Command Reference

This appendix provides a command reference for those Cisco IOS commands—or aspects of the commands—that are unique to Layer 3 switching. This appendix contains the following commands:

QoS Commands

qos switching

Use the **qos switching** command to enable quality of service (QoS) mapping on the device.

qos switching

Syntax Description

This command has no keywords or arguments.

Defaults

QoS mapping is enabled.

Command Modes

Device configuration

Examples

The following example shows how to enable QoS mapping using the **qos switching** configuration command:

```
Router# qos switching
```

Related Commands

qos mapping precedence

qos mapping precedence

Use the **qos mapping precedence** command to configure QoS mapping at the system or interface level. Use the **no** form of this command to set the QoS precedence back to the default value.

qos mapping [**source** *source-int*] [**destination** *dest-int*] **precedence** *value* **wrr-weight** *weight*

no qos mapping precedence

Syntax Description

source *source-int*	(Optional) Source interface from which you want to define a traffic precedence.
destination *dest-int*	(Optional) Destination interface to which you want to define a traffic precedence.
value	Precedence value (0 to 3) derived from the IP precedence field. The higher 2 bits of the IP precedence field is used.
wrr-weight *weight*	WRR-scheduling weight (1 to 15); this parameter specifies the weight assigned to traffic with the given precedence.

Defaults

The default WRR-weights for precedence values 0, 1, 2, 3 are 1, 2, 3, and 4, respectively.

Command Modes

Device configuration

Usage Guidelines

When a precedence value *n* is specified, it implicitly assigns the same WRR weight to the precedence *n + 1*.

Examples

The following example shows how to set the system-level QoS mapping using the **qos mapping precedence** configuration command:

```
Router(config)# qos mapping precedence 0 wrr-weight 4
```

Related Commands

qos switching

rate-limit

Use the **rate-limit** command to configure QoS rate limits on a per-physical port basis.

rate-limit input {*32000-100000000*} {*0-64000*}

rate-limit output {*32000-100000000*} {*0-64000*}

Syntax Description

input	Keyword that specifies limiting the input rate.
32000-100000000	Target bit rate in bits per second.
0-64000	Burst size in bytes.
output	Keyword that specifies limiting the output rate.

Command Modes

Device configuration

Usage Guidelines

Rate limiting is applied to the entire interface traffic and is not confined to IP layer3 traffic only. However, high priority traffic destined to the CPU, traffic originating from the CPU or traffic which is process switched by the CPU is not subjected to per-port rate limiting.

Examples

The following example shows how to configure input rate limiting with a target bit rate of 1000000 bits per second and a burst size of 1000:

```
Router(config-if)# rate-limit input 1000000 1000
Router(config-if)#
```

The following example shows how to configure output rate limiting with a target bit rate of 1000000 bits per second and a burst size of 1000:

```
Router(config-if)# rate-limit output 1000000 1000
Router(config-if)#
```

Related Commands

show run interface

show qos switching

Use the **show qos switching** command to show whether QoS mapping is enabled on the device.

show qos switching

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Examples

The following example shows how to display whether QoS mapping is enabled using the **show qos switching** command:

```
Router# show qos switching
QoS Based IP Switching enabled
```

Related Commands

show qos mapping

show qos mapping

Use the **show qos mapping** command to show the QoS mapping in effect at the system or destination interface level.

show qos mapping [**source** *source-int*] [**destination** *dest-int*]

Syntax Description

source *source-int*	(Optional) Source interface from which you want to display QoS mapping; optional.
destination *dest-int*	(Optional) Destination interface to which you want to display QoS mapping; optional.

Command Modes

Privileged EXEC

Examples

The following example shows how to display the system-level QoS mapping using the **show qos mapping** command:

```
Router# show qos mapping
Precedence WRR-Weight
     0       1
     1       2
     2       3
     3       4
```

Related Commands

qos switching

traffic-shape rate

Use the **traffic-shape rate** command to configure QoS traffic shaping at the interface level.

traffic-shape rate {*32000-100000000*} {*0-512000*}

Syntax Description

32000-100000000	Target bit rate in bits per second.
0-512000	Interval sustained burst size in bits.

Command Modes

Device configuration

Usage Guidelines

Shaping is applied to the entire interface output traffic and is not confined to IP layer3 traffic only. However, traffic originating from the CPU or process switched by the CPU is not subjected to per-port shaping.

Examples

The following example shows how to configure traffic shaping with a target bit rate of 1000000 bits per second and a burst size of 1000:

```
Router(config-if)# traffic-shape rate 1000000 1000
```

Related Commands

show run interface

SDM Commands

sdm access-list

Use the **sdm access-list** command to partition the ternary content addressable memory (TCAM) space for the access list region.

sdm access-list *num-entries*

Syntax Description

num-entries	Size expressed as the number of entries, in the range of 512 to 16384.

Command Modes

Global configuration

Usage Guidelines

The enhanced Gigabit Ethernet interface module supports TCAM sizes of 32K. The combined size of the protocol regions and access lists should not exceed your TCAM space. The default size of the access lists in a 32K TCAM is 512 entries. You can enter the **sdm access-list** command to partition the TCAM space for access lists.

Examples

The following example shows how to partition the TCAM space to 600 entries:

```
Router(config-if)# sdm access-list 600
Router(config-if)#
```

Related Commands

show sdm size

sdm autolearn

Use the **sdm autolearn** command to enable the Switching Database Manager (SDM) autolearn feature. Use the **no** form of this command to disable it.

sdm autolearn

no sdm autolearn

Syntax Description

This command has no keywords or arguments.

Defaults

SDM autolearn is enabled.

Command Modes

Global configuration

Usage Guidelines

When the SDM autolearn feature is enabled, SDM automatically saves mask-length distribution for the routing database. SDM then uses this mask-length distribution as the initial mask-length distribution, which takes effect during the next system reboot.

Examples

The following example shows how to enable autolearning on the SDM:

```
Router(config-if)# sdm autolearn
Router(config-if)#
```

sdm size

Use the **sdm size** command to configure the size of each protocol region in the SDM.

sdm size *region-name* {*num-entries* | **k-entries** *num-k-entries*}

Syntax Description

region-name	Name of the protocol region for which you want to configure the size. • **ipx-bvi-network** • **ip-adjacency** • **ipx-node** • **ip-prefix** • **ipx-network** • **ip-mcast** • **l2-switching** (MAC addresses) • **udp-flooding** • **access-list**
num-entries	Size expressed as the number of entries, in the range of 32 to 262144.
num-k-entries	When used with the keyword **k-entries**, specifies the size in multiples of 1024 entries.

Command Modes

Global configuration

Usage Guidelines

The combined size entered for all the protocol regions should not exceed 32K, which is the total TCAM size. The supported size can be displayed using the **show sdm size** command. The size of SDM is represented as the number of base entries. Each protocol region entry can occupy one or more TCAM entries. The combined size of all the protocol regions should be calculated in terms of the base entries. Table A-1 lists the number of TCAM entries needed for each protocol region.

Table A-1 Number of TCAM Entries Needed for Each Protocol Region

Protocol Region	TCAM Entries
ipx-bvi-network	1
ip-adjacency	1
ipx-node	2
ip-prefix	1
ipx-network	1
ip-mcast	2
l2-forwarding	2
upd-flooding	2
access-list	4

Because the ip-prefix region occupies one TCAM entry, the **sdm size ip-prefix k-entries 6** command configures 6K TCAM entries in the SDM for the ip-prefix region. Because each ipx-node entry occupies two TCAM entries, the **sdm size ipx-node k-entries 3** command configures 6K TCAM entries in the SDM for the ipx-node region.

Examples

The following example shows how to set the region to ipx-node and the number of entries to 32:

```
Router(config-if)# sdm size ipx-node 32
Router(config-if)#
```

Related Commands

show sdm size

show sdm size

Use the **show sdm size** command to display the TCAM size and the size of each protocol region. The size is shown as the number of entries.

show sdm size

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Examples

The following example shows how to display the **show sdm size** command output:

```
Router# show sdm size
Switching Database Region Sizes :
    IPX BVI Network     : 32      32-bit entries
    IP Adjacency        : 2048    32-bit entries
    IPX Node            : 2048    64-bit entries
    IP Prefix           : 8192    32-bit entries
    IPX Network         : 6144    32-bit entries
    IP Multicast        : 3072    64-bit entries
    MAC Addr            : 1024    64-bit entries
    Access List         : 512     128-bit entries
```

Related Commands

sdm size

IP Uplink Redirect Commands

ip uplink-redirect

Use the **ip uplink-redirect** command to enable the IP uplink redirect feature. Use the **no** form of this command to disable it.

ip uplink-redirect

Syntax Description

This command has no keywords or arguments.

Defaults

Show ip uplink-redirect is disabled.

Command Modes

Global configuration

Usage Guidelines

The IP uplink redirect feature is supported on the Catalyst 2948G-L3 only. IP uplink redirect enables traffic between Fast Ethernet interfaces to be switched through the Gigabit Ethernet interface. ACLs applied on the Gigabit Ethernet filter traffic switched between Fast Ethernet interfaces.

The network processor on the Fast Ethernet interface does not switch certain IP packets, for instance IP packets with options, which are CPU process switched. The CPU switches the packets based on the IOS routing table. When the redirect feature is enabled, the network processor switched packets and the CPU process switched packets between two hosts connected to different Fast Ethernet interfaces will take different paths. ACLs can block traffic between two Fast Ethernet interfaces allowing IP packets with options to go through because the packets will be routed by the CPU process and not redirected to the Gigabit Ethernet interface.

⚠ **Caution** If the upstream router has an alternate better path (than the path used by the Gigabit Ethernet interface) to the Fast Ethernet interfaces of the Catalyst 2948G-L3 switch router, it could result in routing loops.

Examples

The following example shows how to enable IP uplink redirect:

```
Router(config-if)# ip uplink redirect
Router(config-if)#
```

Related Commands

show ip uplink-redirect

show ip uplink-redirect

Use the **show ip uplink-redirect** command to display the running IP uplink redirect configuration.

show ip uplink-redirect

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Examples

The following is sample output from the **show ip uplink-redirect** command:

```
Router# show ip uplink-redirect

IP Uplink Redirect Configuration:

Running Configuration :no ip uplink-redirect
Configuration on next reload :ip uplink-redirect
Router#
```

Related Commands

ip uplink-redirect

IP Services Commands

access-list (IP standard)

Use the standard version of the **access-list** global configuration command to define a standard IP ACL. Use the **no** form of this command to remove a standard ACLs.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

no access-list *access-list-number*

Syntax Description

access-list-number	Number of an ACL; This number is a decimal from 1 to 99 or from 1300 to 1999.
deny	Keyword that denies access if the conditions are matched.
permit	Keyword that permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. You can use 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 source and source-wildcard of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. You can use 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 source and source-wildcard of 0.0.0.0 255.255.255.255.

Defaults

The ACL defaults to an implicit deny statement for everything. The ACL is always terminated by an implicit deny statement for everything.

Command Modes

Global configuration

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the ACL.

You can use ACLs to control the transmission of packets on an interface, control virtual terminal line access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all ACLs.

Use the **show ip access-list** EXEC command to display the contents of one ACL.

Examples

The following example of a standard ACL allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the ACL statements will be rejected.

```
Router(config)# access-list 1 permit 192.5.34.0  0.0.0.255
Router(config)# access-list 1 permit 128.88.0.0  0.0.255.255
Router(config)# access-list 1 permit 36.0.0.0  0.255.255.255
! (Note:all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. The following two configuration commands are identical in effect:

```
Router(config)# access-list 2 permit 36.48.0.3
Router(config)# access-list 2 permit 36.48.0.3  0.0.0.0
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP ACL.
ip access-group	Controls access to an interface.
show access-lists	Displays the contents of current IP and rate-limit ACLs.
show ip access-list	Displays the contents of all current IP ACLs.

access-list (IP extended)

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

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

access-list *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*]

Internet Group Management Protocol (IGMP)

access-list *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*]

TCP

access-list *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

User Datagram Protocol (UDP)

access-list *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

Syntax Description

access-list-number	Number of an access list. This number is a decimal from 100 to 199 or from 2000 to 2699.
deny	Keyword that denies access if the conditions are matched.
permit	Keyword that permits access if the conditions are matched.
protocol	Name or number of an IP protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, **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.
source	Number of the network or host from which the packet is being sent. You have 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. You have 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. You have 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. You have 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) Keyword and variable that specifies 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) Keyword and variable that specifies 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."
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 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.
icmp-message	(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 section "Usage Guidelines."
igmp-type	(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."

operator	(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 *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) 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.

Defaults

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

Command Modes

Global configuration

Usage Guidelines

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to 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 an 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 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.

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

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

```
Router(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Router(config)# access-list 102 permit tcp any host 128.88.1.2 eq smtp
Router(config)# access-list 102 permit tcp any any eq domain
Router(config)# access-list 102 permit udp any any eq domain
Router(config)# access-list 102 permit icmp any any echo
Router(config)# 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 shows how to permit 192.108.0.0 255.255.0.0 but deny any more specific routes of 192.108.0.0 (including 192.108.0.0 255.255.255.0).

```
Router(config)# access-list 101 permit ip 192.108.0.0 0.0.0.0   255.255.0.0 0.0.0.0
Router(config)# access-list 101 deny ip 192.108.0.0 0.0.255.255  255.255.0.0 0.0.255.255
```

The following example shows how to permit 131.108.0/24 but deny 131.108/16 and all other subnets of 131.108.0.0.

```
Router(config)# access-list 101 permit ip 131.108.0.0 0.0.0.0     255.255.255.0 0.0.0.0
Router(config)# access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0   0.0.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
show access-list	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

deny (IP)

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

deny {*source* [*source-wildcard*] | **any**}

no deny {*source* [*source-wildcard*] | **any**}

deny *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]

no deny *protocol source source-wildcard destination destination-wildcard*

ICMP

deny icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*]

IGMP

deny igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*]

TCP

deny tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

UDP

deny udp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

Syntax Description

source	Number of the network or host from which the packet is being sent. YOu have 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. You have 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
protocol	Name or number of an IP protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, **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.

destination	Number of the network or host to which the packet is being sent. You have 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 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-wildcard	Wildcard bits to be applied to the destination. You have three alternative ways to specify the destination wildcard: • 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.
precedence *precedence*	(Optional) Keyword that specifies 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) Keyword and variable that specifies 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 (IP 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 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.
icmp-message	(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** (IP extended) command.
igmp-type	(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** (IP extended) command.
operator	(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 *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) 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** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.

Defaults

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

Command Modes

Access-list configuration

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions for a named IP access list.
show ip access-list	Displays the contents of all current IP access lists.

ip access-group

Use the **ip access-group** interface configuration command to control access to an interface. Use the **no** form of this command to remove the specified access group.

ip access-group {*access-list-number* | *name*}{**in** | **out**}

no ip access-group {*access-list-number* | *name*}{**in** | **out**}

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 199.
name	Name of an IP access list as specified by an ip access-list command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Usage Guidelines

For inbound ACLs, after receiving a packet, the microcode performs a source address lookup at the start of the ACL or a 5 tuple for an extended ACL in the TCAM containing the ACE's. If the ACL permits the address, the software continues to process the packet. If the ACL rejects the address, the software discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the microcode performs a source address lookup in a standard IP ACL or a 5 tuple lookup in an extended IP ACL in the TCAM containing ACE's. If the ACL permits the address, the software transmits the packet. If the ACL rejects the address, the software discards the packet.

When you apply an ACL that has not yet been defined to an interface, the software will act as if the ACL has not been applied to the interface and will accept all packets. Remember this behavior if you use undefined ACLs as a means of security in your network.

Note An ICMP Host Unreachable message is not sent to the Catalyst 2948G-L3 or 4908G-L3 switch routers when a packet is discarded due to a deny ACL.

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router(config)# interface ethernet 0
Router(config)# ip access-group 101 out
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of current IP and rate-limit access lists.

ip access-list

Use the **ip access-list** global configuration command to define an IP access list by name. Use the **no** form of this command to remove a named IP access lists.

ip access-list {**standard** | **extended**} *name*

no ip access-list {**standard** | **extended**} *name*

Syntax Description

standard	Keyword that specifies a standard IP access list.
extended	Keyword that specifies an extended IP access list.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No named IP access list is defined.

Command Modes

Global configuration

Usage Guidelines

Use this command to configure a named IP access list as opposed to a numbered IP 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 or extended with the **ip access-list** command determines the prompt you get when you enter access-list configuration mode.

Use the **ip access-group** command to apply the access-list to an interface.

Examples

The following example defines a standard access list named Internetfilter:

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

Related Commands

Command	Description
deny (IP)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
permit (IP)	Sets conditions for a named IP access list.
show ip access-list	Displays the contents of all current IP access lists.

permit (IP)

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

permit {*source* [*source-wildcard*] | **any**}

no permit {*source* [*source-wildcard*] | **any**}

permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]

no permit *protocol source source-wildcard destination destination-wildcard*

ICMP

permit icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*]

IGMP

permit igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*]

TCP

permit tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

UDP

permit udp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

Syntax Description

source	Number of the network or host from which the packet is being sent. You have 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. You have 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
protocol	Name or number of an IP protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, **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.

destination	Number of the network or host to which the packet is being sent. You have 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 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-wildcard	Wildcard bits to be applied to the destination. You have three alternative ways to specify the destination wildcard: • 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.
precedence *precedence*	(Optional) Keyword that specifies 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) Keyword and variable that specifies 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 (IP 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 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.
icmp-message	(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** (IP extended) command.
igmp-type	(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** (IP extended) command.
operator	(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 *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) 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** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.

Defaults

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

Command Modes

Access-list configuration

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
deny (IP)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
show ip access-list	Displays the contents of all current IP access lists.

show access-lists

Use the **show access-lists** privileged EXEC command to display the contents of current access lists.

show access-lists [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
name	(Optional) Name of the IP access list to display.

Defaults

The system displays all access lists.

Command Modes

Privileged EXEC

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101
Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches)
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches)
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
    deny   ip 192.150.42.0 0.0.0.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches.

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.

Command	Description
ip access-list	Defines an IP access list by name.
show ip access-list	Displays the contents of all current IP access lists.

show ip access-list

Use the **show ip access-list** EXEC command to display the contents of all current IP access lists.

show ip access-list [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
name	(Optional) Name of the IP access list to display.

Defaults

Displays all standard and extended IP access lists.

Command Modes

EXEC

Usage Guidelines

The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-list** command when all are requested:

```
Router# show ip access-list
Extended IP access list 101
   deny udp any any eq ntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter
Extended IP access list Internetfilter
    permit tcp any 171.69.0.0 0.0.255.255 eq telnet
    deny tcp any any
    deny udp any 171.69.0.0 0.0.255.255 lt 1024
    deny ip any any log
```

IPX Commands

access-list (IPX standard)

Use the standard version of the **access-list** global configuration command to define a standard IPX access list. Use the **no** form of this command to remove a standard access list.

access-list *access-list-number* {**deny** | **permit**} *source-network*
[*destination-network*[.*destination-node* [*destination-node-mask*]]]

no access-list *access-list-number* {**deny** | **permit**} *source-network*
[*destination-network*[.*destination-node* [*destination-node-mask*]]]

Syntax Description

access-list-number	Number of the access list. This is a number from 800 to 899.
deny	Keyword that denies access if the conditions are matched.
permit	Keyword that permits access if the conditions are matched.
source-network	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.
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-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.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Usage Guidelines

Standard IPX access lists filter on the source network. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface. The access list filters all outgoing packets on the interface.

To delete a standard access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the **no access-list** *access-list-number* command.

To delete the access list for a specific network, use the **no access-list** *access-list-number* {**deny** | **permit**} *source-network* command.

Examples

The following example denies access to traffic from all IPX networks (-1) to destination network 2:

```
Router(config)# access-list 800 deny -1 2
```

The following example denies access to all traffic from IPX address 1.0000.0c00.1111:

```
Router(config)# access-list 800 deny 1.0000.0c00.1111
```

The following example denies access from all nodes on network 1 that have a source address beginning with 0000.0c:

```
Router(config)# access-list 800 deny 1.0000.0c00.0000 0000.00ff.ffff
```

The following example denies access from source address 1111.1111.1111 on network 1 to destination address 2222.2222.2222 on network 2:

```
Router(config)# access-list 800 deny 1.1111.1111.1111 0000.0000.0000 2.2222.2222.2222 0000.0000.0000
```

or

```
Router(config)# access-list 800 deny 1.1111.1111.1111 2.2222.2222.2222
```

Related Commands

Command	Description
deny (standard)	Sets conditions for a named IPX access list.
ipx access-group	Applies generic input and output filters to an interface.

deny (standard)

Use the **deny** access-list configuration command to set conditions for a named IPX access list. Use the **no** form of this command to remove a deny condition from an access list.

deny *source-network* [*destination-network*[*.destination-node* [*destination-node-mask*]]]

no deny *source-network* [*destination-network*[*.destination-node* [*destination-node-mask*]]]

Syntax Description

source-network	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.
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-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.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Usage Guidelines

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

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples

The following example creates a standard access list named *fred*. It denies communication with only IPX network number 5678.

```
Router(config)# ipx access-list standard fred
Router(config)# deny 5678 any
Router(config)# permit any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
ipx access-group	Applies generic input and output filters to an interface.
show ipx access-list	Displays the contents of all current IPX access lists.

ipx access-group

Use the **ipx access-group** interface configuration command to apply generic input and output filters to an interface. Use the **no** form of this command to remove filters.

ipx access-group {*access-list-number* | *name*} [**in** | **out**]

no ipx access-group {*access-list-number* | *name*} [**in** | **out**]

Syntax Description

access-list-number	Number of the access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, *access-list-number* is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
in	(Optional) Keyword that filters inbound packets. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list.
out	(Optional) Keyword that filters outbound packets. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. This is the default when you do not specify an input (**in**) or output (**out**) keyword in the command line.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Usage Guidelines

Generic filters control which data packets an interface receives or sends out based on the packet's source and destination addresses, IPX protocol type, and source and destination socket numbers. You use the standard **access-list** and extended **access-list** commands to specify the filtering conditions.

You can apply only one input filter and one output filter per interface or subinterface.

When you do not specify an input (**in**) or output (**out**) filter in the command line, the default is an output filter.

Examples

The following example applies access list 801 to Gigabit interface 1. Because the command line does not specify an input filter or output filter with the keywords **in** or **out**, the software assumes that it is an output filter.

```
Router(config)# interface gigabit 1
Router(config)# ipx access-group 801
```

The following example applies access list 802 to Gigabit interface 1. The access list is an input filter access list as specified by the keyword **in**.

```
Router(config)# interface gigabit 1
Router(config)# ipx access-group 802 in
```

To remove the input access list filter in the previous example, you must specify the **in** keyword when you use the **no** form of the command. The following example correctly removes the access list:

```
Router(config)# interface gigabit 1
Router(config)# no ipx access-group 802 in
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
permit (IPX standard)	Sets conditions for a named IPX extended access list.

permit (IPX standard)

Use the **permit** access-list configuration command to set conditions for a named IPX access list. Use the **no** form of this command to remove a permit condition from an access list.

permit *source-network* [*destination-network*[.*destination-node*[*destination-node-mask*]]]

no permit *source-network* [*destination-network*[.*destination-node*[*destination-node-mask*]]]

Syntax Description

source-network	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.
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-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.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Usage Guidelines

Use this command following the **access-list** (IPX standard) command to specify conditions under which a packet passes the named access list.

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples

The following example creates a standard access list named *fred*. It permits communication with only IPX network number 5678.

```
Router(config)# ipx access-list standard fred
Router(config)# permit 5678 any
Router(config)# deny any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-group	Applies generic input and output filters to an interface.
show ipx access-list	Displays the contents of all current IPX access lists.

show ipx access-list

Use the **show ipx access-list** EXEC command to display the contents of all current IPX access lists.

show ipx access-list [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the IPX access list to display. This is a number from 800 to 899.
name	(Optional) Name of the IPX access list to display.

Defaults

Displays all standard, extended, SAP, and NLSP route aggregation summary IPX access lists.

Command Modes

EXEC

Usage Guidelines

The **show ipx access-list** command provides output identical to the **show access-lists** command, except that it is IPX specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ipx access-list** command when all access lists are requested:

```
Router# show ipx access-list
IPX extended access list 899
 deny any 1
IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

The following is sample output from the **show ipx access-list** command when the name of a specific access list is requested:

```
Router# show ipx access-list London
IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```