supported in Cisco IOS software.

To configure the router to send a Service Advertising Protocol (SAP) update immediately following a Routing Information Protocol (RIP) broadcast, use the **ipx update sap-after-rip** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx update sap-after-rip

no ipx update sap-after-rip

Syntax Description

This command has no arguments or keywords.

Defaults

RIP and SAP updates are sent every 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **ipx update sap-after-rip** command causes the router to issue a SAP update immediately following a RIP broadcast. This ensures that the SAP update follows the RIP broadcast, and that the SAP update is sent using the RIP update interval. It also ensures that the receiving router has learned the route to the service interface via RIP prior to getting the SAP broadcast.

Examples

The following example configures the router to issue a SAP broadcast immediately following a RIP broadcast on serial interface 0.

```
interface serial 0
```

```
ipx update sap-after-rip
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx update interval	Adjusts the RIP or SAP update interval.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx watchdog

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **ipx watchdog** command is not supported in Cisco IOS software.

To enable watchdog, use the **ipx watchdog** command in interface configuration mode. To specify filtering, spoofing, or how long spoofing is to be enabled or disabled, use arguments and keywords. To disable filtering or spoofing, use the **no** form of this command.

ipx watchdog {**filter** | **spoof** [*enable-time-hours disable-time-minutes*]}

no ipx watchdog {**filter** | **spoof**}

Syntax Description

filter	Discards IPX server watchdog packets when a DDR link is not connected.
spoof	Answers IPX server watchdog packets when a DDR link is not connected.
enable-time-hours	(Optional) Number of consecutive hours spoofing is to stay enabled. Values are 1 through 24.
disable-time-minutes	(Optional) Number of consecutive minutes spoofing is to stay disabled. Values are 18 through 1440.

Defaults

There is no watchdog processing.

Command Modes

Interface configuration

Command History

Release	Modification
11.2(9.1)	This command was introduced. This command replaces the **ipx watchdog-spoof** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **ipx watchdog** command when you want to enable watchdog processing. Use this command only on a serial interface with dial-on-demand (DDR) routing enabled.

Using the **filter** keyword when the DDR link is not connected will cause IPX server watchdog packets to be discarded, preventing them from bringing the DDR link up again.

Using the **spoof** keyword will allow IPX server watchdog packets to be answered when the DDR link is not connected. You can control how long spoofing is to be enabled or disabled by using the *enable-time-hours* and *disable-time-minutes* arguments.

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.

ipx watchdog-spoof

The **ipx watchdog-spoof** command is replaced by the **ipx watchdog** command. See the description of the **ipx watchdog** command in this chapter for more information.

log-adjacency-changes (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-adjaceny-changes (IPX)** command is not supported in Cisco IOS software.

To generate a log message when an NetWare Link-Services Protocol (NLSP) adjacency changes state (up or down), use the **log-adjacency-changes** command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

Defaults

Adjacency changes are not logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

This command allows the monitoring of NLSP adjacency state changes. Adjacency state monitoring can be very useful when monitoring large networks. Messages are logged using the system error message facility. Messages are of the form:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

Messages regarding the use of NLSP multicast and broadcast addressing are also logged. For example, if broadcast addressing is in use on Ethernet interface 1.2, and the last neighbor requiring broadcasts goes down, the following messages will be logged:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Down, hold time
expired
%CLNS-5-MULTICAST: NLSP: Multicast address in use on Ethernet1.2
```

If multicast addressing is in use and a new neighbor that supports only broadcast addressing comes up, the following messages will be logged:

```
%CLNS-5-ADJCHANGE: NLSP: Adjacency to 0000.0C34.D838 (Ethernet1.2) Up, new adjacency
%CLNS-5-MULTICAST: NLSP Broadcast address is in use on Ethernet1.2
```

Examples

The following example instructs the router to log adjacency changes for the NLSP process area1:

```
ipx router nlsp area1
 log-adjacency-changes
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

log-neighbor-changes (EIGRP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-neighbor-changes (EIGRP)** command is not supported in Cisco IOS software.

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **log-neighbor-changes** command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

No adjacency changes are logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Enable the logging of neighbor adjacency changes in order to monitor the stability of the routing system and to help detect problems. Log messages are of the following form:

`%DUAL-5-NBRCHANGE: IPX EIGRP` *as-number* `: Neighbor` *address* `(`*interface*`) is` *state*`:` *reason*

where the arguments have the following meanings:

as-number	Autonomous system number
address (interface)	Neighbor address
state	Up or down
reason	Reason for change

Examples The following configuration will log neighbor changes for EIGRP process 209:

```
ipx router eigrp 209
 log-neighbor-changes
```

log-neighbor-warnings

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **log-neighbor-warnings** command is not supported in Cisco IOS software.

Note Effective with Cisco IOS Release 15.0(1)M, 12.2(33)SRE and Cisco IOS XE Release 2.5, the **log-neighbor-warnings** command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **log-neighbor-warnings** command in router configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

log-neighbor-warnings [*seconds*]

no log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 through 65535.

Command Default Neighbor warning messages are logged.

Command Modes Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
12.2(33)SRE	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.
Cisco IOS XE Release 2.5	This command was replaced by the **eigrp log-neighbor-warnings** command for IPv4 and IPv6 configurations. The **log-neighbor-warnings** command is still available for IPX configurations.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With the **log-neighbor-warnings** command, you can disable and enable the logging of neighbor warning messages and configure the interval between repeated neighbor warning messages.

Examples

The following example shows that neighbor warning messages will be logged for EIGRP process 1 and warning messages will be repeated in 5-minute (300 seconds) intervals:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# log-neighbor-warnings 300
```

Related Commands

Command	Description
log-neighbor-changes	Enables the logging of changes in EIGRP neighbor adjacencies.

lsp-gen-interval (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-gen-interval (IPX)** command is not supported in Cisco IOS software.

To set the minimum interval at which link-state packets (LSPs) are generated, use the **lsp-gen-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

lsp-gen-interval *seconds*

no lsp-gen-interval *seconds*

Syntax Description

seconds	Minimum interval, in seconds. It can be a number in the range 0 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **lsp-gen-interval** command controls the rate at which LSPs are generated on a per-LSP basis. For instance, if a link is changing state at a high rate, the default value of the LSP generation interval limits the signaling of this change to once every 5 seconds. Because the generation of an LSP may cause all routers in the area to perform the SPF calculation, controlling this interval may have area-wide impact. Raising this interval can reduce the load on the network imposed by a rapidly changing link.

Examples

The following example sets the minimum interval at which LSPs are generated to 10 seconds:

```
lsp-gen-interval 10
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

lsp-mtu (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-mtu (IPX)** command is not supported in Cisco IOS software.

To set the maximum size of a link-state packet (LSP) generated by Cisco IOS software, use the **lsp-mtu** command in router configuration mode. To restore the default Maximum Transmission Unit (MTU) size, use the **no** form of this command.

lsp-mtu *bytes*

no lsp-mtu *bytes*

Syntax Description

bytes	MTU size, in bytes. It can be a number in the range 512 to 4096. The default is 512 bytes.

Defaults

512 bytes

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

You can increase the LSP MTU if there is a very large amount of information generated by a single router, because each device is limited to approximately 250 LSPs. In practice, this should never be necessary.

The LSP MTU must never be larger than the smallest MTU of any link in the area. This is because LSPs are flooded throughout the area.

The **lsp-mtu** command limits the size of LSPs generated by this router only; Cisco IOS software can receive LSPs of any size up to the maximum.

Examples

The following example sets the maximum LSP size to 1500 bytes:

```
lsp-mtu 1500
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

lsp-refresh-interval (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **lsp-refresh-interval (IPX)** command is not supported in Cisco IOS software.

To set the link-state packet (LSP) refresh interval, use the **lsp-refresh-interval** command in router configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds*

no lsp-refresh-interval *seconds*

Syntax Description

seconds	Refresh interval, in seconds. It can be a value in the range 1 to 50,000 seconds. The default is 7200 seconds (2 hours).

Defaults

7200 seconds (2 hours)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The refresh interval determines the rate at which Cisco IOS software periodically transmits the route topology information that it originates. This is done in order to keep the information from becoming too old. By default, the refresh interval is 2 hours.

LSPs must be periodically refreshed before their lifetimes expire. The refresh interval must be less than the LSP lifetime specified with the **max-lsp-lifetime (IPX)** router configuration command. Reducing the refresh interval reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. (This is an extremely unlikely event, however, because there are other safeguards against corruption.) Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Examples

The following example changes the LSP refresh interval to 10,800 seconds (3 hours):

```
lsp-refresh-interval 10800
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
max-lsp-lifetime (IPX)	Sets the maximum time that LSPs persist without being refreshed.

max-lsp-lifetime (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **max-lsp-lifetime (IPX)** command is not supported in Cisco IOS software.

To set the maximum time for which link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default time, use the **no** form of this command.

max-lsp-lifetime [**hours**] *value*

no max-lsp-lifetime

Syntax Description

hours	(Optional) If specified, the lifetime of the LSP is set in hours. If not specified, the lifetime is set in seconds.
value	Lifetime of LSP, in hours or seconds. It can be a number in the range 1 to 32,767. The default is 7500 seconds.

Defaults

7500 seconds (2 hours, 5 minutes)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **hours** keyword enables the router to interpret the maximum lifetime field in hours, allowing the router to keep LSPs for a much longer time. Keeping LSPs longer reduces overhead on slower-speed serial links and keeps ISDN links from becoming active unnecessarily.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval (IPX)** router configuration command. The maximum LSP lifetime must be greater than the LSP refresh interval.

Examples

The following example sets the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

```
max-lsp-lifetime 11000
```

The following example sets the maximum time that the LSP persists to 15 hours:

```
max-lsp-lifetime hours 15
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
lsp-refresh-interval (IPX)	Sets the LSP refresh interval.

multicast

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **multicast** command is not supported in Cisco IOS software.

To configure the router to use multicast addressing, use the **multicast** command in router configuration mode. To configure the router to use broadcast addressing, use the **no** form of this command.

multicast

no multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast addressing is enabled.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

This command allows the router to use NetWare Link-Services Protocol (NLSP) multicast addressing. If an adjacent neighbor does not support NLSP multicast addressing, the router will revert to using broadcasts on the affected interface.

The router will also revert to using broadcasts on any interface where multicast addressing is not supported by the hardware or driver.

Examples

The following example disables multicast addressing on the router:

```
ipx router nlsp
 no multicast
```

nasi authentication

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **nasi authentication** command is not supported in Cisco IOS software.

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

nasi authentication {**default** | *list-name*}

no nasi authentication {**default** | *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication nasi** command.
list-name	Uses the list created with the **aaa authentication nasi** command.

Defaults

Uses the default set with the **aaa authentication nasi** command.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi** command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1* be used on line 7:

```
line 7
 nasi authentication list1
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

netbios access-list (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **netbios access-list (IPX)** command is not supported in Cisco IOS software.

To define an IPX NetBIOS FindName access list filter, use the **netbios access-list** command in global configuration mode. To remove a filter, use the **no** form of this command.

netbios access-list host *name* {**deny** | **permit**} *string*

no netbios access-list host *name* {**deny** | **permit**} *string*

netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

no netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
name	Name of the access list being defined. The name can be an alphanumeric string.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
string	Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument *string* can include the following wildcard characters: • *—Matches one or more characters. You can use this wildcard character only at the end of a string. • ?—Matches any single character.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
offset	Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.
byte-pattern	Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument *byte-pattern* can include the double asterisk (**) wildcard character to match any digits for that byte.

Defaults No filters are predefined.

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Keep the following points in mind when configuring IPX NetBIOS access control:

- Host (node) names are case-sensitive.
- Host and byte access lists can have the same names. They are independent of each other.
- When filtering by node name for IPX NetBIOS, the names in the access lists are compared with the destination name field for IPX NetBIOS “find name” requests.
- When filtering by byte offset, note that these access filters can have a significant impact on the packets’ transmission rate across the bridge because each packet must be examined. You should use these access lists only when absolutely necessary.
- If a node name is not found in an access list, the default action is to deny access.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

To delete an IPX NetBIOS access list, specify the minimum number of keywords and arguments needed to delete the proper list. For example, to delete the entire list, use the following command:

no netbios access-list {**host** | **bytes**} *name*

To delete a single entry from the list, use the following command:

no netbios access-list host *name* {**permit** | **deny**} *string*

Examples

The following example defines the IPX NetBIOS access list engineering:

```
netbios access-list host engineering permit eng-ws1 eng-ws2 eng-ws3
```

The following example removes a single entry from the engineering access list:

```
netbios access-list host engineering deny eng-ws3
```

The following example removes the entire engineering NetBIOS access list:

```
no netbios access-list host engineering
```

Related Commands

Command	Description
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
ipx netbios output-access-filter	Controls outgoing NetBIOS FindName messages.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

network (IPX Enhanced IGRP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **network (IPX Enhanced IGRP)** command is not supported in Cisco IOS software.

To enable Enhanced Interior Gateway Routing Protocol (EIGRP), use the **network** (IPX Enhanced IGRP) command in router configuration mode. To disable Enhanced IGRP, use the **no** form of this command.

network {*network-number* | **all**}

no network {*network-number* | **all**}

Syntax Description

network-number	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **network** (IPX Enhanced IGRP) command to enable the routing protocol specified in the **ipx router** command on each network.

Examples

The following commands disable RIP on network 10 and enable Enhanced IGRP on networks 10 and 20:

```
ipx router rip
 no network 10
```

```
ipx router eigrp 12
 network 10
 network 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

permit (IPX extended)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (IPX extended)** command is not supported in Cisco IOS software.

To set conditions for a named IPX extended access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the keyword **any** to match all protocol types.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.*source-node*	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.
source-socket	Socket name or number (hexadecimal) from which the packet is being sent. You can also use the word **all** to match all sockets.

destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

There is no specific condition under which a packet passes the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX protocol names and numbers, and IPX socket names and numbers, see the **access-list** (IPX extended) command.

Examples

The following example creates an extended access list named *sal* that denies all SPX packets and permits all others:

```
ipx access-list extended sal
 deny spx any all any all log
 permit any
```

The following example provides a time range to permit access:

```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (IPX standard)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (IPX standard)** command is not supported in Cisco IOS software.

To set conditions for a named IPX access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

no permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

Syntax Description

source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*source-node*	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*destination-node*	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are defined.

Command Modes Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples The following example creates a standard access list named *fred*. It permits communication with only IPX network number 5678.

```
ipx access-list standard fred
 permit 5678 any
 deny any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (NLSP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (NLSP)** command is not supported in Cisco IOS software.

To allow explicit route redistribution in a named NetWare Link-Services Protocol (NLSP) route aggregation access list, use the **permit** command in access-list configuration mode. To remove a permit condition, use the **no** form of this command.

permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

no permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description

network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary, expressed as an eight-digit hexadecimal number. The high-order bits specified for the *network-mask* argument must be contiguous 1s, while the low-order bits must be contiguous zeros (0). An arbitrary mix of 1s and 0s is not permitted.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which networks that are permitted by the access list entry can be redistributed as explicit networks, without summarization.

For additional information on creating access lists that deny or permit area addresses that summarize routes, see the **access-list** (NLSP route aggregation summarization) command.

Examples

The following example allows networks 12345600 and 12345601 to be redistributed explicitly. Other routes in the range 12345600 to 123456FF are summarized into a single aggregated route. All other routes will be redistributed as explicit routes.

```
ipx access-list summary finance
 permit 12345600
 permit 12345601
 deny 12345600 ffffff00
 permit -1
```

Related Commands

Command	Description
access-list (NLSP)	Defines an access list that denies or permits area addresses that summarize routes.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (SAP filtering)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **permit (SAP filtering)** command is not supported in Cisco IOS software.

To set conditions for a named IPX Service Advertising Protocol (SAP) filtering access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *network*[*.node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no permit *network*[*.node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	(Optional) Node on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.node-mask	(Optional) Mask to be applied to the *network* and *node* arguments. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX SAP service types, see the **access-list** (SAP filtering) command.

Examples

The following example creates a SAP access list named MyServer that allows only MyServer to be sent in SAP advertisements:

```
ipx access-list sap MyServer
 permit 1234 4 MyServer
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

prc-interval (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **prc-interval (IPX)** command is not supported in Cisco IOS software.

To control the hold-down period between partial route calculations, use the **prc-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds*

no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between partial route calculations, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **prc-interval** command controls how often Cisco IOS software can performs a partial route (PRC) calculation. The PRC calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially on slower router models. Increasing the PRC interval reduces the processor load of the router, but potentially slows down the rate of convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first calculations.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
prc-interval 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

redistribute (IPX)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **redistribute (IPX)** command is not supported in Cisco IOS software.

To redistribute from one routing domain into another, and vice versa, use one of the following **redistribute** commands in router configuration mode. To disable this feature, use the **no** form of these commands.

For Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

no redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

Syntax Description

connected	Specifies connected routes.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.
rip	Specifies the RIP protocol. You can configure only one RIP process on the router. Thus, you cannot redistribute RIP into RIP.
static	Specifies static routes.
access-list *name*	(Optional) Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

Redistribution is enabled between all routing domains except between separate Enhanced IGRP processes.

Redistribution of floating static routes is disabled.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	The **access-list** keyword and *access-list-number* argument have been removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Redistribution provides for routing information generated by one protocol to be advertised in another.

The only connected routes affected by this redistribute command are the routes not specified by the **network** command.

If you have enabled floating static routes by specifying the **floating** keyword in the **ipx route** global configuration command and you redistribute floating static routes into a dynamic IPX routing protocol, any nonhierarchical topology causes the floating static destination to be redistributed immediately via a dynamic protocol back to the originating router, causing a routing loop. This occurs because dynamic protocol information overrides floating static routes. For this reason, automatic redistribution of floating static routes is off by default. If you redistribute floating static routes, you should specify filters to eliminate routing loops.

- Enhanced IGRP version 1.1 environments
- RIP version 1.1 environments

Examples

The following example does not redistributes RIP routing information:

```
ipx router eigrp 222
 no redistribute rip
```

The following example redistributes Enhanced IGRP routes from autonomous system 100 into Enhanced IGRP autonomous system 300:

```
ipx router eigrp 300
 redistribute eigrp 100
```

Related Commands

Command	Description
ipx access-list	Defines an IPX access list by name.
ipx router	Specifies the routing protocol to use.

route-aggregation (NLSP)

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **route-aggregation (NLSP)** command is not supported in Cisco IOS software.

To enable the generation of aggregated routes in an NetWare Link-Services Protocol (NLSP) area, use the **route-aggregation** command in router configuration mode. To disable generation, use the **no** form of this command.

route-aggregation

no route-aggregation

Syntax Description

This command has no arguments or keywords.

Defaults

Route summarization is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When route summarization is disabled, all routes redistributed into an NLSP area will be explicit routes.

When route summarization is enabled, the router uses the access list associated with the **redistribute** command (if one exists) for the routing process associated with each route as a template for route summarization. Explicit routes that match a range denied by the access list trigger generation of an aggregated route instead. Routes permitted by the access list are redistributed as explicit routes.

If no access list exists, the router instead uses the area address (if one exists) of the routing process associated with each route as a template for route summarization. Explicit routes that match the area address trigger generation of an aggregated route instead.

Note Because an Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) routing process cannot have an area address, it is not possible to generate aggregated routes without the use of an access list.

Examples

The following example enables route summarization between two NLSP areas. Route summarization is based on the area addresses configured for each area.

```
ipx routing
ipx internal-network 123
!
interface ethernet 1
 ipx nlsp area1 enable
!
interface ethernet 2
 ipx nlsp area2 enable
!
ipx router nlsp area1
 area-address 1000 fffff000
 route-aggregation
!
ipx router nlsp area2
 area-address 2000 fffff000
 route-aggregation
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
redistribute (IPX)	Redistributes from one routing domain into another.

show ipx access-list

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx access-list** command is not supported in Cisco IOS software.

To display the contents of all current IPX access lists, use the **show ipx access-list** command in EXEC mode.

show ipx access-list [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the IPX access list to display. This is a number from 800 to 899, 900 to 999, 1000 to 1099, or 1200 to 1299.
name	(Optional) Name of the IPX access list to display.

Defaults

Displays all standard, extended, and Service Advertising Protocol (SAP) IPX access lists.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

The **show ipx access-list** command provides output identical to the **show access-lists** command, except that it is IPX specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ipx access-list** command when all access lists are requested:

```
Router# show ipx access-list

IPX extended access list 900
 deny any 1
```

```
IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

The following is sample output from the **show ipx access-list** command when the name of a specific access list is requested:

```
Router# show ipx access-list London

IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

show ipx accounting

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx accounting** command is not supported in Cisco IOS software.

To display the active or checkpoint accounting database, use the **show ipx accounting** command in EXEC mode.

show ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Displays entries in the checkpoint database.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx accounting** command:

```
Router# show ipx accounting

Source                  Destination               Packets           Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72            2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14             624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62            3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20            1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20            1470

Accounting data age is     6
```

Table 6 describes the fields shown in the display.

Table 6 show ipx accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets transmitted from the source address to the destination address.
Bytes	Number of bytes transmitted from the source address to the destination address.
Accounting data age is ...	Time since the accounting database has been cleared. It can be in one of the following formats: *mm*, *hh*:*mm*, *dd*:*hh*, and *ww*:*dd*, where *m* is minutes, *h* is hours, *d* is days, and *w* is weeks.

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.

show ipx cache

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx cache** command is not supported in Cisco IOS software.

To display the contents of the IPX fast-switching cache, use the **show ipx cache** command in EXEC mode.

show ipx cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx cache** command:

```
Router# show ipx cache

Novell routing cache version is 9
Destination          Interface              MAC Header
*1006A               Ethernet 0             00000C0062E600000C003EB0064
*14BB                Ethernet 1             00000C003E2A00000C003EB0064
```

Table 7 describes the fields shown in the display.

Table 7 show ipx cache Field Descriptions

Field	Description
Novell routing cache version is ...	Number identifying the version of the fast-switching cache table. It increments each time the table changes.
Destination	Destination network for this packet. Valid entries are marked by an asterisk (*).
Interface	Route interface through which this packet is transmitted.
MAC Header	Contents of this packet's MAC header.

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
ipx route-cache	Enables IPX fast switching.

show ipx eigrp interfaces

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp interfaces** command is not supported in Cisco IOS software.

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp interfaces** command in EXEC mode.

show ipx eigrp interfaces [*type number*] [*as-number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
as-number	(Optional) Autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **show ipx eigrp interfaces** command to determine on which interfaces Enhanced IGRP is active and to find out information about Enhanced IGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which Enhanced IGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all Enhanced IGRP processes are displayed.

Examples

The following is sample output from the **show ipx eigrp interfaces** command:

```
Router> show ipx eigrp interfaces

IPX EIGRP interfaces for process 109
```

```
                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

Table 8 describes the fields shown in the display.

Table 8 show ipx eigrp interfaces Field Descriptions

Field	Description
process 109	Autonomous system number of the process.
Interface	Interface name.
Peers	Number of neighbors on the interface.
Xmit Queue	Count of unreliable and reliable packets queued for transmission.
Mean SRTT	Average round-trip time for all neighbors on the interface.
Pacing Time	Number of milliseconds to wait after transmitting unreliable and reliable packets.
Multicast Flow Timer	Number of milliseconds to wait for acknowledgment of a multicast packet by all neighbors before transmitting the next multicast packet.
Pending Routes	Number of routes still to be transmitted on this interface.

Related Commands

Command	Description
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

show ipx eigrp neighbors

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp neighbors** command is not supported in Cisco IOS software.

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipx eigrp neighbors [**servers**] [**detail** | *interface interface-number*] [**regexp** *name*]

Syntax Description

servers	(Optional) Displays the server list advertised by each neighbor. This list is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
detail	(Optional) Displays detailed peer information.
interface	(Optional) Specifies the type of interface.
interface-number	(Optional) Specifies the interface number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The following keyword and argument were added: • **regexp** • *name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **regexp** and **servers** keywords were removed. The *name* argument was removed.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use **show ipx eigrp neighbors** command to display the neighbors discovered by EIGRP.

Examples

The following are sample outputs of **show ipx eigrp neighbors** commands:

```
Router# show ipx eigrp neighbors

EIGRP-IPX Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.aabb.cc00.0e00       Et0/0             12 00:01:17  166   996  0  4
0   10.aabb.cc00.0a00       Et0/0             12 00:01:19  173  1038  0  9

Router# show ipx eigrp neighbors detail

EIGRP-IPX Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.aabb.cc00.0e00       Et0/0             14 00:01:20  166   996  0  4
   Version 5.0/3.0, Retrans: 0, Retries: 0, Prefixes: 1
   Topology-ids from peer - 0
0   10.aabb.cc00.0a00       Et0/0             14 00:01:22  173  1038  0  9
   Version 5.0/3.0, Retrans: 0, Retries: 0, Prefixes: 1
   Topology-ids from peer - 0
```

Table 9 describes the fields shown in the display.

Table 9 show ipx eigrp neighbors Field Descriptions

Field	Description
AS()	Autonomous system number specified in the **ipx router** configuration command.
H	Handle. An arbitrary and unique number inside this router that identifies the neighbor.
Address	IPX address of the Enhanced IGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time, in seconds, that Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.
Uptime	Elapsed time (in hours, minutes, and seconds) since the local router first heard from this neighbor.

Table 9 show ipx eigrp neighbors Field Descriptions (continued)

Field	Description
Q Cnt	Number of IPX Enhanced IGRP packets (Update, Query, and Reply) that Cisco IOS software is waiting to send.
Seq Num	Sequence number of the last Update, Query, or Reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds it takes for an IPX Enhanced IGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. This is the amount of time Cisco IOS software waits before retransmitting a packet from the retransmission queue to a neighbor.
Type	Contains codes from the Codes field to indicates how service was learned.

Related Commands

Command	Description
ipx sap-incremental	Sends SAP updates only when a change occurs in the SAP table.

show ipx eigrp topology

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp topology** command is not supported in Cisco IOS software.

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show ipx eigrp topology** command in user EXEC mode or privileged EXEC mode.

show ipx eigrp topology [*network-number* [*ipx-network-mask*] | **active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors | base** [*network-number* [*ipx-network-mask*] | **active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors | accounting** | **events** [[**errmsg** | **sia**] [*start-event-number end-event-number*] | **type**]]]

Syntax Description

network-number	(Optional) Specifies the IPX network number whose topology table entry is displayed. Specifies the base IPX network number of the topology table when used with the **base** keyword.
ipx-network-mask	(Optional) Specifies the IPX network mask. Specifies the base IPX network mask when used with the **base** keyword.
active	(Optional) Displays only the active topology entries. Displays active base topology entries when used with the **base** keyword.
all-links	(Optional) Displays summary information of all entries in the EIGRP topology table. Displays the base summary information of all entries in the EIGRP topology table when used with the **base** keyword.
detail-links	(Optional) Displays detailed information about all entries in the EIGRP topology table. Displays detailed base information about all entries in the EIGRP topology table when used with the **base** keyword.
pending	(Optional) Displays all entries in the EIGRP topology table that are eiher waiting for an update from a neighbor or waiting to reply to a neighbor. Displays the base events pending for transmission when used with the **base** keyword.
summary	(Optional) Displays a summary of the EIGRP topology table. Displays the base summary of the EIGRP topology table when used with the **base** keyword.
zero-successors	(Optional) Displays available routes in the EIGRP topology table. Displays the available base routes in the EIGRP topology table when used with the **base** keyword.
base	(Optional) Specifies the base topology.
accounting	(Optional) Specifies the accounting prefix of the base topology.
events	(Optional) Specifies the base topology logged events.
start-event-number	(Optional) Specifies the starting event number.

errmsg	(Optional) Displays the logged error messages.
end-event-number	Specifies the ending event number.
sia	(Optional) Displays the stuck in active (sia) logged events.
type	(Optional) Displays the type of the logged events.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE. This command was modified. The **accounting**, **base**, **errmsg**, **events, sia**, and **type** keywords were removed. The *start-event-number* and *end-event-number* arguments were removed.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output of **show ipx eigrp topology** command:

```
Router# show ipx eigrp topology

IPX EIGRP Topology Table for process 109
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 42, 1 successors, FD is 0
   via 160.0000.0c00.8ea9 (345088/319488), Ethernet0
P 160, 1 successor via Connected, Ethernet
   via 160.0000.0c00.8ea9 (307200/281600), Ethernet0
P 165, 1 successors, FD is 307200
   via Redistributed (287744/0)
   via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
P 164, 1 successors, flags: U, FD is 200
   via 160.0000.0c00.8ea9 (307200/281600), Ethernet1
   via 160.0000.0c01.2b71 (332800/307200), Ethernet1
P A112, 1 successors, FD is 0
   via Connected, Ethernet2
   via 160.0000.0c00.8ea9 (332800/307200), Ethernet0
P AAABBB, 1 successors, FD is 10003
   via Redistributed (287744/0),
   via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
A A112, 0 successors, 1 replies, state: 0, FD is 0
   via 160.0000.0c01.2b71 (307200/281600), Ethernet1
   via 160.0000.0c00.8ea9 (332800/307200), r, Ethernet1
```

Table 10 describes the fields shown in the display.

Table 10 show ipx eigrp topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the Enhanced IGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No Enhanced IGRP computations are being performed for this destination.
A – Active	Enhanced IGRP computations are being performed for this destination.
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set after Cisco IOS software has sent a query and is waiting for a reply.
42, 160, and so on	Destination IPX network number.
successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
FD	Feasible distance. This value is used in the feasibility condition check. If the neighbor's reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the router determines it has a feasible successor, it does not have to send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
via	IPX address of the peer who told Cisco IOS software about this destination. The first *n* of these entries, where *n* is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(345088/319488)	The first number is the Enhanced IGRP metric that represents the cost to the destination. The second number is the Enhanced IGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.

The following are sample outputs from the **show ipx eigrp topology** command when an IPX network number is specified:

Internal EIGRP IPX Network: Example

```
Router# show ipx eigrp topology BB

EIGRP-IPX Topology Entry for AS(2)/ID(0.aabb.cc01.f600) for BB
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
  Descriptor Blocks:
  AA.aabb.cc01.f500 (Ethernet0/0), from AA.aabb.cc01.f500, Send flag is 0x0
      Composite metric is (409600/128256), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

External EIGRP IPX Network: Example

```
Router# show ipx eigrp topology CC

EIGRP-IPX Topology Entry for AS(2)/ID(0.aabb.cc01.f600) for CC
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
  Descriptor Blocks:
  AA.aabb.cc01.f500 (Ethernet0/0), from AA.aabb.cc01.f500, Send flag is 0x0
      Composite metric is (409600/128256), route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is  aabb.cc01.f500
        AS number of route is 0
        External protocol is RIP, external metric is 1
        Administrator tag is 0 (0x00000000)
```

Table 11 describes the fields shown in the display.

Table 11 show ipx eigrp topology Field Descriptions—Specific Network

Field	Description
BB, CC	IPX network number of the destination.
State is ...	State of this entry. It can be either Passive or Active. Passive means that no Enhanced IGRP computations are being performed for this destination, and Active means that they are being performed.
Query origin flag	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
Successor(s)	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
Ethernet0	Interface from which this information was learned.

Table 11 show ipx eigrp topology Field Descriptions—Specific Network (continued)

Field	Description
from	Peer from whom the information was learned. For connected and redistributed routers, this is 0.0000.0000.0000. For information learned via Enhanced IGRP, this is the peer's address. Currently, for information learned via Enhanced IGRP, the peer's IPX address always matches the address in the "Next hop is" field.
Composite metric is	Enhanced IGRP composite metric. The first number is this device's metric to the destination, and the second is the peer's metric to the destination.
Send flag	Numeric representation of the "flags" field described in Table 9. It is 0 when nothing is being sent, 1 when an Update is being sent, 3 when a Query is being sent, and 4 when a Reply is being sent. Currently, 2 is not used.
Route is ...	Type of router. It can be either internal or external. Internal routes are those that originated in an Enhanced IGRP autonomous system, and external are routes that did not. Routes learned through RIP are always external.
This is an ignored route	Indicates that this path is being ignored because of filtering.
Vector metric:	This section describes the components of the Enhanced IGRP metric.
Minimum bandwidth	Minimum bandwidth of the network used to reach the next hop.
Total delay	Delay time to reach the next hop.
Reliability	Reliability value used to reach the next hop.
Load	Load value used to reach the next hop.
Minimum MTU	Minimum MTU size of the network used to reach the next hop.
Hop count	Number of hops to the next hop.
External data:	This section describes the original protocol from which this route was redistributed. It appears only for external routes.
Originating router	Network address of the router that first distributed this route into Enhanced IGRP.
External protocol..metric..delay	External protocol from which this route was learned. The metric will match the external hop count displayed by the **show ipx route** command for this destination. The delay is the external delay.
Administrator tag	Not currently used.
Flag	Not currently used.

show ipx eigrp traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx eigrp traffic** command is not supported in Cisco IOS software.

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received, use the **show ipx eigrp traffic** command in privileged EXEC mode.

show ipx eigrp *autonomous-system-number* **traffic**

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is the sample output from the **show ipx eigrp traffic** command:

```
Router# show ipx eigrp 2 traffic

EIGRP-IPX Traffic Statistics for AS(2)
  Hellos sent/received: 7454/2507
  Updates sent/received: 20/20
  Queries sent/received: 1/17
  Replies sent/received: 9/1
  Acks sent/received: 22/27
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 199
  PDM Process ID: 171
  Socket Queue: 0 (current)
  Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

Table 12 describes the significant fields shown in the display.

Table 12 show ipx eigrp traffic Field Descriptions

Field	Description
AS	Autonomous system number specified in the **ip router** command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

show ipx interface

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx interface** command is not supported in Cisco IOS software.

To display the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show ipx interface** command in EXEC mode.

show ipx interface [*type number*]

Syntax Description

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.
number	(Optional) Interface number.

Command Modes EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to add Get General Service (GGS) filters and some counters per interface.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples The following is sample output from the **show ipx interface** command:

```
Router# show ipx interface serial 2/0

Serial2/0 is up, line protocol is up
  IPX address is 123.00e0.1efc.0b01 [up]
  Delay of this IPX network, in ticks is 6 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 60 seconds
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is 900
  Outgoing access list is not set
  IPX helper access list is not set
```

```
SAP GGS output filter list is 1000
SAP GNS processing enabled, delay 0 ms, output filter list is not set
SAP Input filter list is not set
SAP Output filter list is not set
SAP Router filter list is not set
Input filter list is not set
Output filter list is not set
Router filter list is not set
Netbios Input host access list is not set
Netbios Input bytes access list is not set
Netbios Output host access list is not set
Netbios Output bytes access list is not set
Updates each 60 seconds aging multiples RIP:3 SAP:3
SAP interpacket delay is 55 ms, maximum size is 480 bytes
RIP interpacket delay is 55 ms, maximum size is 432 bytes
RIP response delay is not set
 Watchdog spoofing is currently enabled
      On duration 1 hour(s), 00:24:50 remaining
      Off duration 18 minute(s), 00:00:00 remaining
 SPX spoofing is disabled, idle time 60
 IPX accounting is disabled
 IPX fast switching is configured (enabled)
 RIP packets received 0, RIP packets sent 906, 0 Throttled
 RIP specific requests received 0, RIP specific replies sent 0
 RIP general requests received 0, 0 ignored, RIP general replies sent 0
 SAP packets received 0, SAP packets sent 25, 0 Throttled
 SAP GNS packets received 0,k SAP GNS replies sent 0
 SAP GGS packets received 0, 0 ignored, SAP GGS replies sent 0
```

Table 13 describes the fields shown in the display.

Table 13 show ipx interface Field Descriptions

Field	Description
Serial is ..., line protocol is...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
IPX address is ...	Network and node address of the local router interface, followed by the type of encapsulation configured on the interface and the status of the interface. See the **ipx network** command for a list of possible values.
[up]	Indicates whether IPX routing is enabled (up) or disabled (down) on the interface.
NOVELL-ETHER	Type of encapsulation being used on the interface, if any.
Delay of this IPX network, in ticks ...	Value of the ticks field (configured with the **ipx delay** command).
throughput	Throughput of the interface (configured with the **ipx spx-idle-time** interface configuration command).
link delay	Link delay of the interface (configured with the **ipx link-delay** interface configuration command).
IPXWAN processing...	Indicates whether IPXWAN processing has been enabled on this interface with the **ipx ipxwan** command.

Table 13 show ipx interface Field Descriptions (continued)

Field	Description
IPX SAP update interval	Indicates the frequency of outgoing Service Advertising Protocol (SAP) updates (configured with the **ipx update interval** command).
IPX type 20 propagation packet forwarding...	Indicates whether forwarding of IPX type 20 propagation packets (used by NetBIOS) is enabled or disabled on this interface, as configured with the **ipx type-20-propagation** command.
Incoming access list	Indicates whether an incoming access list has been configured on this interface.
Outgoing access list	Indicates whether an access list has been enabled with the **ipx access-group** command.
IPX helper access list	Number of the broadcast helper list applied to the interface with the **ipx helper-list** command.
SAP GGS output filter list	Number of the Get General Server (GGS) response filter applied to the interface with the **ipx output-ggs-filter** command.
SAP GNS processing ...	Indicates if GNS processing is enabled, what the response delay set is, and if there is any GNS output access-list configured
delay	Indicates the delay of this ipx network, represented in metric ticks for routers on this interface using the IPX RIP routing protocol.
output filter list	Number of the Get Nearest Server (GNS) response filter applied to the interface with the **ipx output-gns-filter** command.
SAP Input filter list	Number of the input SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Output filter list	Number of the output SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Router filter list	Number of the router SAP filter applied to the interface with the **ipx router-sap-filter** command.
Input filter list	Number of the input filter applied to the interface with the **ipx input-network-filter** command.
Output filter list	Number of the output filter applied to the interface with the **ipx output-network-filter** command.
Router filter list	Number of the router entry filter applied to the interface with the **ipx router-filter** command.
Netbios Input host access list	Name of the IPX NetBIOS input host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Input bytes access list	Name of the IPX NetBIOS input bytes filter applied to the **ipx netbios input-access-filter** interface with the **ipx netbios input-access-filter bytes** command.

Table 13 show ipx interface Field Descriptions (continued)

Field	Description
Netbios Output host access list	Name of the IPX NetBIOS output host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Output bytes access list	Name of the IPX NetBIOS output bytes filter applied to the interface with the **input netbios input-access-filter bytes** command.
Updates each ...	How often Cisco IOS software sends Routing Information Protocol (RIP) updates, as configured with the **ipx update sap-after-rip** command.
SAP interpacket delay	Interpacket delay for SAP updates.
RIP interpacket delay	Interpacket delay for RIP updates.
RIP response delay	Delay for RIP responses.
Watchdog spoofing ...	Indicates whether watchdog spoofing is enabled or disabled for this interface, as configured with the **ipx watchdog spoof** command. This information is displayed only on serial interfaces.
SPX spoofing ...	Indicates whether SPX spoofing is enabled or disabled for this interface.
IPX accounting	Indicates whether IPX accounting has been enabled with the **ipx accounting** command.
IPX fast switching IPX autonomous switching	Indicates whether IPX fast switching is enabled (default) or disabled for this interface, as configured with the **ipx route-cache** command. (If IPX autonomous switching is enabled, it is configured with the **ipx route-cache cbus** command.)
RIP packets received, RIP packets sent, Throttled	Number of RIP packets received, sent, or dropped.
RIP specific requests received, RIP specific replies sent,	Number of RIP specific requests received and the number of RIP specific replies sent.
RIP general requests received, ignored, RIP general replies sent	Number of RIP general requests received and ignored. Number of RIP general replies sent.
SAP GNS packets received, SAP GNS packets sent, Throttled	Number of SAP Get Nearest Server (GNS) packets received, sent, or dropped.
SAP GGS packets received, SAP GGS packets sent, Throttled	Number of SAP Get General Server (GGS) packets received, sent, or dropped.
SAP packets received, SAP packets sent, Throttled	Number of SAP packets received, sent, or dropped.

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
access-list (IPX standard)	Defines a standard IPX access list.
ipx accounting	Enables IPX accounting.

Command	Description
ipx default-output-rip delay	Sets the default interpacket delay for RIP updates sent on all interfaces.
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx delay	Sets the tick count.
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
ipx netbios output-access-filter	Controls outgoing IPX NetBIOS FindName messages.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-network-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx output-sap-filter	Controls which services are included in SAP updates sent by Cisco IOS software.
ipx route-cache	Enables IPX fast switching.
ipx router-filter	Filters the routers from which packets are accepted.
ipx router-sap-filter	Filters SAP messages received from a particular router.
ipx routing	Enables IPX routing.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
ipx watchdog	Enables watchdog processing.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.

show ipx nasi connections

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nasi connections** command is not supported in Cisco IOS software.

To display the status of NetWare Asynchronous Services Interface (NASI) connections, use the **show ipx nasi connections** command in EXEC mode.

show ipx nasi connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

Use the **show ipx nasi connections** command to view the addresses of remote NASI clients local connection addresses and status bits. If the connection is associated with a tty port then the `Connected to` line field appears in the **show ipx nasi connections** output.

Examples

The following is sample output from the **show ipx nasi connections** command:

```
Router# show ipx nasi connections

NASI Remote: A001500::0020.afe5.3ec5:626C   Local: ACBB::0000.0000.0001:2010
  flags 0

NASI Remote: A001500::0020.afe5.3ec5:6E6C   Local: ACBB::0000.0000.0001:20D0
  flags 0
   Connected to line 2  incount 0  outcount 0  OVF 0
```

The following sample display shows an incoming NASI connection on tty line 2:

```
Router# show users
```

```
    Line     User      Host(s)              Idle Location
*   0 con 0            idle                    1
    2 tty 2  chris     incoming                1 A001500.0020.afe5.3ec5
```

Table 14 describes the significant fields shown in the display.

Table 14 show ipx nasi connections Field Descriptions

Field	Description
NASI Remote	• xxxxxxx::yyyyyyyyy:zzzz is the address for the remote NASI client connected to the router. • xxxx is the Internetwork Packet Exchange (IPX) network number. • yyyyyyy is the IPX host node (MAC address) for the client. • zzzz is the SPX connection number.
Local	xxxxxxx::yyyyyyyyyy:zzzz is the local address associated with this connection on the router end of the link.
flags	A status bit that is used internally to allow and close connections.
Connected to line 2	Appears only when the connection is associated with a tty port. Indicates that this NASI connection is attached to tty 2.
incount 0	Data from the remote client.
outcount 0	Data to be sent to the remote client.
OVF 0	Refers to the number of times data could not be written to the tty line, because the buffers were full. Ideally, this counter should stay at 0.

Related Commands

Command	Description
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

show ipx nhrp

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nhrp** command is not supported in Cisco IOS software.

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ipx nhrp** command in EXEC mode.

show ipx nhrp [**dynamic** | **static**] [*type number*]

Syntax Description

dynamic	(Optional) Displays only the dynamic (learned) IPX-to-NBMA address cache entries.
static	(Optional) Displays only the static IPX-to-NBMA address entries in the cache (configured through the **ipx nhrp map** command).
type	(Optional) Interface type for which to display the NHRP cache. Valid options are **atm**, **serial**, and **tunnel**.
number	(Optional) Interface number for which to display the NHRP cache.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx nhrp** command:

```
Router# show ipx nhrp

1.0000.0c35.de01, Serial1 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: c141.0001.0001
```

```
1.0000.0c35.e605, Serial1 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: c141.0001.0002
```

Table 15 describes the fields shown in the display.

Table 15 show ipx nhrp Field Descriptions

Field	Description
1.0000.0c35.de01	IPX address in the IPX-to-NBMA address cache.
Serial1 created 0:00:43	Interface type and number and how long ago it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ipx nhrp holdtime** command.
Type	Value can be one of the following: • dynamic—NBMA address was obtained from NHRP Request packet. • static—NBMA address was statically configured.
Flags	Value can be one of the following: • authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IPX address mapping for a particular destination. • implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router. • negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.
NBMA address	Nonbroadcast, multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, SMDS, multipoint tunnel).

Related Commands

Command	Description
ipx nhrp map	Statically configures the IPX-to-NBMA address mapping of IPX destinations connected to an NBMA network.

show ipx nhrp traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nhrp traffic** command is not supported in Cisco IOS software.

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ipx nhrp traffic** command in EXEC mode.

show ipx nhrp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx nhrp traffic** command:

```
Router# show ipx nhrp traffic

Tunnel0
  request packets sent: 2
  request packets received: 4
  reply packets sent: 4
  reply packets received: 2
  register packets sent: 0
  register packets received: 0
  error packets sent: 0
  error packets received: 0
```

Table 16 describes the fields shown in the display.

Table 16 show ipx nhrp traffic Field Descriptions

Field	Description
Tunnel 0	Interface type and number.
request packets sent	Number of NHRP Request packets originated from this station.
request packets received	Number of NHRP Request packets received by this station.
reply packets sent	Number of NHRP Reply packets originated from this station.
reply packets received	Number of NHRP Reply packets received by this station.
register packets sent	Number of NHRP Register packets originated from this station. Currently, our routers do not send Register packets, so this value is 0.
register packets received	Number of NHRP Register packets received by this station. Currently, our routers do not send Register packets, so this value is 0.
error packets sent	Number of NHRP Error packets originated by this station.
error packets received	Number of NHRP Error packets received by this station.

show ipx nlsp database

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp database** command is not supported in Cisco IOS software.

To display the entries in the link-state packet (LSP) database, use the **show ipx nlsp database** command in EXEC mode.

show ipx nlsp [*tag*] **database** [*lspid*] [**detail**]

Syntax Description

tag	(Optional) Names the NLSP process. The *tag* can be any combination of printable characters.
lspid	(Optional) Link-state protocol ID (LSPID). You must specify this in the format *xxxx.xxxx.xxxx.yy-zz*. The components of this argument have the following meaning: • *xxxx.xxxx.xxxx* is the system identifier. • *yy* is the pseudo identifier. • *zz* is the LSP number.
detail	(Optional) Displays the contents of the LSP database entries. If you omit this keyword, only a summary display is shown.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When you specify an NLSP *tag*, the router displays the link-state packet database entries for that NLSP process. An NLSP *process* is a router's databases working together to manage route information about an area. NLSP version 1.0 routers are always in the same area. Each router has its own adjacencies,

link-state, and forwarding databases. These databases operate collectively as a single *process* to discover, select, and maintain route information about the area. NLSP version 1.1 routers that exist within a single area also use a single process.

NLSP version 1.1 routers that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These routers manage an adjacencies, link-state, and area address database for each area to which they attach. Collectively, these databases are still referred to as a *process*. The forwarding database is shared among processes within a router. The sharing of entries in the forwarding database is automatic when all processes interconnect NLSP version 1.1 areas.

Configure multiple NLSP processes when a router interconnects multiple NLSP areas.

Note NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

If you omit all options, a summary display is shown.

Examples

The following is sample output from the **show ipx nlsp database** command:

```
Router# show ipx nlsp database detail

LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.3097.00-00* 0x00000042   0xC512        699           0/0/0
0000.0C00.3097.06-00* 0x00000027   0x0C27        698           0/0/0
0000.0C02.7471.00-00  0x0000003A   0x4A0F        702           0/0/0
0000.0C02.7471.08-00  0x00000027   0x0AF0        702           0/0/0
0000.0C02.7471.0A-00  0x00000027   0xC589        702           0/0/0
0000.0C02.747D.00-00  0x0000002E   0xC489        715           0/0/0
0000.0C02.747D.06-00  0x00000027   0xEEFE        716           0/0/0
0000.0C02.747D.0A-00  0x00000027   0xFE38        716           0/0/0
0000.0C02.74AB.00-00  0x00000035   0xE4AF        1059          0/0/0
0000.0C02.74AB.0A-00  0x00000027   0x34A4        705           0/0/0
0000.0C06.FBEE.00-00  0x00000038   0x3838        1056          0/0/0
0000.0C06.FBEE.0D-00  0x0000002C   0xD248        1056          0/0/0
0000.0C06.FBEE.0E-00  0x0000002D   0x7DD2        1056          0/0/0
0000.0C06.FBEE.17-00  0x00000029   0x32FB        1056          0/0/0

0000.0C00.AECC.00-00* 0x000000B6   0x62A8        7497          0/0/0
  IPX Area Address: 00000000 00000000
  IPX Mgmt Info 87.0000.0000.0001  Ver 1  Name oscar
  Metric: 45 Lnk 0000.0C00.AECC.06  MTU 1500  Dly 8000  Thru 64K  PPP
  Metric: 20 Lnk 0000.0C00.AECC.02  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
  Metric: 20 Lnk 0000.0C01.EF90.0C  MTU 1500  Dly 1000  Thru 10000K  802.3 Raw
0000.0C00.AECC.02-00* 0x00000002   0xDA74        3118          0/0/0
  IPX Mgmt Info E0.0000.0c00.aecc  Ver 1  Name Ethernet0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  802.3 Raw
0000.0C00.AECC.06-00* 0x00000002   0x5DB9        7494          0/0/0
  IPX Mgmt Info 0.0000.0000.0000  Ver 1  Name Serial0
  Metric: 0  Lnk 0000.0C00.AECC.00  MTU 0  Dly 0  Thru 0K  PPP
  Metric: 1  IPX Ext D001  Ticks 0
  Metric: 1  IPX SVC Second-floor-printer  D001.0000.0000.0001  Sock 1  Type 4
```

Table 17 describes the fields shown in the display.

Table 17 show ipx nlsp database Field Descriptions

Field	Description
LSPID	System ID (network number), pseudonode circuit identifier, and fragment number.
LSP Seq Num	Sequence number of this LSP.
LSP Checksum	Checksum of this LSP.
LSP Holdtime	Time until this LSP expires, in hours or seconds.
ATT/P/OL	Indicates which of three bits are set. A “1” means the bit is set, and a “0” means it is not set. ATT is the L2-attached bit. OL is the overload bit. P is the partition repair bit. This bit is not used in NLSP.
IPX Area Address:	Area address of the router advertising the LSP.
IPX Mgmt Info	Management information. For nonpseudonode LSPs, the internal network number is advertised in this field. For pseudonode LSPs, the network number of the associated interface is advertised.
Ver	NLSP version running on the advertising router.
Name	For nonpseudonode LSPs, the name of the router. For pseudonode LSPs, the name (or description, if configured) of the associated interface.
Link Information	Information about the link.
Metric:	NLSP metric (cost) for the link. Links from a pseudonode to real nodes have a cost of 0 so that this link cost is not counted twice.
Lnk	System ID of the adjacent node.
MTU	MTU of the link in bytes. For pseudonode LSPs, the value in this field is always 0.
Dly	Delay of the link in microseconds. For pseudonode LSPs, the value in this field is always 0.
Thru	Throughput of the link in bits per second. For pseudonode LSPs, the value in this field is always 0.
802.3 Raw, Generic LAN	Link media type.
External (RIP) Networks	Information about an external (RIP) network.
Metric:	Received RIP hop count.
IPX Ext	IPX network number.
Ticks	Received RIP tick count.

Table 17 show ipx nlsp database Field Descriptions (continued)

Field	Description
SAP Services	Information about SAP services.
Metric:	Received SAP hop count.
IPX SVC	Name of the IPX service.
D001.000.0000.0001	IPX address of the server advertising this service.
Sock	Socket number of the service.
Type	Type of service.

show ipx nlsp neighbors

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp neighbors** command is not supported in Cisco IOS software.

To display NetWare Link Services Protocol (NLSP) neighbors and their states, use the **show ipx nlsp neighbors** command in EXEC mode.

show ipx nlsp [*tag*] **neighbors** [*interface*] [**detail**]

Syntax Description

tag	(Optional) Names the NLSP process. The value of the *tag* argument can be any combination of printable characters.
interface	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about the neighbor. If you omit this keyword, only a summary display is shown.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

When you specify an NLSP *tag* value, the router displays the NLSP neighbors for that NLSP process. An NLSP process is a router's databases working together to manage route information about an area. NLSP version 1.0 routers must be in a single area. Each router has its own adjacencies, link-state, and forwarding databases. These databases operate collectively as a single process to discover, select, and maintain route information about the area. NLSP version 1.1 routers that exist within a single area also use a single process.

NLSP version 1.1 routers that interconnect multiple areas use multiple processes to discover, select, and maintain route information about the areas they interconnect. These routers manage adjacencies, link-state, and area address databases for each area to which they attach. Collectively, these databases

are still referred to as a process. The forwarding database is shared among processes within a router. The sharing of entries in the forwarding database is automatic when all processes interconnect NLSP version 1.1 areas.

You must configure multiple NLSP processes when a router interconnects multiple NLSP areas.

Note NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

If you omit the keyword **detail**, a summary display is shown.

Examples

The following command output from the **show ipx nlsp neighbors** command shows a summary display of three adjacencies on two circuits:

```
Router# show ipx nlsp neighbors

System Id  Interface  State  Holdtime  Priority  Cir  Adj  Circuit Id
dtp-37     Et1.2      Up     21        64        mc   mc   dtp-37.03
dtp-37     Et1.1      Up     58        44        bc   mc   dtp-17.02
dtp-17     ET1.1      Up     27        64        bc   bc   dtp-17.02
```

This display indicates the following information about the first circuit (Circuit Id = dtp-37.03):

- Multicast addressing is in use (Cir = mc).
- The neighbor supports multicast addressing (Adj = mc).

This display indicates the following information about the second circuit (Circuit Id = dtp-17.02):

- The broadcast address is in use (Cir = bc).
- The first neighbor (System Id = dtp-37) supports multicast addressing (Adj = mc).
- The second neighbor (System Id = dtp-17) does not support multicast addressing (Adj = bc). This adjacency explains why the broadcast address is in use on the second circuit.

The following is sample output from the **show ipx nlsp neighbors detail** command:

```
Router# show ipx nlsp neighbors detail

System Id       Interface  State  Holdtime  Priority  Cir  Adj  Circuit Id
0000.0C01.EF90  Ethernet1  Up     25        64        mc   mc   0000.0C01.EF90.0C
  IPX Address: E1.0000.0c01.ef91
  IPX Areas:  00000000/00000000
  Uptime: 2:59:11
```

Table 18 describes the fields shown in the display.

Table 18 show ipx nlsp neighbors Field Descriptions

Field	Description
System Id	System ID of the neighbor.
Interface	Interface on which the neighbor was discovered.
State	State of the neighbor adjacency.
Holdtime	Remaining time before the router assumes that the neighbor has failed.
Priority	Designated router election priority.

Table 18 show ipx nlsp neighbors Field Descriptions (continued)

Field	Description
Cir	NLSP addressing state (multicast or broadcast) of the interface.
Adj	NSLP addressing state (multicast or broadcast) of the adjacent neighbor.
Circuit Id	Neighbor's internal identifier for the circuit.
IPX Address:	IPX address on this network of the neighbor.
IPX Areas:	IPX area addresses configured on the neighbor.
Uptime:	Time since the router discovered the neighbor. Time is formatted in *hh*:*mm*:*ss*.

show ipx nlsp spf-log

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx nlsp spf-log** command is not supported in Cisco IOS software.

To display a history of the shortest path first (SPF) calculations for NetWare Link Services Protocol (NLSP), use the **show ipx nlsp spf-log** command in EXEC mode.

show ipx nlsp [*tag*] **spf-log**

Syntax Description

tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx nlsp spf-log** command:

```
Router# show ipx nlsp spf-log

    Level 1 SPF log
  When   Duration  Nodes  Count  Triggers
0:30:59     1028     84      1  TLVCONTENT
0:27:09     1016     84      1  TLVCONTENT
0:26:30     1136     84      1  TLVCONTENT
0:23:11     1244     84      1  TLVCONTENT
0:22:39      924     84      2  TLVCONTENT
0:22:08     1036     84      1  TLVCONTENT
0:20:02     1096     84      1  TLVCONTENT
0:19:31     1140     84      1  TLVCONTENT
0:17:25      964     84      2  PERIODIC TLVCONTENT
0:16:54      996     84      1  TLVCONTENT
```

```
0:16:23      984     84       1  TLVCONTENT
0:15:52     1052     84       1  TLVCONTENT
0:14:34     1112     84       1  TLVCONTENT
0:13:37      992     84       1  TLVCONTENT
0:13:06     1036     84       1  TLVCONTENT
0:12:35     1008     84       1  TLVCONTENT
0:02:52     1032     84       1  TLVCONTENT
0:02:16     1032     84       1  PERIODIC
0:01:44     1000     84       3  TLVCONTENT
```

Table 19 describes the fields shown in the display.

Table 19 show ipx nlsp spf-log Field Descriptions

Field	Descriptions
When	Amount of time since the SPF calculation took place.
Duration	Amount of time (in milliseconds) that the calculation required.
Nodes	Number of link state packets (LSPs) encountered during the calculation.
Count	Number of times that the SPF calculation was triggered before it actually took place. An SPF calculation is normally delayed for a short time after the event that triggers it.
Triggers	List of the types of triggers that were recorded before the SPF calculation occurred (more than one type may be displayed): • PERIODIC—Periodic SPF calculation (every 15 minutes). • NEWSYSID—New system ID was assigned. • NEWAREA—New area address was configured. • RTCLEARED—IPX routing table was manually cleared. • NEWMETRIC—Link metric of an interface was reconfigured. • ATTACHFLAG—Level 2 router has become attached or unattached from the rest of the level 2 topology. • LSPEXPIRED—LSP has expired. • NEWLSP—New LSP has been received. • LSPHEADER—LSP with changed header fields was received. • TLVCODE—LSP with a changed (Type-Length-Value) TLV code field was received. • TLVCONTENT—LSP with changed TLV contents was received. • AREASET—Calculated area address set has changed. • NEWADJ—New neighbor adjacency came up. • DBCHANGED—NLSP link state database was manually cleared.

show ipx route

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, 15.2(2)T, and 15.1(1)SY, the **show ipx route** command is not supported in Cisco IOS software.

To display the contents of the IPX routing table, use the **show ipx route** command in EXEC mode.

show ipx route [*network*] [**default**] [**detailed**]

Syntax Description

network	(Optional) Number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
default	(Optional) Displays the default route. This is equivalent to specifying a value of FFFFFFFE for the argument *network*.
detailed	(Optional) Displays detailed route information.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced. The following keywords were added: • **default** • **detailed**
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.
15.1(1)SY	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx route** command:

```
Router# show ipx route

Codes: C - Connected primary network,     c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

8 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D40 is the internal network
C        100 (NOVELL-ETHER), Et1
C       7000 (TUNNEL),       Tu1
S        200 via     7000.0000.0c05.6023,        Tu1
R        300 [02/01] via      100.0260.8c8d.e748,   19s, Et1
S       2008 via     7000.0000.0c05.6023,        Tu1
R     CC0001 [02/01] via      100.0260.8c8d.e748,   19s, Et1
```

Table 20 describes the fields shown in the display.

Table 20 show ipx route Field Descriptions

Field	Description
Codes	Codes defining how the route was learned.
L - Local	Internal network number.
C - Connected primary network	Directly connected primary network.
c - connected secondary network	Directly connected secondary network.
S - Static	Statically defined route via the **ipx route** command.
R - RIP	Route learned from a RIP update.
E - EIGRP	Route learned from an Enhanced IGRP (EIGRP) update.
W - IPXWAN	Directly connected route determined via IPXWAN.
8 Total IPX routes	Number of routes in the IPX routing table.
No parallel paths allowed	Maximum number of parallel paths for which the Cisco IOS software has been configured with the **ipx maximum-paths** command.
Novell routing algorithm variant in use	Indicates whether Cisco IOS software is using the IPX-compliant routing algorithms (default).
Net 1	Network to which the route goes.
[3/2]	Delay/Metric. Delay is the number of IBM clock ticks (each tick is 1/18 seconds) reported to the destination network. Metric is the number of hops reported to the same network. Delay is used as the primary routing metric, and the metric (hop count) is used as a tie breaker.
via *network.node*	Address of a router that is the next hop to the remote network.

Table 20 show ipx route Field Descriptions (continued)

Field	Description
age	Amount of time (in hours, minutes, and seconds) that has elapsed since information about this network was last received.
uses	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
Ethernet0	Interface through which packets to the remote network will be sent.
(NOVELL-ETHER)	Encapsulation (frame) type. This is shown only for directly connected networks.
is directly connected	Indicates that the network is directly connected to the router.

When Cisco IOS software generates an aggregated route, the **show ipx route** command displays a line item similar to the following:

```
NA      1000 FFFFF000 [**][**/06] via        0.0000.0000.0000,  163s, Nu0
```

In the following example, the router that sends the aggregated route also generates the aggregated route line item in its table. But the entry in the table points to the null interface (*Nu0*), indicating that if this aggregated route is the most-specific route when a packet is being forwarded, the router drops the packet instead.

```
Router# show ipx route

Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

13 Total IPX routes. Up to 4 parallel paths and 16 hops allowed.

No default route known.

NA      1000 FFFFF000 [**][**/06] via        0.0000.0000.0000,  163s, Nu0
L       2008 is the internal network
C          1 (NOVELL-ETHER),  Et0
C         89 (SAP),           To0
C         91 (SAP),           To1
C        100 (NOVELL-ETHER),  Et1
N          2 [19][01/01]          via       91.0000.30a0.51cd,  317s, To1
N          3 [19][01/01]          via       91.0000.30a0.51cd,  327s, To1
N         20 [20][01/01]          via        1.0000.0c05.8b24, 2024s, Et0
N        101 [19][01/01]          via       91.0000.30a0.51cd,  327s, To1
NX      1000 [20][02/02][01/01]   via        1.0000.0c05.8b24, 2024s, Et0
N       2010 [20][02/01]          via        1.0000.0c05.8b24, 2025s, Et0
N       2011 [19][02/01]          via       91.0000.30a0.51cd,  328s, To1
```

The following is sample output from the **show ipx route detailed** command:

```
Router# show ipx route detailed
```

```
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, s - seconds, u - uses

9 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

L        D35 is the internal network
C       E001 (SAP),           Et0
C      D35E2 (NOVELL-ETHER),  Et2
R        D34 [02/01]
           -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
N        D36 [20][02/01]
           -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                  10000000:1000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
NX       D40 [20][03/02][02/01]
           -- via    D35E2.0000.0c02.8cfc, 704s,     1u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
R      D34E1 [01/01]
           -- via     E001.0000.0c02.8cf9,  43s,     1u, Et0
NX     D40E1 [20][02/02][01/01]
           -- via    D35E2.0000.0c02.8cfc, 704s,     3u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
N     D36E02 [20][01/01]
           -- via    D35E2.0000.0c02.8cfc, 705s,     2u, Et2
                  10000000:2000:1500:0000.0c02.8cfb:6:0000.0c02.8cfc
```

Table 21 describes the additional fields shown in the display.

Table 21 show ipx route detailed Field Descriptions

Field	Description
1u	Number of times this network has been looked up in the route table. This field is incremented when a packet is process-switched, even if the packet is eventually filtered and not sent. As such, this field represents a fair estimate of the number of times a route gets used.
10000000	(NLSP only) Throughput (end to end).
3000	(NLSP only) Link delay (end to end).
1500	(NLSP only) MTU (end to end).
0000.0c02.8cfb	(NLSP only) System ID of the next-hop router.
6	(NLSP only) Local circuit ID.
0000.0c02.8cfc	(NLSP only) MAC address of the next-hop router.

Related Commands

Command	Description
clear ipx route	Deletes routes from the IPX routing table.
ipx maximum-paths	Sets the maximum number of equal-cost paths Cisco IOS software uses when forwarding packets.
ipx nlsp metric	Configures an interface to use multicast addressing.
ipx route	Adds a static route or static NLSP route summary to the routing table.

show ipx servers

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx servers** command is not supported in Cisco IOS software.

To list the IPX servers discovered through Service Advertising Protocol (SAP) advertisements, use the **show ipx servers** command in EXEC mode.

show ipx servers [**detailed**] [**network** *network-number*] [**type** *service-type-number*] [**unsorted** | [**sorted** [**name** | **network** | **type**]]] [**regexp** *name*]

Syntax Description

detailed	(Optional) Displays comprehensive information including path details.
network	(Optional) Displays IPX SAP services on a specified network.
network-number	(Optional) IPX network number. 1 to FFFFFFFF.
type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.
service-type-number	(Optional) IPX service type number. 1 to FFFF. When used with the **network** keyword, displays a list of all SAPs known to a particular network number.
unsorted	(Optional) Does not sort entries when displaying IPX servers.
sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
network	(Optional) Displays the IPX servers numerically by network number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Defaults

IPX servers are displayed numerically by SAP service type.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **unsorted** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.

Release	Modification
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following example uses a regular expression to display SAP table entries corresponding to a particular group of servers in the accounting department of a company:

```
Router# show ipx servers regexp ACCT\_SERV.+

Codes: S - Static, P - Periodic, E - EIGRP, H - Holddown, + = detail
9 Total IPX Servers

Table ordering is based on routing and server info

 Type  Name            Net  Address        Port  Route  Hops Itf
S 108  ACCT_SERV_1     7001.0000.0000.0001:0001   1/01   2   Et0
S 108  ACCT_SERV_2     7001.0000.0000.0001:0001   1/01   2   Et0
S 108  ACCT_SERV_3     7001.0000.0000.0001:0001   1/01   2   Et0
```

For more information on regular expressions, refer to the “Regular Expressions” appendix in *Cisco IOS Dial Technologies Command Reference*.

Related Commands

Command	Description
ipx sap	Specifies static SAP entries.

show ipx spx-spoof

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx spx-spoof** command is not supported in Cisco IOS software.

To display the table of Sequenced Packet Exchange (SPX) connections through interfaces for which SPX spoofing is enabled, use the **show ipx spx-spoof** command in EXEC mode.

show ipx spx-spoof

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx spx-spoof** command:

```
Router# show ipx spx-spoof

Local SPX Network.Host:sock Cid  Remote SPX Network.Host:sock Cid   Seq  Ack  Idle
CC0001.0000.0000.0001:8104  0D08 200.0260.8c8d.e7c6:4017      7204  09   0021 120
CC0001.0000.0000.0001:8104  0C08 200.0260.8c8d.c558:4016      7304  07   0025 120
```

Table 22 describes the fields shown in the display.

Table 22 show ipx spx-spoof Field Descriptions

Field	Description
Local SPX Network.Host:sock	Address of the local end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the local end of the SPX connection.
Remote SPX Network.Host:sock	Address of the remote end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the remote end of the SPX connection.
Seq	Sequence number of the last data packet transferred.
Ack	Number of the last solicited acknowledge received.
Idle	Amount of time elapsed since the last data packet was transferred.

Related Commands

Command	Description
ipx spx-idle-time	Sets the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer.
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.

show ipx traffic

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show ipx traffic** command is not supported in Cisco IOS software.

To display information about the number and type of IPX packets sent and received, use the **show ipx traffic** command in EXEC mode.

show ipx [**nlsp**] **traffic** [**since** {**bootup** | **show**}]

Syntax Description

nlsp	(Optional) Displays only NetWare Link Services Protocol (NLSP) traffic counters.
since bootup	(Optional) Displays traffic statistics since bootup.
since show	(Optional) Displays traffic statistics since last **show** command.

Defaults

Display traffic statistics since bootup or since the last **clear** command was entered.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	The following keywords were added: • **nlsp** • **since bootup** • **since show**
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show ipx traffic** command:

```
Router# show ipx traffic

System Traffic for 0.0000.0000.0001 System-Name: Router
Time since last clear: never
Rcvd:  0 total, 0 format errors, 0 checksum errors, 0 bad hop count
       0 packets pitched, 0 local destination, 0 multicast
Bcast: 0 received, 0 sent
Sent:  0 generated, 0 forwarded
       0 encapsulation failed, 0 no route
SAP:   0 Total SAP requests, 0 Total SAP replies, 1 servers
       0 SAP General Requests, 2 sent, 0 ignored, 0 replies
       0 SAP Get Nearest Server requests, 0 replies
       0 SAP Nearest Name requests, 0 replies
          0 SAP General Name requests, 0 replies
          0 SAP advertisements received, 324 sent, 0 Throttled
       0 SAP flash updates sent, 0 SAP format errors
RIP:   0 RIP requests, 0 ignored, 0 RIP replies, 3 routes
       0 RIP advertisements received, 684 sent, 0 Throttled
       0 RIP flash updates sent, 0 atlr sent
          2 RIP general requests sent
          0 RIP format errors
Echo:  Rcvd 0 requests, 0 replies
       Sent 0 requests, 0 replies
       0 unknown: 0 no socket, 0 filtered, 0 no helper
            0 SAPs throttled, freed NDB len 0
Watchdog:
       0 packets received, 0 replies spoofed
Queue lengths:
       IPX input: 0, SAP 0, RIP 0, GNS 0
       SAP throttling length: 0/(no limit), 0 nets pending lost route reply
       Delayed process creation: 0
EIGRP: Total received 0, sent 0
       Updates received 0, sent 0
       Queries received 0, sent 0
       Replies received 0, sent 0
       SAPs received 0, sent 0
NLSP:  Time since last clear: never
NLSP:  Level-1 Hellos (sent/rcvd): 0/0
       PTP Hellos    (sent/rcvd): 0/0
       Level-1 LSPs sourced (new/refresh): 1/0
       Level-1 LSPs flooded (sent/rcvd): 0/0
            LSP Retransmissions: 0
       Level-1 CSNPs (sent/rcvd): 0/0
       Level-1 PSNPs (sent/rcvd): 0/0
       Level-1 DR Elections: 0
       Level-1 SPF Calculations: 1
       Level-1 Partial Route Calculations: 0
       LSP checksum errors received: 0
Trace:  Rcvd 0 requests, 0 replies
        Sent 0 requests, 0 replies
```

Table 23 describes the fields shown in the display.

Table 23 show ipx traffic Field Descriptions

Field	Description
Time since last clear	Elapsed time since last **clear** command issued.
Rcvd:	Description of the packets received.
total	Total number of packets received.
format errors	Number of bad packets discarded (for example, packets with a corrupted header). Includes IPX packets received in an encapsulation that this interface is not configured for.
checksum errors	Number of packets containing a checksum error. This number should always be 0, because IPX rarely uses a checksum.
bad hop count	Number of packets discarded because their hop count exceeded 16.
packets pitched	Number of times the device received its own broadcast packet.
local destination	Number of packets sent to the local broadcast address or specifically to the router.
multicast	Number of packets received that were addressed to an IPX multicast address.
Bcast:	Description of broadcast packets the router received and sent.
received	Number of broadcast packets received.
sent	Number of broadcast packets sent, including those the router is either forwarding or has generated.
Sent:	Description of packets the software generated and sent and those the software received and routed to other destinations.
generated	Number of packets sent that the router generated itself.
forwarded	Number of packets sent that the router forwarded from other sources.
encapsulation failed	Number of packets the software was unable to encapsulate.
no route	Number of times the software could not locate a route to the destination in the routing table.
SAP:	Description of the Service Advertising Protocol (SAP) packets sent and received.
Total SAP requests	Cumulative sum of SAP requests received: • SAP general requests • SAP Get Nearest Server (GNS) requests
Total SAP replies	Cumulative sum of all SAP reply types: General, Get Nearest Server, Nearest Name, and General Name.
servers	Number of servers in the SAP table.
SAP General Requests, received, sent, ignored, replies	Number of general SAP requests, sent requests, ignored requests, and replies. This field applies to Cisco IOS Release 11.2 and later.
SAP Get Nearest Server, requests, replies	Number of GNS requests and replies. This field applies to Cisco IOS Release 11.2 and later.

Table 23 show ipx traffic Field Descriptions (continued)

Field	Description
SAP Nearest Name requests, replies	Number of SAP Nearest Name requests and replies. This field applies to Cisco IOS Release 11.2 and later.
SAP advertisements received and sent	Number of SAP advertisements generated and then sent as a result of a change to the routing or service tables.
Throttled	Number of SAP advertisements discarded because they exceeded buffer capacity.
SAP flash updates sent	Number of SAP flash updates generated and sent because of changes to routing or service tables.
SAP format errors	Number of incorrectly formatted SAP advertisements received.
RIP:	Description of the Routing Information Protocol (RIP) packets received and sent.
RIP requests	Number of RIP requests received.
ignored	Number of RIP requests ignored.
RIP replies	Number of RIP replies sent in response to RIP requests.
routes	Number of RIP routes in the current routing table.
RIP advertisements received	Number of RIP advertisements received from another router.
sent	Number of RIP advertisements generated and then sent.
Throttled	Number of RIP advertisements discarded because they exceeded buffer capacity.
RIP flash updates sent atlr sent	Number of RIP flash updates generated and sent and number of advertisements to lost routes sent because of changes to the routing table.
RIP general requests sent	Number of RIP general requests generated and then sent.
RIP format errors	Number of incorrectly formatted RIP packets received.
Echo:	Description of the ping replies and requests received and sent.
Rcvd requests, replies	Number of ping requests and replies received.
Sent requests, replies	Number of ping requests and replies sent.
unknown	Number of unsupported packets received on socket.
no socket, filtered, no helper	Number of packets that could not be forwarded because helper addresses were improperly configured.
SAPs throttled	Number of SAP packets discarded because they exceeded buffer capacity.
freed NDB len	Number of Network Descriptor Blocks removed from the network but still needing to be removed from the routing table of the router.
Watchdog:	Description of the watchdog packets the software handled.
packets received	Number of watchdog packets received from IPX servers on the local network.
replies spoofed	Number of times the software responded to a watchdog packet on behalf of the remote client.

Table 23 show ipx traffic Field Descriptions (continued)

Field	Description
Queue lengths	Description of outgoing packets currently in buffers waiting to be processed.
IPX input	Number of incoming packets waiting to be processed.
SAP	Number of outgoing SAP packets waiting to be processed.
RIP	Number of outgoing RIP packets waiting to be processed.
GNS	Number of outgoing GNS packets waiting to be processed.
SAP throttling length	Maximum number of outgoing SAP packets allowed in the buffer. Additional packets received are discarded.
nets pending lost reply route	Number of "downed" routes being processed by the Lost Route Algorithm.
EIGRP: Total received, sent	Description of the Enhanced Interior Gateway Protocol (IGRP) packets the router received and sent.
Updates received, sent	Number of Enhanced IGRP updates received and sent.
Queries received, sent	Number of Enhanced IGRP queries received and sent.
Replies received, sent	Number of Enhanced IGRP replies received and sent.
SAPs received, sent	Number of SAP packets received from and sent to Enhanced IGRP neighbors.
NLSP:	Description of the NetWare Link Services Protocol (NLSP) packets the router sent and received.
Time since last clear	Elapsed time since last **clear** command issued.
Level-1 Hellos (sent/rcvd)	Number of LAN hello packets sent and received.
PTP Hellos (sent/rcvd)	Number of point-to-point Hello packets sent and received.
Level-1 LSPs sourced (new/refresh)	Number of local link-state packets (LSPs) created/refreshed by this router.
Level 1-LSPs flooded (sent/rcvd)	Number of LSPs sent and received by this router.
LSP Retransmissions	Number of LSPs resent by this router.
Level-1 CSNPs (sent/rcvd)	Number of complete sequence number PDU (CSNP) packets sent and received.
Level-1 PSNPs (sent/rcvd)	Number of partial sequence number PDU (PSNP) packets sent and received.
Level-1 DR Elections	Number of times the software calculated its designated router election priority.
Level-1 SPF Calculations	Number of times the software performed the shortest path first (SPF) calculation.
Level-1 Partial Route Calculations	Number of times the software recalculated routes without running SPF.
LSP Checksum errors received	Number of LSPs rejected because of checksum errors.

Table 23 show ipx traffic Field Descriptions (continued)

Field	Description
Trace:	Description of the trace packets the router received and sent.
RCvd requests, replies	Number of trace requests and replies received.
Sent requests, replies	Number of trace requests and replies sent.

Related Commands

Command	Description
clear ipx traffic	Clears IPX protocol and NLSP traffic counters.

show sse summary

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **show sse summary** command is not supported in Cisco IOS software.

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** command in EXEC mode.

show sse summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Examples

The following is sample output from the **show sse summary** command:

```
Router# show sse summary

SSE utilization statistics

                Program words  Rewrite bytes  Internal nodes  Depth
Overhead                  499              1               8
IP                          0              0               0      0
IPX                         0              0               0      0
SRB                         0              0               0      0
CLNP                        0              0               0      0
IP access lists             0              0               0
Total used                499              1               8
Total free              65037         262143
Total available         65536         262144

Free program memory
  [499..65535]
Free rewrite memory
```

```
  [1..262143]

Internals
  75032 internal nodes allocated, 75024 freed
  SSE manager process enabled, microcode enabled, 0 hangs
  Longest cache computation 4ms, longest quantum 160ms at 0x53AC8
```

spf-interval

Note Effective with Cisco IOS Release 15.1(3)S, XE 3.4, and 15.2(2)T, the **spf-interval** command is not supported in Cisco IOS software.

To customize Intermediate System-to-Intermediate System (IS-IS) throttling of shortest path first (SPF) calculations, use the **spf-interval** command in router configuration mode. To restore default values, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

no spf-interval

Syntax Description

level-1	(Optional) Apply intervals to Level-1 areas only.
level-2	(Optional) Apply intervals to Level-2 areas only.
spf-max-wait	Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.
spf-initial-wait	(Optional) Indicates the initial SPF calculation delay (in milliseconds) after a topology change. The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).
spf-second-wait	(Optional) Indicates the hold time between the first and second SPF calculation (in milliseconds). The range is 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

Defaults

spf-max-wait: 10 seconds
spf-initial-wait: 5500 milliseconds
spf-second-wait: 5500 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.1	The **level-1** and **level-2** keywords were added; the *spf-max-wait*, *spf-initial-wait*, and *spf-second-wait* arguments were added. The default interval between SPF calculations was changed from 5 seconds to 10 seconds.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)S	This command was modified. Support was removed for the Novell IPX protocol.

Release	Modification
Cisco IOS XE Release 3.4	This command was modified. Support was removed for the Novell IPX protocol.
15.2(2)T	This command was modified. Support was removed for the Novell IPX protocol.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** command controls how often Cisco IOS software performs the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows down the rate of convergence.

The following description will help you determine whether to change the default values of this command:

- The *spf-initial-wait* argument indicates the initial wait time (in milliseconds) after a topology change before the first SPF calculation.
- The *spf-second-wait* argument indicates the interval (in milliseconds) between the first and second SPF calculation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *spf-max-wait* interval specified; the SPF calculations are throttled or slowed down after the initial and second intervals. Once the *spf-max-wait* interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the *spf-max-wait* interval, fast behavior is restored (the initial wait time).

SPF throttling is not a dampening mechanism; that is, SPF throttling does not prevent SPF calculations or mark any route, interface, or router as down. SPF throttling simply increases the intervals between SPF calculations.

Examples

The following example configures intervals for SPF calculations, partial route calculation (PRC), and link-state packet (LSP) generation:

```
router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100
```