Command	Purpose
access-list *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination* [**log**] [**time-range** *time-range-name*]	Define an extended IP access list using an abbreviation for a source and source wildcard of *source* 0.0.0.0, and an abbreviation for a destination and destination wildcard of *destination* 0.0.0.0.
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] [**time-range** *time-range-name*]	Define a dynamic access list. For information about lock-and-key access, refer to the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Security Configuration Guide*.

For more information about configuring IP extended access lists, see the "Configuring IP Services" chapter in the *Network Protocols Configuration Guide, Part 1* and the "Access Control Lists: Overview and Guidelines" chapter in the *Security Configuration Guide*.

Create an IPX Extended Access List

To create an IPX named extended access list, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	**ipx access-list extended** *name*	Define an extended IPX access list using a name. (Generic routing and broadcast filters use this type of access list.)

periodic

To specify when a time range is in effect, use the **periodic** time-range configuration command. To remove the time limitation, use the **no** form of this command.

periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*
no periodic *days-of-the-week hh:mm* **to** [*days-of-the-week*] *hh:mm*

Syntax Description

days-of-the-week — The first occurrence of this argument is the starting day or days that the associated time range is in effect. The second occurrence is the ending day or days the associated statement is in effect.

This argument can be any single day or combinations of days: **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**. Other possible values are:

daily -- Monday through Sunday

weekdays -- Monday through Friday

weekend -- Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

hh:mm — The first occurrence of this argument is the starting *hours***:***minutes* that the associated time range is in effect. The second occurrence is the ending *hours***:***minutes* the associated statement is in effect.

The *hours***:***minutes* are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Default

The time range has no recurring time limit in it.

Command Mode

Time-range configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1).

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** command, which identifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week are the same as the start, they can be omitted.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** items are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The **time-range** *time-range-name* keyword and argument first appeared in Release 12.0(1).

You can use access lists to control the transmission of packets on an interface, control virtual terminal line access, and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match against the TCP source port, the type of service value, or the packet's precedence.

Note After a numbered access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific numbered access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of type of service (TOS) names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found by typing a **?** in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the "Usage Guidelines" section of the **access-list (extended)** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

IPX Commands

This section documents the revised commands related to time-based access lists. All other commands used with this feature are documented in the Cisco IOS Release 12.0 *Network Protocols Command Reference, Part 2* in the "IPX Commands" chapter.

- **access-list (IPX extended)**
- **deny (extended)**
- **ipx access-list**
- **permit (IPX extended)**

access-list (IPX extended)

To define an extended Novell IPX access list, use the extended version of the **access-list** global configuration command. 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-nodemask*]] [*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-nodemask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

access-list-number	Number of the access list. This is a number from 900 to 999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. Table 1 in the "Usage Guidelines" section lists some IPX protocol names and numbers.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

*source-network-mask***.**	(Optional) Mask to be applied to *source-network*. 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 *source-node-mask*.
source-node-mask	(Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-socket	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. Table 2 in the "Usage Guidelines" section lists some IPX socket names and numbers.
*destination***.***network*	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*destination-node*	(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-network-mask	(Optional) Mask to be applied to *destination-network*. 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 *destination-node-mask*.
destination-node-mask	(Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent. Table 2 in the "Usage Guidelines" section lists some IPX socket names and numbers.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.