



Time-Based Access Lists Using Time Ranges

Feature Summary

It is now possible to implement access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the **permit** or **deny** statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

Benefits

There are many possible benefits of time ranges, such as the following:

- The network administrator has more control over permitting or denying a user access to resources. These resources could be an application (identified by an IP address/mask pair and a port number), policy routing, or an on-demand link (identified as interesting traffic to the dialer).
- Network administrators can set time-based security policy, including:
 - Perimeter security using the Cisco IOS Firewall feature set or access lists
 - Data confidentiality with Cisco Encryption Technology or IPSEC
- Policy-based routing and queuing functions are enhanced.
- When provider access rates vary by time of day, it is possible to automatically reroute traffic cost effectively.
- Service providers can dynamically change a Committed Access Rate (CAR) configuration to support the Quality of Service (QOS) Service Level Agreements (SLAs) that are negotiated for certain times of day.
- Network administrators can control logging messages. Access list entries can log traffic at certain times of the day, but not constantly. Therefore, administrators can simply deny access without having to analyze many logs generated during peak hours.

Platforms

This feature is supported on all Cisco IOS platforms.

Configuration Tasks

Perform the following required tasks to implement time ranges:

- Define a Time Range
- Reference the Time Range

Note The time range relies on the router's system clock. For this feature to work the way you intend, you need a reliable clock source. It is recommended that you use Network Time Protocol (NTP) to synchronize the router clock.

Define a Time Range

To define a time range, use the following commands beginning in global configuration mode.

Step	Command	Purpose
1	time-range <i>time-range-name</i>	Identify the time-range by a meaningful name.
2	absolute [<i>start time date</i>] [<i>end time date</i>] and/or periodic <i>days-of-the-week hh:mm to</i> <i>[days-of-the-week] hh:mm</i>	In time-range configuration mode, specify when the function it will be applied to will be in effect. Specify some combination of these commands; multiple periodic statements are allowed; only one absolute statement is allowed.

Repeat these tasks if you have multiple items you want in effect at different times. For example, repeat the steps to include multiple **permit** or **deny** statements in an access list in effect at different times.

Reference the Time Range

In order for a time range to be applied, you must reference it by name in a feature that can implement time ranges. To reference the time range, perform one of the following tasks:

- Create an IP Extended Access List
- Create an IPX Extended Access List

Create an IP Extended Access List

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

Step	Command	Purpose
1	ip access-list extended <i>name</i>	Define an extended IP access list using a name.
2	{deny permit} <i>protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</i>	In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations. Specify a time range to restrict when the permit or deny statement is in effect.
	or	
	{deny permit} <i>protocol any any [log] [time-range time-range-name]</i>	Define an extended IP access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
	or	
	{deny permit} <i>protocol host source host destination [log] [time-range time-range-name]</i>	Define an extended IP access list using an abbreviation for a source and source wildcard of <i>source</i> 0.0.0.0, and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.
	or	
	dynamic <i>dynamic-name [timeout minutes]</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</i>	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 <i>Security Configuration Guide</i> .

To create an IP numbered extended access list, use one of the following commands in global configuration mode:

Command	Purpose
access-list <i>access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</i>	Define an extended IP access list number and the access conditions. Use the log keyword to get access list logging messages, including violations. Specify a time range to restrict when the permit or deny statement is in effect.
access-list <i>access-list-number {deny permit} protocol any any [log] [time-range time-range-name]</i>	Define an extended IP access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.

Command	Purpose
access-list <i>access-list-number</i> { deny permit } <i>protocol</i> host <i>source</i> host <i>destination</i> [log] [time-range <i>time-range-name</i>]	Define an extended IP access list using an abbreviation for a source and source wildcard of <i>source</i> 0.0.0.0, and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.
access-list <i>access-list-number</i> [dynamic <i>dynamic-name</i> [timeout <i>minutes</i>]] { deny permit } <i>protocol</i> <i>source</i> <i>source-wildcard</i> <i>destination</i> <i>destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log] [time-range <i>time-range-name</i>]	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 <i>Security Configuration Guide</i> .

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 <i>name</i>	Define an extended IPX access list using a name. (Generic routing and broadcast filters use this type of access list.)

Step	Command	Purpose
2	<pre>{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]</pre>	In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations. Specify a time range to restrict when the permit or deny statement is in effect.
	or	
	<pre>{deny permit} protocol [log] [time-range time-range-name]</pre>	Define an extended IPX access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
	or	
	<pre>{deny permit} protocol host source host destination [log] [time-range time-range-name]</pre>	Define an extended IPX access list using an abbreviation for a source and source wildcard of <i>source</i> 0.0.0.0, and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.
	or	
	<pre>dynamic dynamic-name [timeout minutes] {deny permit} protocol source-network [.destination-node] destination-node-mask] [.destination-node destination-network-mask.destination-node- mask] [log] [time-range time-range-name]</pre>	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 <i>Security Configuration Guide</i> .

To create an IPX numbered extended access list, use one or more of the following commands in global configuration mode:

Command	Purpose
<pre>access-list access-list-number {deny permit} source-network[.source-node[source-node-mask]] [destination-network[.destination-node destination-node-mask]]][time-range time-range-name]</pre>	Define an extended IPX access list number and the access conditions. (Generic, routing, and broadcast filters use this type of access list.) Specify a time range to restrict when the permit or deny statement is in effect.
<pre>access-list access-list-number {deny permit} protocol [source-network[.source-node source-network-mask.source-node-mask]] source-socket [destination-network [.destination-node destination-network-mask.destination-node-mask] destination-socket] [log] [time-range time-range-name]</pre>	Define an extended IPX access list using a number. (Generic, routing, and broadcast filters use this type of access list.) Use the log keyword to get access list logging messages, including violations. Specify a time range to restrict when the permit or deny statement is in effect.

Command	Purpose
access-list <i>access-list-number</i> { deny permit } <i>protocol</i> host <i>source</i> host <i>destination</i> [log] [time-range <i>time-range-name</i>]	Define an extended IPX access list using an abbreviation for a source and source wildcard of <i>source</i> 0.0.0.0, and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.

For more information about configuring IPX access lists, see the “Configuring Novell IPX” chapter in the *Network Protocols Configuration Guide, Part 2* and the “Access Control Lists: Overview and Guidelines” chapter in the *Security Configuration Guide*.

Use the Access List

After creating an access list, you must reference it to make it work. There are many ways to use an access list, such as the following:

- Apply it to a line or interface, as shown in the chapter “Configuring IP Services” in the *Network Protocols Configuration Guide, Part 1*.
- Apply it to a line or interface, as shown in the chapter “Configuring IPX” in the *Network Protocols Configuration Guide, Part 2*.
- Control policy routing, as shown in the chapter “Configuring IP Routing Protocol-Independent Features” in the *Network Protocols Configuration Guide, Part 1*.
- Control dialer functions, as shown in the *Dial Solutions Configuration Guide*.

Configuration Examples

This section contains the following configuration examples for time ranges for IP and IPX:

- IP Time Range Examples
- IPX Time Range Examples

IP Time Range Examples

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 am and 6:00 pm on IP. The example allows UDP traffic on Saturday and Sunday from noon to 8:00 pm only.

```
time-range no-http
  periodic weekdays 8:00 to 18:00
!
time-range udp-yes
  periodic weekend 12:00 to 20:00
!
ip access-list extended strict
  deny tcp any any eq http time-range no-http
  permit udp any any time-range udp-yes
!
interface ethernet 0
  ip access-group strict in
```

IPX Time Range Examples

The following example permits SPX traffic only on Monday through Friday between the hours of 8:00 am and 6:00 pm on IPX:

```
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
!
```

Command Reference

These sections document the new and modified time range and time-based access list commands:

- Time Range Commands
- IP Commands
- IPX Commands

Time Range Commands

This section documents the following new time range commands:

- **absolute**
- **periodic**
- **time-range**

absolute

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

```
absolute [start time date] [end time date]
no absolute
```

Syntax Description

start <i>time date</i>	(Optional) Absolute time and date that the associated permit or deny statement starts going into effect. The <i>time</i> is expressed in a 24-hour clock, in the form of <i>hours:minutes</i> . For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The <i>date</i> is expressed in the format <i>day month year</i> . The minimum start is 00:00 1 January 1993. If no start time and date are specified, the permit or deny statement is in effect immediately.
end <i>time date</i>	(Optional) Absolute time and date that the associated permit or deny statement is no longer in effect. Same <i>time</i> and <i>date</i> format as described for the start . The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the permit or deny statement is in effect indefinitely.

Default

There is no absolute time when the time range is in effect.

Command Mode

Time-range configuration

Usage Guidelines

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

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

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.

Note All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, the system clock should be synchronized. Use NTP or the hardware calendar to synchronize the clock. For more information, refer to the “Performing Basic System Management” chapter of the *Configuration Fundamentals Configuration Guide*.

Examples

The following example configures an access list named northeast, which references a time range named xyz. The access list and time range together permit traffic on Ethernet interface 0 starting at 12:00 noon on January 1, 2001 and going forever.

```
time-range xyz
  absolute start 12:00 1 January 2001
!
ip access-list extended northeast
  permit ip any any time-range xyz
!
interface ethernet 0
  ip access-group northeast in
```

The following example permits UDP traffic until noon on December 31, 2000. After that time, UDP traffic is no longer allowed out Ethernet interface 0.

```
time-range abc
  absolute end 12:00 31 December 2000
!
ip access-list extended northeast
  permit udp any any time-range abc
!
interface ethernet 0
  ip access-group northeast out
```

The following example permits UDP traffic out Ethernet interface 0 on weekends only, from 8:00 am on January 1, 1999 to 6:00 pm on December 31, 2001:

```
time-range test
```

```
absolute start 8:00 1 January 1999 end 18:00 31 December 2001
periodic weekends 00:00 to 23:59
!
ip access-list extended northeast
 permit udp any any time-range test
!
interface ethernet 0
 ip access-group northeast out
```

Related Commands

deny
deny (extended)
permit
permit (IPX extended)
time-range

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.

Note All time specifications are taken as local time. To ensure that the time range entries take effect at the desired times, you should synchronize the system clock, using NTP or the hardware calendar.

Here are some typical settings for your convenience:

If you want:	Configure this:
Monday through Friday, 8:00 am to 6:00 pm only	periodic weekday 8:00 to 18:00
Every day of the week, from 8:00 am to 6:00 pm only	periodic daily 8:00 to 18:00
Every minute from Monday 8:00 am to Friday 8:00 pm	periodic monday 8:00 to friday 20:00
All weekend, from Saturday morning through Sunday night	periodic weekend 00:00 to 23:59
Saturdays and Sundays, from noon to midnight.	periodic weekend 12:00 to 23:59

Examples

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 am and 6:00 pm:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays between the hours of 9:00 am and 5:00 pm:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
```

Related Commands

access-list (extended)
access-list (IPX extended)
deny
deny (extended)
permit
permit (IPX extended)
time-range

time-range

To specify when an access list or other feature is in effect, use the **time-range** global configuration command. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*
no time-range *time-range-name*

Syntax Description

time-range-name Name of a time range. The name cannot contain a space or quotation mark, and must begin with an alphabetic character.

Default

None

Command Mode

Global configuration

Usage Guidelines

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

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Currently, only IPX and IP extended access lists use the time-range feature. Multiple time ranges can occur in a single access list or other feature.

After the **time-range** command, use the **periodic** command, the **absolute** command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Note Note that the names for time-range entries and named access lists are different names. To avoid confusion, do not use the same name for both.

Example

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 am and 6:00 pm. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
  periodic weekdays 8:00 to 18:00
!
time-range udp-yes
  periodic weekend 12:00 to 24:00
!
ip access-list extended strict
  deny tcp any any eq http time-range no-http
  permit udp any any time-range udp-yes
!
interface ethernet 0
  ip access-group strict in
```

Related Commands

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

IP Commands

This section documents the revised commands related to time-based access lists for IP. All other commands used with this feature are documented in the Cisco IOS Release 12.0 *Network Protocols Command Reference, Part 1* in the “IP Services Commands” chapter.

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

access-list (extended)

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, use the **no** form of this command.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    protocol source source-wildcard destination destination-wildcard [precedence precedence]
    [tos tos] [log] [time-range time-range-name]
no access-list access-list-number
```

For Internet Control Message Protocol (ICMP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] |
    icmp-message] [precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For Internet Group Management Protocol (IGMP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    igmp source source-wildcard destination destination-wildcard [igmp-type]
    [precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For TCP, you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    tcp source source-wildcard [operator port [port]] destination destination-wildcard
    [operator port [port]] [established] [precedence precedence] [tos tos] [log] [time-range
    time-range-name]
```

For User Datagram Protocol (UDP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    udp source source-wildcard [operator port [port]] destination destination-wildcard
    [operator port [port]] [precedence precedence] [tos tos] [log] [time-range
    time-range-name]
```

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 100 to 199.
dynamic <i>dynamic-name</i>	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Security Configuration Guide</i> .

timeout <i>minutes</i>	(Optional) Specifies the absolute length of time (in minutes) that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Security Configuration Guide</i> .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the keyword ip . Some protocols allow further qualifiers described below.
<i>source</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

<i>destination-wildcard</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(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 <i>tos</i>	(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 section “Usage Guidelines.”
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section “Usage Guidelines.”
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section “Usage Guidelines.”
<i>operator</i>	(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port. If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names are listed in the section “Usage Guidelines.” TCP port names can only be used when filtering TCP. UDP port names are listed in the section “Usage Guidelines.” UDP port names can only be used when filtering UDP. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.

established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
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.

Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Mode

Global configuration

Usage Guidelines

The UDP form of this command first appeared in Cisco IOS Release 10.0. All other forms of the command, as well as the following arguments and keywords, first appeared in Cisco IOS Release 10.3:

source
source-wildcard
destination
destination-wildcard
precedence *precedence*
icmp-type
icmp-code
icmp-message
igmp-type
operator
port
established

The following keywords and arguments first appeared in Cisco IOS Release 11.1:

dynamic *dynamic-name*
timeout *minutes*

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**

- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

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**

The following is a list of UDP 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.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Examples

In the following example, serial interface 0 is part of a Class B network with the address 128.88.0.0, and the mail host's address is 128.88.1.2. The keyword **established** is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicate that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example also permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp
```

```
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. They are similar to the bitmasks that are used with normal access lists. Prefix/mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix/mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.108.0.0 255.255.0.0 but denies any more specific routes of 192.108.0.0 (including 192.108.0.0 255.255.255.0).

```
access-list 101 permit ip 192.108.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example permits 131.108.0/24 but denies 131.108/16 and all other subnets of 131.108.0.0.

```
access-list 101 permit ip 131.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example uses a time-range to deny HTTP traffic on Monday through Friday between the hours of 8:00 am and 6:00 pm:

```
time-range no-http
  periodic weekdays 8:00 to 18:00
!
access-list 101 deny tcp any any eq http time-range no-http
!
interface ethernet 0
  ip access-group 101 in
```

Related Commands

- access-class**
- access-list (standard)**
- clear access-temp**
- distribute-list in**
- distribute-list out**
- ip access-group**
- ip access-list**
- logging console**
- priority-list**
- queue-list**
- show access-lists**
- show ip access-list**
- time-range**

deny

To set conditions for a named IP access list, use the **deny** access-list configuration command. To remove a deny condition from an access list, use the **no** form of this command.

```
deny source [source-wildcard]
no deny source [source-wildcard]

deny protocol source source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log] [time-range time-range-name]
no deny protocol source source-wildcard destination destination-wildcard
```

For ICMP, you can also use the following syntax:

```
deny icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] |
icmp-message] [precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For IGMP, you can also use the following syntax:

```
deny igmp source source-wildcard destination destination-wildcard [igmp-type]
[precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For TCP, you can also use the following syntax:

```
deny tcp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [established] [precedence precedence] [tos tos] [log] [time-range
time-range-name]
```

For UDP, you can also use the following syntax:

```
deny udp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [precedence precedence] [tos tos] [log] [time-range
time-range-name]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(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 <i>tos</i>	(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.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.

<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the “Usage Guidelines” section of the access-list (extended) command.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (extended) command.
<i>operator</i>	(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port. If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the access-list (extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
time-range <i>time-range-name</i>	(Optional) Name of the time range that applies to this deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.

Default

There is no specific condition under which a packet is denied passing the named access list.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. The **time-range** keyword and argument first appeared in Release 12.0(1).

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** option allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **deny** statement is in effect.

Examples

The following example sets a deny condition for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example denies HTTP traffic on Monday through Friday between the hours of 8:00 am and 6:00 pm:

```
time-range no-http
periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
deny tcp any any eq http time-range no-http
!
interface ethernet 0
ip access-group strict in
```

Related Commands

- access-list (extended)**
- ip access-group**
- ip access-list**
- permit**
- show ip access-list**
- time-range**

permit

To set conditions for a named IP access list, use the **permit** access-list configuration command. To remove a condition from an access list, use the **no** form of this command.

```
permit source [source-wildcard]
no permit source [source-wildcard]

permit protocol source source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log] [time-range time-range-name]
no permit protocol source source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log] [time-range time-range-name]
```

For ICMP, you can also use the following syntax:

```
permit icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] |
icmp-message] [precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For IGMP, you can also use the following syntax:

```
permit igmp source source-wildcard destination destination-wildcard [igmp-type]
[precedence precedence] [tos tos] [log] [time-range time-range-name]
```

For TCP, you can also use the following syntax:

```
permit tcp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [established] [precedence precedence] [tos tos] [log] [time-range
time-range-name]
```

For UDP, you can also use the following syntax:

```
permit udp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [precedence precedence] [tos tos] [log] [time-range
time-range-name]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(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 <i>tos</i>	(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.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.

<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “Usage Guidelines” section of the access-list (extended) command.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (extended) command.
<i>operator</i>	(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port. If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port. The range operator requires two port numbers. All other operators require one port number.
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the access-list (extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
time-range <i>time-range-name</i>	(Optional) Name of the time range that applies to this permit statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.

Default

There are no specific conditions under which a packet passes the named access list.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. The **time-range** keyword and argument first appeared in Release 12.0(1).

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

The **time-range** option allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays between the hours of 9:00 am and 5:00 pm:

```
time-range testing
periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
permit tcp any any eq telnet time-range testing
!
interface ethernet 0
ip access-group legal in
```

Related Commands

deny
ip access-group
ip access-list
show ip access-list
time-range

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

<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 1 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 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 <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 (xxxx.xxxx.xxxx).

<i>source-network-mask.</i>	(Optional) Mask to be applied to <i>source-network</i>. 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 <i>source-node-mask</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>source-socket</i>	(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.
<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 <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-network-mask.</i>	(Optional) Mask to be applied to <i>destination-network</i>. 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 <i>destination-node-mask</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.
<i>destination-socket</i>	(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 <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.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **log** keyword first appeared in Cisco IOS Release 11.2.

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

Table 1 **Some IPX Protocol Names and Numbers**

IPX Protocol Number (Decimal)	IPX Protocol Name	Protocol (Packet Type)
-1	any	Wildcard; matches any packet type in 900 lists
0		Undefined; refer to the socket number to determine the packet type
1	rip	Routing Information Protocol (RIP)
4	sap	Service Advertising Protocol (SAP)
5	spx	Sequenced Packet Exchange (SPX)
17	ncp	NetWare Core Protocol (NCP)
20	netbios	IPX NetBIOS

Table 2 **Some IPX Socket Names and Numbers**

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
0	all	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

Table 2 Some IPX Socket Names and Numbers (continued)

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
455	netbios	Novell NetBIOS process
456	diagnostic	Novell diagnostic packet
457		Novell serialization socket
4000-7FFF		Dynamic sockets; used by workstations for interaction with file servers and other network servers
8000-FFFF		Sockets as assigned by Novell, Inc.
85BE	eigrp	IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)
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

- 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**

deny (extended)

To set conditions for a named IPX extended access list, use the **deny** access-list configuration command. 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 <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 (xxx.xxxx.xxx).
<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 (xxx.xxxx.xxx). Place ones in the bit positions you want to mask.
<i>source-network-mask.</i>	(Optional) Mask to be applied to <i>source-network</i>. 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 <i>source-node-mask</i>.
<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 <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.
<i>destination-network-mask.</i>	(Optional) Mask to be applied to <i>destination-network</i>. 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 <i>destination-node-mask</i>.
<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.

Default

No access lists are defined.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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

- access-list (IPX extended)**
- ipx access-group**
- ipx access-list**
- permit (IPX extended)**
- show ipx access-list**

ipx access-list

To define an IPX access list by name, use the **ipx access-list** global configuration command. 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*



Caution Named access lists will not be recognized by any software release prior to Cisco IOS Release 11.3.

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.

Default

There is no default named IPX access list.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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.

Named access lists are not compatible with Cisco IOS releases prior to 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

You can use the master indexes or search online to find documentation of related commands.

- access-list (IPX extended)**
- access-list (IPX standard)**
- access-list (NLSP route aggregation summarization)**
- access-list (SAP filtering)**
- deny (extended)**
- deny (NLSP route aggregation summarization)**
- deny (SAP filtering)**
- deny (standard)**
- permit (IPX extended)**
- permit (IPX standard)**
- permit (NLSP route aggregation summarization)**
- permit (SAP filtering)**
- show ipx access-list**

permit (IPX extended)

To set conditions for a named IPX extended access list, use the **permit** access-list configuration command. To remove a permit condition from an access list, use the **no** form of this command.

```
permit protocol [source-network][[.source-node] source-node-mask] | [.source-node
source-network-mask,source-node-mask]] [source-socket] [destination-network]
[[.destination-node] destination-node-mask] | [.destination-node
destination-network-mask,destination-nodemask]] [destination-socket] [log] [time-range
time-range-name]
```

```
no permit protocol [source-network][[.source-node] source-node-mask] | [.source-node
source-network-mask,source-node-mask]] [source-socket] [destination-network]
[[.destination-node] destination-node-mask] | [.destination-node
destination-network-mask,destination-nodemask]] [destination-socket] [log] [time-range
time-range-name]
```

Syntax Description

<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 word 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 <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 (xxx.xxxx.xxx).
<i>source-network-mask.</i>	(Optional) Mask to be applied to <i>source-network</i> . 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 <i>source-node-mask</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 (xxx.xxxx.xxx). Place ones in the bit positions you want to mask.
<i>source-socket</i>	Socket name or number (hexadecimal) from which the packet is being sent. You can also use the word 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 word 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 <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-network-mask.</i>	(Optional) Mask to be applied to <i>destination-network</i>. 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 <i>destination-node-mask</i>.
<i>destination-nodemask</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.
<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.

Default

There is no specific condition under which a packet passes the named access list.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX protocol names and numbers, and IPX socket names and numbers, see the **access-list (IPX extended)** command.

Examples

The following example creates an extended access list named *sal* that denies all SPX packets and permits all others:

```
ipx access-list extended sal
deny spx any all any all log
permit any
```

The following example provides a time range to permit access:

```
time-range no-spx
periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
permit spx any all any all time-range no spx
!
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (IPX extended)

deny (extended)

ipx access-group

ipx access-list

show ipx access-list

