show ipx cache

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.

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 51 describes the fields shown in the display.

Table 51 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

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.

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 52 describes the fields shown in the display.

Table 52 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.

Table 52 show ipx eigrp interfaces Field Descriptions (continued)

Field	Description
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

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

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

Syntax Description

servers	(Optional) Displays the server list advertised by each neighbor. This is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
autonomous-system-number	(Optional) Autonomous system number. It can be a number from 1 to 65,535.
interface	(Optional) Interface type and number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The following keyword and argument were added: • **regexp** • *name*

Examples

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

```
Router# show ipx eigrp neighbors

IPX EIGRP Neighbors for process 1
H   Address                 Interface   Hold    Uptime   SRTT   RTO  Q  Seq
                                        (sec)            (ms)       Cnt Num
0   200.0000.0c34.d83b        Et0/2      11     00:00:18   2    200  0  10
2 total IPX servers for this peer
Type      Name                    Address             Port  Hops
          4 server                2037.0000.0000.0001:0001  2
          4 server2               2037.0000.0000.0001:0001  2
1   200.0000.0c34.d83c        Et0/2      11     00:00:18   2    200  0  10
1 total IPX servers for this peer
Type      Name                    Address             Port  Hops
          4 server                2037.0000.0000.0001:0001  2
```

Table 53 describes the fields shown in the display.

Table 53 show ipx eigrp neighbors Field Descriptions

Field	Description
process 200	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.
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.
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.
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.
Type	Contains codes from the Codes field to indicates how service was learned.
Name	Name of server.
Address	Network address of server.
Port	Source socket number.

Related Commands

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

show ipx eigrp topology

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

show ipx eigrp topology [*network-number*]

Syntax Description

network-number	(Optional) IPX network number whose topology table entry is to be displayed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **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 54 describes the fields shown in the display.

Table 54 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 is sample output from the **show ipx eigrp topology** command when you specify an IPX network number:

```
Router# show ipx eigrp topology 160
```

```
IPX-EIGRP topology entry for 160
State is Passive, Query origin flag is 1, 1 Successor(s)
Routing Descriptor Blocks:
  Next hop is Connected (Ethernet0), from 0.0000.0000.0000
  Composite metric is (0/0), Send flag is 0x0, Route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
Next hop is 164.0000.0c00.8ea9 (Ethernet1), from 164.0000.0c00.8ea9
  Composite metric is (307200/281600), Send flag is 0x0, Route is External
  This is an ignored route
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 2000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
  External data:
    Originating router is 0000.0c00.8ea9
    External protocol is RIP, metric is 1, delay 2
    Administrator tag is 0 (0x00000000)
    Flag is 0x00000000
```

Table 55 describes the fields shown in the display.

Table 55 show ipx eigrp topology Field Descriptions—Specific Network

Field	Description
160	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.
Next hop is ...	Indicates how this destination was learned. It can be one of the following: • Connected—The destination is on a network directly connected to this router. • Redistributed—The destination was learned via RIP or another Enhanced IGRP process. • IPX host address—The destination was learned from that peer via this Enhanced IGRP process.
Ethernet0	Interface from which this information was learned.

Table 55 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 53. 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.

Related Commands

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

show ipx interface

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.

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 56 describes the fields shown in the display.

Table 56 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.
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.

Table 56 show ipx interface Field Descriptions (continued)

Field	Description
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.
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.

Table 56 show ipx interface Field Descriptions (continued)

Field	Description
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.
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).

Command	Description
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 nhrp

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.

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 57 describes the fields shown in the display.

Table 57 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.

Table 57 show ipx nhrp Field Descriptions (continued)

Field	Description
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

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.

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 58 describes the fields shown in the display.

Table 58 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.

Table 58 show ipx nhrp traffic Field Descriptions (continued)

Field	Description
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

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.

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 59 describes the fields shown in the display.

Table 59 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.

Table 59 show ipx nlsp database Field Descriptions (continued)

Field	Description
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.
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

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.

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 60 describes the fields shown in the display.

Table 60 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.
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

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.

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 61 describes the fields shown in the display.

Table 61 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.

Table 61 show ipx nlsp spf-log Field Descriptions (continued)

Field	Descriptions
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

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**

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 62 describes the fields shown in the display.

Table 62 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.
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 63 describes the additional fields shown in the display.

Table 63 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

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.

Examples

The following is sample output from the **show ipx servers** command when NLSP is enabled:

```
Router# show ipx servers

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

Table ordering is based on routing and server info

Type Name                      Net  Address          Port Route Hops Itf
N+   4 MERLIN1-VIA-E03         E03E03.0002.0004.0006:0451 4/03  4    Et0
N+   4 merlin                  E03E03.0002.0004.0006:0451 4/03  3    Et0
```

```
N+    4 merlin 123456789012345  E03E03.0002.0004.0006:0451 4/03  3    Et0
S     4 WIZARD1--VIA-E0         E0.0002.0004.0006:0451     none  2
N+    4 dtp-15-AB               E002.0002.0004.0006:0451   none  4    Et0
N+    4 dtp-15-ABC              E002.0002.0004.0006:0451   none  4    Et0
N+    4 dtp-15-ABCD             E002.0002.0004.0006:0451   none  4    Et0
N+    4 merlin                  E03E03.0002.0004.0006:0451 4/03  3    Et0
N+    4 dtp-15-ABC              E002.0002.0004.0006:0451   none  4    Et0
```

Table 64 describes the fields shown in the display.

Table 64 show ipx servers Field Descriptions

Field	Description
Codes:	Codes that define how the service was learned.
S - Static	Statically defined service via the **ipx sap** command.
P - Periodic	Service learned via a SAP update.
E - EIGRP	Service learned via Enhanced IGRP.
N - NLSP	Service learned via NLSP.
H- Holddown	Indicates that the entry is in holddown mode and is not reachable.
+ - detail	Indicates that multiple paths to the server exist. Use the **show ipx servers detailed** EXEC command to display more detailed information about the paths.
Type	Contains codes from the Codes field to indicates how service was learned.
Name	Name of server.
Net	Network on which the server is located.
Address	Network address of the server.
Port	Source socket number.
Route	Ticks/hops (from the routing table).
Hops	Hops (from the SAP protocol).
Itf	Interface through which to reach the server.

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, N - NLSP, 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
```

See Table 64 for **show ipx servers** field descriptions.

Note 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

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.

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 65 describes the fields shown in the display.

Table 65 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

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**

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 66 describes the fields shown in the display.

Table 66 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.

Table 66 show ipx traffic Field Descriptions (continued)

Field	Description
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.
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.

Table 66 show ipx traffic Field Descriptions (continued)

Field	Description
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.
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.

Table 66 show ipx traffic Field Descriptions (continued)

Field	Description
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.
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

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.

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

To control how often Cisco IOS software performs the Shortest Path First (SPF) calculation, use the **spf-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval *seconds*

no spf-interval *seconds*

Syntax Description

seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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 can perform 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.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
spf-interval 30
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
log-neighbor-changes	Enables the logging of changes in Enhanced IGRP neighbor adjacencies.
prc-interval	Controls the hold-down period between partial route calculations.