



Novell IPX Commands

Novell Internet Packet Exchange (IPX) is derived from the Xerox Network Systems (XNS) Internet Datagram Protocol (IDP). One major difference between IPX and XNS 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 in 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>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. 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	All sockets, 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

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
```



Note

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

```
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)	
	deny (extended)	
	ipx access-group	
	ipx access-list	
	ipx input-network-filter	
	ipx output-network-filter	
	ipx router-filter	
	permit (IPX extended)	
	priority-list protocol	

access-list (IPX standard)

access-list

no

access-list *access-list-number* **deny permit** *source-network* *.source-node* *source-node-mask*
destination-network *.destination-node* *destination-node-mask*

no access-list *access-list-number* **deny permit**
source-network *.source-node* *source-node-mask* *destination-network* *.destination-node*
destination-node-mask

Syntax Description

access-list-number

deny

permit

source-network

.source-node

source-network

xxxx xxxx xxxx

source-node-mask

source-node

xxxx xxxx xxxx

destination-network

.destination-node

destination-network

xxxx xxxx xxxx

destination-node-mask

destination-node

xxxx xxxx xxxx

Defaults

Command Modes

Command History**Release****Modification**

Usage Guidelines**ipx access-group****access-list** *access-list-number***access-list** *access-list-number* **deny permit** *source-network*

Examples

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

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

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

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

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

Related Commands	Command	Description
	access-list (IPX extended)	
	deny (standard)	
	ipx access-group	
	ipx access-list	
	ipx input-network-filter	
	ipx output-network-filter	
	ipx router-filter	
	priority-list protocol	

access-list (NLSP)

access-list
no

access-list *access-list-number* **deny permit** *network network-mask interface* **ticks ticks**
area-count *area-count*

no access-list *access-list-number* **deny permit** *network network-mask interface* **ticks ticks**
area-count *area-count*

Syntax Description

access-list-number

deny

permit

network

network-mask

network-mask

interface

ticks ticks

area-count *area-count*

Defaults

Command Modes

Command History

Release

Modification

interface

Usage Guidelines

-

-

-

-



Note

Examples

```
ipx routing
ipx internal-network 2000

interface ethernet 1
 ipx network 1001
 ipx nlspl areal 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
```

■ access-list (NLSP)

Related Commands	Command	Description
	area-address (NLSP)	
	deny (NLSP)	
	ipx access-list	
	ipx nlsf enable	
	ipx router	
	permit (NLSP)	
	prc-interval	
	redistribute (IPX)	

access-list (SAP filtering)

access-list

no

access-list *access-list-number* **deny permit** *network .node network-mask.node-mask*
service-type server-name

no access-list *access-list-number* **deny permit** *network .node network-mask.node-mask*
service-type server-name

Syntax Description

access-list-number

deny

permit

network

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 00000AA, you can enter AA.

.node

(Optional) Node specified on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxx.xxx.xxx).

network-mask.node-mask

(Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.

service-type

(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.

Table 47 in the “Usage Guidelines” section lists examples of service types.

server-name

(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

Command Modes

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 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

no area-address

Syntax Description

Network number prefix. This is a 32-bit hexadecimal number.

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

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 [ ] neighbors
```

Syntax Description

(Optional) Names the NLSP process. The 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 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 [ mask ] | default | * }
```

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.

(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the `mask` argument, it specifies the an NLSP route summary to clear.

The high-order bits specified for the `mask` argument must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.

Deletes the default route from the routing table.

* Deletes all routes in the routing table.

EXEC

10.0 This command was introduced.

11.1 The following keyword and argument were added:

default

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.

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
```

show ipx route	Displays the contents of the IPX routing table.
-----------------------	---

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

clear ipx [nlsp] traffic

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

Privileged EXEC

12.0(1)T	This command was introduced.
----------	------------------------------

Use the **show ipx traffic since bootup** command to recall traffic statistics that have been previously cleared.

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

```

deny [ protocol ] [ network ] [ mask ] [ socket ] [ log ] [ time-range ]
[ packet ] [ network ] [ mask ] [ socket ] [ log ] [ time-range ]

no deny [ protocol ] [ network ] [ mask ] [ socket ] [ log ] [ time-range ]
[ packet ] [ network ] [ mask ] [ socket ] [ log ] [ time-range ]

```

Syntax Description

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.

(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.

(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 (. .).

(Optional) Mask to be applied to the argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (. .). Place ones in the bit positions you want to mask.

(Optional) Mask to be applied to the 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 argument.

(Optional) Socket name or number (hexadecimal) from which the packet is being sent. You can also use the keyword **all** to match all sockets.

	<p>(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.</p> <p>You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p>
	<p>(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 (. .).</p>
	<p>(Optional) Mask to be applied to the argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (. .). Place ones in the bit positions you want to mask.</p>
	<p>(Optional) Mask to be applied to the argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.</p> <p>The mask must immediately be followed by a period, which must in turn immediately be followed by the argument.</p>
	<p>(Optional) Socket name or number (hexadecimal) to which the packet is being sent.</p>
log	<p>(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).</p>
time-range	<p>(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.</p>

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 •

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 `deny-sp` that denies all SPX packets:

The following example provides a time range to deny access :

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 NLSP route aggregation access list, use the **deny** access-list command in configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

```
deny          [ticks      ] [area-count      ]
no deny      [ticks      ] [area-count      ]
```

Syntax Description

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.

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 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 (Optional) Metric assigned to the route summary. The default is 1 tick.

area-count (Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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

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

Examples

The following example from a configuration file defines the access list named _____ 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.

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

```
deny [ network ] [ node ] [ mask ] [ service ] [ server ]
no deny [ network ] [ node ] [ mask ] [ service ] [ server ]
```

Syntax Description

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.

(Optional) Node on . This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (. .).

(Optional) Mask to be applied to and . Place ones in the bit positions to be masked.

(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.

(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*

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

access-list (SAP filtering)

ipx access-group

ipx access-list

permit (SAP filtering)

show ipx access-list

deny
no

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*

source-network

.source-node

source-node-mask

xxxx xxxx xxxx

source-node

xxxx xxxx xxxx

destination-network

.destination-node

destination-node-mask

xxxx xxxx xxxx

destination-node

xxxx xxxx xxxx

ipx access-list

access-list

fred

ipx access-list standard fred
deny 5678 any
permit any

access-list (IPX standard)

ipx access-group

ipx access-list

prc-interval

show ipx access-list

distribute-list in

no

distribute-list *access-list-number name* **in** *interface-name*

no distribute-list *access-list-number name* **in** *interface-name*

access-list-number

name

in

interface-name

```
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
```

access-list (IPX standard)

access-list (NLSP)

deny (NLSP)

deny (standard)

distribute-list out (IPX)

ipx access-list

permit (NLSP)

pre-interval

redistribute (IPX)

distribute-list out

no

distribute-list *access-list-number name* **out** *interface-name routing-process*

no distribute-list *access-list-number name* **out** *interface-name routing-process*

access-list-number

name

out

interface-name



distribute-list out
ipx router eigrp

interface-name

routing-process

eigrp *autonomous-system-number*

rip

nlsp *tag*

distribute-list out

**distribute-list out
distribute-list out**

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

access-list (IPX standard)

access-list (NLSP)

deny (NLSP)

deny (standard)

distribute-list in (IPX)

ipx access-list

ipx router

permit (NLSP)

prc-interval

redistribute (IPX)

distribute-sap-list in
no

distribute-sap-list *access-list-number name* **in** *interface-name*

no distribute-sap-list *access-list-number name* **in** *interface-name*

access-list-number

name

interface-name

area1

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

access-list (SAP filtering)

deny (SAP filtering)

distribute-list out (IPX)

ipx access-list

permit (SAP filtering)

redistribute (IPX)

distribute-sap-list out

no

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*

access-list-number

name

interface-name



distribute-sap-list out
ipx router eigrp

interface-name

routing-process

eigrp *autonomous-system-number*

nlsp *tag*

rip

distribute-sap-list out

distribute-sap-list out
distribute-sap-list out

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

access-list (SAP filtering)

deny (SAP filtering)

distribute-sap-list in

ipx access-list

ipx router

permit (SAP filtering)

redistribute (IPX)

ipx access-group

no

ipx access-group *access-list-number* *name* **in out**

no ipx access-group *access-list-number* *name* **in out**

access-list-number

access-list-number

access-list-number

name

in

out

in

out

access-list

access-list

in

out

any

any

in out

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

in

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

in

no

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

access-list (IPX extended)

access-list (IPX standard)

deny (extended)

deny (standard)

ipx access-list

permit (IPX extended)

prc-interval

priority-list protocol

ipx access-list
no

ipx access-list standard extended sap summary *name*

no ipx access-list standard extended sap summary *name*

standard

extended

sap

summary

name

deny permit

standard extended sap summary ipx access-list



fred

access-list (IPX extended)

access-list (IPX standard)

access-list (NLSP)

access-list (SAP filtering)

deny (extended)

deny (NLSP)

deny (SAP filtering)

deny (standard)

permit (IPX extended)

permit (IPX standard)

permit (NLSP)

permit (SAP filtering)

prc-interval

show ipx access-list

ipx accounting
no

ipx accounting

no ipx accounting

clear ipx accounting

ipx accounting-list

ipx accounting-threshold

ipx accounting-transits

show ipx accounting

ipx accounting-list

no

ipx accounting-list *number mask*

no ipx accounting-list *number mask*

number

mask

ipx accounting-transits

clear ipx accounting

ipx accounting

ipx accounting-threshold

ipx accounting-transits

show ipx accounting

ipx accounting-transits
no

ipx accounting-transits *count*

no ipx accounting-transits

count

ipx accounting-list
ipx accounting-list

clear ipx accounting

ipx accounting-list

ipx accounting-threshold

show ipx accounting

ipx advertise-default-route-only (RIP)

Syntax Description

Defaults

Command Modes

Command History

Release	Modification
---------	--------------

Usage Guidelines



Note

Examples

Related Commands**Command****Description**

ipx advertise-to-lost-route

Syntax Description

Defaults

Command Modes

Command History

Release	Modification
---------	--------------

Usage Guidelines



Note

Examples

ipx backup-server-query-interval (EIGRP)

```
ipx backup-server-query-interval  
no
```

```
ipx backup-server-query-interval  
no ipx backup-server-query-interval
```

Syntax Description

Defaults

Command Modes

Command History

Usage Guidelines

Examples

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

ipx bandwidth-percent eigrp

Syntax Description

Defaults

Command Modes

Command History

Release	Modification
---------	--------------

Usage Guidelines

Examples

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

Related Commands

Command	Description
---------	-------------
