



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 router functionality.

Use the commands in this chapter to configure and monitor Novell IPX networks. For IPX configuration information and examples, refer to the "Configuring Novell IPX" chapter of the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*.



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)

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	
<i>access-list-number</i>	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.
<i>protocol</i>	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. Table 45 in the “Usage Guidelines” section lists some IPX protocol names and numbers.
<i>source-network</i>	(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.
<i>.source-node</i>	(Optional) Node on the <i>source-network</i> from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>source-network-mask</i>	(Optional) Mask to be applied to the <i>source-network</i> 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 <i>source-node-mask</i> argument.
<i>source-socket</i>	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. Table 46 in the “Usage Guidelines” section lists some IPX socket names and numbers.

<i>destination.network</i>	(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.
<i>.destination-node</i>	(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 (<i>xxx.xxxx.xxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network-mask.</i>	(Optional) Mask to be applied to the <i>destination-network</i> 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 <i>destination-node-mask</i> argument.
<i>destination-socket</i>	(Optional) Socket name or number (hexadecimal) to which the packet is being sent. Table 46 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 <i>time-range-name</i>	(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: <ul style="list-style-type: none"> time-range <i>time-range-name</i>

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 **ipx 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 45](#) lists some IPX protocol names and numbers. [Table 46](#) lists some IPX socket names and numbers. For additional information about IPX protocol numbers and socket numbers, contact Novell.

Table 45 *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 46 *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.
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.

Table 46 Some IPX Socket Names and Numbers (continued)

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
85BE	eigrp	IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP).
9001	nlsp	NetWare Link Services Protocol.
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.
	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.
	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 routers 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)

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	
<i>access-list-number</i>	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.
<i>source-network</i>	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.
<i>.source-node</i>	(Optional) Node on <i>source-network</i> from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to <i>source-node</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(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.
<i>.destination-node</i>	(Optional) Node on <i>destination-network</i> to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to <i>destination-node</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). 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.

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.
ipx 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 routers from which packets are accepted.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list (NLSP)

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		
<i>access-list-number</i>		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 router redistributes an aggregated route instead.
permit		Permits redistribution of explicit routes if the conditions are matched.
<i>network</i>		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.
<i>network-mask</i>		Specifies the portion of the network address that is common to all addresses in the route summary. The high-order bits of <i>network-mask</i> must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.
<i>interface</i>		(Optional) Interface on which the access list should be applied to incoming updates.
ticks <i>ticks</i>		(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count <i>area-count</i>		(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 <i>interface</i> argument was added.

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 router to redistribute an aggregated route instead of the explicit route. The access list also contains a “permit all” statement that instructs the router 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 router 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 router to filter aggregated routes from passing into the NLSP version 1.0 areas and to redistribute explicit routes instead.

**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 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 nlspl area1 enable

interface ethernet 2
 ipx network 2001

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

ipx router nlspl 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 nlspl 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.

Command	Description
prc-interval	Controls the hold-down period between partial route calculations.
redistribute (IPX)	Redistributes from one routing domain into another.

access-list (SAP filtering)

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	
<i>access-list-number</i>	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.
<i>network</i>	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.
<i>.node</i>	(Optional) Node specified on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>network-mask.node-mask</i>	(Optional) Mask to be applied to <i>network</i> and <i>node</i> . Place ones in the bit positions to be masked.
<i>service-type</i>	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. Table 47 in the “Usage Guidelines” section lists examples of service types.
<i>server-name</i>	(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.

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 47](#) 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 47 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
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 router.
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)

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 router 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

<i>address</i>	Network number prefix. This is a 32-bit hexadecimal number.
<i>mask</i>	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

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

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 routers 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 router.

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 FFFFFFFE0
```

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

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.

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 router 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.

```
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
```

```
Router# clear ipx accounting
```

```
Router# show ipx accounting
```

Source	Destination	Packets	Bytes
Accounting data age is 0			

```
Accounting data age is 0
```

```
Router# 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

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.

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

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
	11.1	This command was introduced.

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 nlspp neighbors

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

clear ipx nlspp [tag] neighbors

Syntax Description

<i>tag</i>	(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.

Usage Guidelines

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

When you specify an NLSP tag, the router clears all NLSP adjacencies discovered by 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.

Examples

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

```
clear ipx nlspp neighbors
```

The following example deletes the NLSP adjacencies for process area2:

```
clear ipx nlspp 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

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		
<i>network</i>		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.
<i>network-mask</i>		(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the <i>network</i> argument, it specifies the an NLSP route summary to clear. The high-order bits specified for the <i>network-mask</i> 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: <ul style="list-style-type: none"> • <i>network-mask</i> • default

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

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.
	<i>sap-type</i>	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.
	<i>sap-name</i>	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.

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

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.

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: <pre>clear ipx traffic</pre>
-----------------	--

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

deny (extended)

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

<i>protocol</i>	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.
<i>source-network</i>	(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.
<i>.source-node</i>	(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 (<i>xxxx.xxx.xxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxx.xxx</i>). Place ones in the bit positions you want to mask.
<i>source-network-mask.</i>	(Optional) Mask to be applied to the <i>source-network</i> 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 <i>source-node-mask</i> argument.
<i>source-socket</i>	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. You can also use the keyword all to match all sockets.

<i>destination-network</i>	(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.
<i>.destination-node</i>	(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 (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network-mask.</i>	(Optional) Mask to be applied to the <i>destination-network</i> 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 <i>destination-node-mask</i> argument.
<i>destination-socket</i>	(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 <i>time-range-name</i>	(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: <ul style="list-style-type: none"> time-range <i>time-range-name</i>

deny (extended)**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 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 access-list	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)

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

<i>network</i>	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.
<i>network-mask</i>	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 <i>network-mask</i> 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 <i>ticks</i>	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count <i>area-count</i>	(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.

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.

deny (NLSP)

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 fffffff0
 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)

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

<i>network</i>	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.
<i>.node</i>	(Optional) Node on <i>network</i> . This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>network-mask.node-mask</i>	(Optional) Mask to be applied to <i>network</i> and <i>node</i> . Place ones in the bit positions to be masked.
<i>service-type</i>	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
<i>server-name</i>	(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.

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 (SAP filtering)

```
deny 1234 4 MyServer
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
ipx 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)

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	
<i>source-network</i>	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.
<i>.source-node</i>	(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 (<i>xxxx.xxxx.xxxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(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.
<i>.destination-node</i>	(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 (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.

Defaults No access lists are defined.

Command Modes Access-list configuration

■ deny (standard)

Command History

Release	Modification
11.3	This command was introduced.

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.
ipx 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

To filter networks received in updates, use the **distribute-list in** command in router 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

<i>access-list-number</i>	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.
<i>name</i>	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.
<i>interface-name</i>	(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

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

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

To suppress networks from being advertised in updates, use the **distribute-list out** command in router 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

<i>access-list-number</i>	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.
<i>name</i>	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.
<i>interface-name</i>	(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.
	 <p>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 <i>interface-name</i> argument. If you do not specify an interface, the routers will not exchange any routes or SAPs with their neighbors.</p>
<i>routing-process</i>	(Optional) Name of a particular routing process as follows: <ul style="list-style-type: none"> • eigrp <i>autonomous-system-number</i> • rip • nlsp [<i>tag</i>]

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

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

distribute-sap-list in

To filter services received in updates, use the **distribute-sap-list in** command in router 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		
	<i>access-list-number</i>	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.
	<i>name</i>	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.
	<i>interface-name</i>	(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 Router configuration

Command History	Release	Modification
	11.1	This command was introduced.

Examples In the following example, the router 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 nlsr 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

To suppress services from being advertised in SAP updates, use the **distribute-sap-list out** command in router 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

<i>access-list-number</i>	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.
<i>name</i>	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.
<i>interface-name</i>	(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.
	 <p>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 <i>interface-name</i> argument. If you do not specify an interface, the routers will not exchange any routes or SAPs with their neighbors.</p>
<i>routing-process</i>	(Optional) Name of a particular routing process as follows: <ul style="list-style-type: none"> • eigrp <i>autonomous-system-number</i> • nlsp [<i>tag</i>] • rip

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.

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

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

<i>access-list-number</i>	Number of the access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, the value for the <i>access-list-number</i> argument is a number from 900 to 999.
<i>name</i>	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.

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 access-list	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

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.
<i>name</i>	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.

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.
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.
pre-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

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.

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 router 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 router.

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

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

<i>number</i>	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.
<i>mask</i>	Network mask.

Defaults

No filters are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The source and destination addresses of each IPX packet traversing the router 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

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	<i>threshold</i>	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.

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 router 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

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	<i>count</i>	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.

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)

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

<i>network</i>	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.

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 routers.

This command applies only to RIP. NLSP and Enhanced IGRP are not affected when you enable this command. They continue to advertise all routes that they know about.



Note

Not all routers recognize and support the default route. Use this command with caution if you are not sure if all routers 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
```

■ **ipx advertise-default-route-only (RIP)**

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

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.

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)

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	<i>interval</i>	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.

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: <code>ipx backup-server-query-interval 5</code>
-----------------	--

ipx bandwidth-percent eigrp

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	<i>as-number</i>	Autonomous system number.
	<i>percent</i>	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.

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

To enable the router 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.

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 router to fast switch IPX directed broadcast packets. This may be useful in certain broadcast-based applications that rely on helpering.

Note that the router 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 router to fast switch IPX directed broadcast packets:

```
ipx broadcast-fastswitching
```