CHAPTER 5

Security Commands

This chapter describes the Cisco NX-OS security commands available on the switch.

aaa accounting default

To configure the authentication, authorization, and accounting (AAA) accounting feature to use the default accounting method for accounting services, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

aaa accounting default {**group** *server-group-list* | **local**}

no aaa accounting default {**group** *server-group-list* | **local**}

Syntax Description

group	Specifies that a server group be used for the accounting services.
server-group-list	Specifies a space-delimited list of RADIUS or TACACS+ server groups. The list can include the following: • **radius** for all configured RADIUS servers • **tacacs+** for all configured TACACS+ servers • Any configured RADIUS or TACACS+ server group name The server group list can be maximum 127 characters.
local	Specifies that the local database be used for accounting.

Command Default

The local database is the default.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The AAA accounting feature tracks the services that users are accessing and the network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server, or the local database, in the form of accounting records.

The **group** *server-group-list* method refers to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method, or the **local** method, or both and they fail, the accounting authentication fails.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch(config)# aaa accounting default group radius
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
aaa group server tacacs+	Configures TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa accounting	Displays AAA accounting status information.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

aaa authentication login console

To configure AAA authentication methods for console logins, use the **aaa authentication login console** command. To disable AAA authentication, use the **no** form of this command.

aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

Syntax Description

group	Specifies that a server group be used for authentication.
group-list	Specifies a space-delimited list of RADIUS or TACACS+ server groups that can include the following: • **radius** for all configured RADIUS servers • **tacacs+** for all configured TACACS+ servers • Any configured RADIUS or TACACS+ server group name
none	(Optional) Specifies that there is no authentication to get to the console access.
local	(Optional) Specifies that console access is authenticated by a local username and password.

Command Default

The local database.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **local** method, a username and password have to be configured in the local database of the switch. Local is the default and is used when no authentication methods are configured or when all the configured methods fail to respond.

If you specify the **group** method or **local** method and they fail, the authentication can fail. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

Examples

This example shows how to have console access authenticated using a server group:

```
switch(config)# aaa authentication login console group radius
```

This example shows how to have console access authenticated by a local username and password:

```
switch(config)# aaa authentication login console local
```

This example shows how to have no authentication:

```
switch(config)# aaa authentication login console none
```

This example shows how to disable console access authentication using a server group:

```
switch(config)# no aaa authentication login console group radius
```

Related Commands

Command	Description
aaa group server radius	Configures RADIUS server groups.
aaa group server tacacs+	Configures TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

aaa authentication login default

To configure the default AAA authentication methods, use the **aaa authentication login default** command. To disable AAA authentication, use the **no** form of this command.

aaa authentication login default {**group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

Syntax Description

group	Specifies that a server group be used for authentication.
group-list	Specifies a space-separated list of RADIUS or TACACS+ server groups that can include the following: • **radius** for all configured RADIUS servers • **tacacs+** for all configured TACACS+ servers • Any configured RADIUS or TACACS+ server group name
none	(Optional) Specifies that there is no authentication.
local	(Optional) Specifies that authentication is done using a local username and password.

Command Default

The local database.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **local** method, a username and password have to be configured in the local database of the switch. Local is the default and is used when no authentication methods are configured or when all the configured methods fail to respond.

If you specify the **group** method or **local** method and they fail, the authentication fails. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

Examples

This example shows how to configure default AAA authentication using a server group:

```
switch(config)# aaa authentication login default group radius
```

This example shows how to disable the default AAA authentication using a server group:

```
switch(config)# no aaa authentication login default group radius
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
aaa group server tacacs+	Configures AAA TACACS+ server groups.
radius-server host	Specifies a RADIUS server host.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.
tacacs-server host	Specifies a TACACS+ server host.

aaa authentication login error-enable

To configure a AAA authentication failure message to display on the console, use the **aaa authentication login error-enable** command. To disable the display of AAA authentication failure messages on the console, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

If none of the remote AAA servers respond when a user logs in, the authentication is processed by the local user database. If you have enabled the display, one of the following message is generated for the user:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

Examples

This example shows how to enable the display of AAA authentication failure messages to the console:

```
switch(config)# aaa authentication login error-enable
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
switch(config)# no aaa authentication login error-enable
```

Related Commands

Command	Description
show aaa authentication	Displays the status of the AAA authentication failure message display.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication at login, use the **aaa authentication login mschap enable** command. To disable MS-CHAP, use the **no** form of this command.

aaa authentication login mschap enable

no aaa authentication login mschap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable MS-CHAP authentication:

```
switch(config)# aaa authentication login mschap enable
```

This example shows how to disable MS-CHAP authentication:

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the status of MS-CHAP authentication.
show running-config aaa	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

aaa group server radius

To create a RADIUS server group and enter RADIUS server group configuration mode, use the **aaa group server radius** command. To remove a RADIUS server group from the configuration list, use the **no** form of this command.

aaa group server radius *server-group-name*

no aaa group server radius *server-group-name*

Syntax Description

server-group-name	RADIUS server group name. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch(config-radius)# no aaa group server radius RadServer
```

Related Commands

Command	Description
radius server host	Defines the IP address or hostname for a RADIUS server.
show aaa groups	Displays AAA server group information.
show radius-server	Displays RADIUS server information.

aaa group server tacacs+

To create a Terminal Access Controller Access Control System Plus (TACACS+) server group and enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

aaa group server tacacs+ *server-group-name*

no aaa group server tacacs+ *server-group-name*

Syntax Description

server-group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Before you can configure TACACS+ server groups, you must enable TACACS+ on the switch by using the **feature tacacs+** command. The commands for configuring TACACS+ server groups are not visible until you enable TACACS+.

Examples

This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)#
```

This example shows how to delete a TACACS+ server group:

```
switch(config-tacacs+)# no aaa group server tacacs+ TacServer
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show aaa groups	Displays AAA server group information.
show tacacs-server	Displays TACACS+ server information.
tacacs+ hostname	Defines the IP address or hostname for a TACACS+ server.

action

To specify what the switch does when a packet matches a **permit** command in a VLAN access control list (VACL), use the **action** command. To remove an **action** command, use the **no** form of this command.

action {**drop** | **forward** | **redirect ethernet** *slot*}

no action {**drop** | **forward** | **redirect ethernet** *slot*}

Syntax Description

drop	Specifies that the switch drops the packet.
forward	Specifies that the switch forwards the packet to its destination port.
redirect	Specifies that the switch redirect the packets to a specified interface.
ethernet	Specifies the Ethernet interface the packet should be forwarded to.
slot	Ethernet interface slot number and port number specified in the format 1/1.

Command Default

No default behavior or values.

Command Modes

Vlan access-map configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in the ACL specified by the **match** command.

Examples

This example creates a VLAN access map named vlan-map-01, assigns an IPv4 ACL named ip-acl-01 to the map, and specifies that the switch forwards packets matching the ACL:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)#
```

Related Commands

Command	Description
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

clear access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the switch clears. The name cannot contain a space, and can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear counters for all IPv4 ACLs:

```
switch# clear access-list counters
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
```

Related Commands

Command	Description
ip access-group	Applies an IPv4 ACL to an interface.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays information about one or all IPv4, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes for the interval. The range is from 0 to 1440 minutes. Setting the dead-time interval to 0 disables the timer.

Command Default

0 minutes.

Command Modes

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS.

Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.

Command	Description
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

deny (IPv4)

To create an IPv4 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of a protocol. The *protocol* argument can be one of the keywords **icmp**, **igmp**, **ip**, **tcp**, or **udp**, or an integer in the range from 0 to 255. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**.
icmp	Specifies that the rule applies only to ICMP traffic.
igmp	Specifies that the rule applies only to Internet Group Management Protocol (IGMP) traffic.
ip	Specifies that the rule applies to all IP traffic.
tcp	Specifies that the rule applies only to TCP traffic.
udp	Specifies that the rule applies only to UDP traffic.
source	Specifies the source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Specifies the destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
dscp *dscp*	(Optional) Matches the packets with the given 6-bit Differentiated Services Code Point (DSCP) value. See “DSCP Values” in the “Usage Guidelines” section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets. See “Precedence Values” in the “Usage Guidelines” section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets. The fragment is either permitted or denied accordingly. **Note** You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
icmp-message	(Optional; IGMP only) Rule matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.

igmp-message	(Optional; IGMP only) Rule matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace
operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument can be **eq** (Equal), **gt** (Greater Than), **lt** (Less Than), **neq** (Note Equal To), or **range** (range of port numbers).
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies the source or destination IP port object group name. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. **Note** Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule matches only packets that have a specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack**—Acknowledge the successful receipt of packets. • **fin**—(Finish) Close the TCP session. • **psh**—(Push) Forcefully deliver data without waiting for buffers to fill. • **rst**—Reset the connection to the remote host. • **syn**—Synchronize sequence numbers during TCP connections. • **urg**—Incoming packets marked as "urgent" are processed immediately.
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the switch assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

Ipv4 acl configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. The syntax is as follows:

  addrgroup *address-group-name*

  Note Use the **object-group ip address** command to create and change IPv4 address group objects.

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address network-wildcard

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address/prefix-len

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

DSCP Values

The *dscp* argument can be a number, which is an integer from 0 to 63 that is the decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.

The *dscp* argument can also be a keyword. Table 5-1 lists the DSCP values.

Table 5-1 DSCP Values

DSCP Value	Description
af11	Assured Forwarding (AF) class 1, low drop probability (001010)
af12	AF class 1, medium drop probability (001100)
af13	AF class 1, high drop probability (001110)
af21	AF class 2, low drop probability (010010)
af22	AF class 2, medium drop probability (010100)
af23	AF class 2, high drop probability (010110)
af31	AF class 3, low drop probability (011010)
af32	AF class 3, medium drop probability (011100)
af33	AF class 3, high drop probability (011110)
af41	AF class 4, low drop probability (100010)
af42	AF class 4, medium drop probability (100100)
af43	AF class 4, high drop probability (100110)
cs1	Class-selector (CS) 1, precedence 1 (001000)
cs2	CS2, precedence 2 (010000)
cs3	CS3, precedence 3 (011000)
cs4	CS4, precedence 4 (100000)
cs5	CS5, precedence 5 (101000)
cs6	CS6, precedence 6 (110000)
cs7	CS7, precedence 7 (111000)
default	Default DSCP value (000000)
ef	Expedited Forwarding (101110)

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also a keyword. Table 5-2 lists the ICMP message types.

Table 5-2 ICMP Message Types

ICMP Message	Description
administratively-prohibited	Administratively prohibited
alternate-address	Alternate address
conversion-error	Datagram conversion
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo (ping)
echo-reply	Echo reply

Table 5-2 ICMP Message Types (continued)

ICMP Message	Description
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for ToS
host-tos-unreachable	Host unreachable for ToS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Net redirect for ToS
net-tos-unreachable	Network unreachable for ToS
net-unreachable	Net unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence-unreachable	Precedence cutoff
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects
router-advertisement	Router discovery advertisements
router-solicitation	Router discovery solicitations
source-quench	Source quenches
source-route-failed	Source route failed
time-exceeded	All time-exceeded messages
timestamp-reply	Time-stamp replies
timestamp-request	Time-stamp requests
traceroute	Traceroute

Table 5-2 ICMP Message Types (continued)

ICMP Message	Description
ttl-exceeded	TTL exceeded
unreachable	All unreachables

Precedence Values

The *precedence* argument can be a number or a keyword. Table 5-3 lists the precedence keywords.

Table 5-3 Precedence Value

Precedence Value	Description
0–7	Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011.
critical	Precedence 5 (101)
flash	Precedence 3 (011)
flash-override	Precedence 4 (100)
immediate	Precedence 2 (010)
internet	Precedence 6 (110)
network	Precedence 7 (111)
priority	Precedence 1 (001)
routine	Precedence 0 (000)

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be a keyword. Table 5-4 lists the TCP port names.

Table 5-4 TCP Ports

TCP Port	Description
bgp	Border Gateway Protocol (179)
chargen	Character generator (19)
cmd	Remote commands (rcmd, 514)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name Service (53)
drip	Dynamic Routing Information Protocol (3949)
echo	Echo (7)
exec	EXEC (rsh, 512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (2)

Table 5-4 TCP Ports (continued)

TCP Port	Description
gopher	Gopher (7)
hostname	NIC hostname server (11)
ident	Ident Protocol (113)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
login	Login (rlogin, 513)
lpd	Printer service (515)
nntp	Network News Transport Protocol (119)
pim-auto-rp	PIM Auto-RP (496)
pop2	Post Office Protocol v2 (19)
pop3	Post Office Protocol v3 (11)
smtp	Simple Mail Transport Protocol (25)
sunrpc	Sun Remote Procedure Call (111)
tacacs	TAC Access Control System (49)
talk	Talk (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (54)
whois	WHOIS/NICNAME (43)
www	World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be a keyword. Table 5-5 lists the UDP ports.

Table 5-5 UDP Ports

UDP Port	Description
biff	Biff (mail notification, comsat, 512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
discard	Discard (9)
dnsix	DNSIX security protocol auditing (195)
domain	Domain Name System (DNS, 53)
echo	Echo (7)
isakmp	Internet Security Association and Key Management Protocol (5)
mobile-ip	Mobile IP registration (434)

Table 5-5 UDP Ports (continued)

UDP Port	Description
nameserver	IEN116 name service (obsolete, 42)
netbios-dgm	NetBIOS datagram service (138)
netbios-ns	NetBIOS name service (137)
netbios-ss	NetBIOS session service (139)
non500-isakmp	Internet Security Association and Key Management Protocol (45)
ntp	Network Time Protocol (123)
pim-auto-rp	PIM Auto-RP (496)
rip	Routing Information Protocol (router, in.routed, 52)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs	TAC Access Control System (49)
talk	Talk (517)
tftp	Trivial File Transfer Protocol (69)
time	Time (37)
who	Who service (rwho, 513)
xdmcp	X Display Manager Control Protocol (177)

Examples

This example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
```

This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.2.0 subnet:

```
switch(config-acl)# deny tcp 192.168.2.0 192.168.2.255 any
```

This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.2.0 subnet:

```
switch(config-acl)# deny udp 192.168.2.0/24 any
```

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.2.132 IPv4 address:

```
switch(config-acl)# deny icmp host 192.168.2.132 any
```

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 192.168.2.23 and 192.168.2.37 networks to the 192.168.0.0 network and a final rule that permits all other IPv4 traffic:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# deny udp 192.168.2.23/16 192.168.0.0/16
```

```
switch(config-acl)# deny tcp 192.168.2.37/16 192.168.0.0/16
switch(config-acl)# deny udp 192.168.2.37/16 192.168.0.0/16
switch(config-acl)# permit ip any any
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
object-group ip address	Configures an IPv4 address group object.
object-group ip port	Configures an IPv4 port group object.
remark	Configures a remark in an IPv4 or MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

deny (MAC)

To create a Media Access Control (MAC) access control list (ACL)+ rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*]

no deny *source destination* [*protocol*] [**cos** *cos-value*]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. Use the format EEEE.EEEE.EEEE. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
destination	Destination MAC addresses that the rule matches. Use the format EEEE.EEEE.EEEE. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see "MAC Protocols" in the "Usage Guidelines" section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.

Command Default

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the switch assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

Mac acl configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the switch applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  ```
  MAC-address MAC-mask
  ```

  The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  The following example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. Protocol numbers are a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—EtherType 0x6000 (0x6000)
- **etype-8042**—EtherType 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an IPv4 or MAC ACL.
show mac access-lists	Displays all MAC ACLs or one MAC ACL.

description (user role)

To add a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text string that describes the user role. The string can be maximum 128 characters.

Command Default

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

Examples

This example shows how to configure the description for a user role:

```
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

This example shows how to remove the description from a user role:

```
switch(config)# role name MyRole
switch(config-role)# no description
```

Related Commands

Command	Description
show role	Displays the user role configuration.

feature (role feature-group)

To configure a feature in a user role feature group, use the **feature** command. To delete a feature in a user role feature group, use the **no** form of this command.

feature *feature-name*

no feature *feature-name*

Syntax Description

feature-name	The switch feature name. The name has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

No default behavior or values.

Command Modes

User role feature group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the **show role feature** command to list the valid feature names to use in this command.

Examples

This example shows how to add features to a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

This example shows how to remove a feature from a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# no feature tacacs
```

Related Commands

Command	Description
role feature-group name	Creates or configures a user role feature group.
show role feature	Displays the user role features.
show role feature-group	Displays the user role feature groups.

interface policy deny

To configure the interface policy for a user role, and enter interface policy configuration mode for the user role, use the **interface policy deny** command. To revert to the default interface policy for a user role, use the **no** form of this command.

interface policy deny

no interface policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter interface policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

This example shows how to revert to the default interface policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

Related Commands

Command	Description
permit interface	Permits access to interfaces for a user role interface policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

ip access-list

To define an IPv4 access control list (ACL) and add rules to it or to enter IP access list configuration mode for a specific ACL, use the **ip access-list** command. To remove an IPv4 ACL, use the **no** form of this command.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv4 ACL. The name can be up to 64 characters long, and cannot contain a space or quotation mark.

Command Default

No IPv4 ACL is defined.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use IPv4 ACLs to filter IPv4 traffic.

When you use the **ip access-list** command, the switch enters IP access-list configuration mode, where you can use the IPv4 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

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

Every IPv4 ACL has the following implicit rule as its last rule:

```
deny ip any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

IPv4 ACLs do not include additional implicit rules to enable the neighbor discovery process. The Address Resolution Protocol (ARP) uses a separate data link layer protocol. By default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Examples

This example shows how to enter IP access list configuration mode for an IPv4 ACL named ip-acl-01:

```
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-group	Applies an IPv4 ACL to an interface.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

ip port access-group

To apply an IPv4 access control list (ACL) to an interface as a port ACL, use the **ip port access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters long.
in	Specifies that the ACL applies to inbound traffic.

Command Default

No IPv4 ACLs are applied to an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can use the **ip port access-group** command to apply an IPv4 ACL as a port ACL to the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 EtherChannel interfaces

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to Ethernet interface 1/2 as a port ACL, and display the configuration:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
switch(config-if)# show running-config interface ethernet 1/2
version 4.1(2)E1(1)

interface Ethernet1/2
  ip port access-group ip-acl-01 in
switch(config-if)#
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no ip port access-group ip-acl-01 in
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

mac access-list

To create a Media Access Control (MAC) access control list (ACL) or to enter MAC access list configuration mode for a specific ACL, use the **mac access-list** command. To remove a MAC ACL, use the **no** form of this command.

mac access-list *access-list-name*

no mac access-list *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL. The name cannot contain a space or quotation mark, and must be maximum 64 characters.

Command Default

No MAC ACLs are defined by default.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use MAC ACLs to filter non-IP traffic. If you disable packet classification, you can use MAC ACLs to filter all traffic.

When you use the **mac access-list** command, the switch enters MAC access list configuration mode, where you can use the MAC **deny** and **permit** commands to configure rules for the ACL. If the ACL specified does not exist, the switch creates it when you enter this command.

Use the **mac port access-group** command to apply the ACL to an interface.

Every MAC ACL has the following implicit rule as its last rule:

```
deny any any protocol
```

This implicit rule ensures that the switch denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

Examples

This example shows how to enter MAC access list configuration mode for a MAC ACL named mac-acl-01:

```
switch(config)# mac access-list mac-acl-01
switch(config-mac-acl)#
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac port access-group	Applies a MAC ACL to an interface.
permit (MAC)	Configures a permit rule in a MAC ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

mac port access-group

To apply a MAC access control list (ACL) to an interface, use the **mac port access-group** command. To remove a MAC ACL from an interface, use the **no** form of this command.

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL. The name is case-sensitive, and can be up to 64 alphanumeric characters.

Command Default

No MAC ACLs are applied to an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

MAC ACLs apply to non-IP traffic. If packet classification is disabled, MAC ACLs apply to all traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

- Layer 2 interfaces
- Layer 2 EtherChannel interfaces

You can also apply a MAC ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies MAC ACLs only to inbound traffic. When the switch applies a MAC ACL, the switch checks packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply a MAC ACL named mac-acl-01 to Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no mac port access-group mac-acl-01
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs.
show mac access-lists	Shows either a specific MAC ACL or all MAC ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

match

To specify an access control list (ACL) for traffic filtering in a VLAN access map, use the **match** command. To remove a **match** command from a VLAN access map, use the **no** form of this command.

match {**ip** | **mac**} **address** *access-list-name*

no match {**ip** | **mac**} **address** *access-list-name*

Syntax Description

ip	The specified ACL is an IPv4 ACL.
mac	The specified ACL is a MAC ACL.
address *access-list-name*	Specifies the ACL name. The name is case-sensitive and can be maximum 64 characters.

Command Default

By default, the switch classifies traffic and applies IPv4 ACLs to IPv4 traffic and MAC ACLs to all other traffic.

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can specify only one **match** command per access map.

Examples

This example creates a VLAN access map named vlan-map-01, and assigns an IPv4 ACL named ip-acl-01 to the map:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)#
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

object-group ip address

To create and change IPv4 address group objects, use the **object-group ip address** command. To remove an address group, use the **no** form of this command.

object-group ip address *obj-group-name*

no object-group ip address *obj-group-name*

Syntax Description

obj-group-name	Name of the IP address group object. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use this command to create IP address groups that you can use as the source or destination address in an IPv4 ACL configuration.

Examples

This example shows how to create an IP address group:

```
switch(config)# object-group ip address lab-gateway-svrs
switch(config)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.

object-group ip port

To create and change IPv4 port-group objects, use the **object-group ip address** command. To remove a port-group object, use the **no** form of this command.

object-group ip port *obj-group-name*

no object-group ip port *obj-group-name*

Syntax Description

obj-group-name	Name of the port-group object. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use this command to create IP port-groups that you can use as the source or destination port-group in an IPv4 ACL configuration.

Examples

This example shows how to create an port group object:

```
switch(config)# object-group ip port lab-gateway-port
switch(config)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.

permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **permit** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**]

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol. The *protocol* argument can be one of the keywords **icmp**, **igmp**, **ip**, **tcp**, or **udp**, or an integer in the range from 0 to 255. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**.
icmp	Specifies that the rule applies only to ICMP traffic.
igmp	Specifies that the rule applies only to Internet Group Management Protocol (IGMP) traffic.
ip	Specifies that the rule applies to all IPv4 traffic.
tcp	Specifies that the rule applies only to TCP traffic. Table 5-4 lists the TCP ports.
udp	Specifies that the rule applies only to UDP traffic. Table 5-5 lists the UDP ports.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
dscp *dscp*	(Optional) Matches the packets with the given 6-bit Differentiated Services Code Point (DSCP) value. Table 5-1 lists the DSCP values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets. Table 5-3 lists the precedence values that you can use to define the ACL.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets. The fragment is either permitted or denied accordingly. **Note** You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
icmp-message	(Optional; IGMP only) Rule matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed in Table 5-2.

igmp-message	(Optional; IGMP only) Rule matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace
operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument can be **eq** (Equal), **gt** (Greater Than), **lt** (Less Than), **neq** (Note Equal To), or **range** (range of port numbers).
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies the source or destination IP port object group name. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. **Note** Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule matches only packets that have a specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack**—Acknowledge the successful receipt of packets. • **fin**—(Finish) Close the TCP session. • **psh**—(Push) Forcefully deliver data without waiting for buffers to fill. • **rst**—Reset the connection to the remote host. • **syn**—Synchronize sequence numbers during TCP connections. • **urg**—Incoming packets marked as "urgent" are processed immediately.
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

Ipv4 acl configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. The syntax is as follows:

  addrgroup *address-group-name*

  Note Use the **object-group ip address** command to create and change IPv4 address group objects.

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address network-wildcard

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address/prefix-len

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

Examples

This example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
```

This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.2.0 subnet:

```
switch(config-acl)# permit tcp 192.168.2.0 192.0.2.255 any
```

This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.2.0 subnet:

```
switch(config-acl)# permit udp 192.168.2.0/24 any
```

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.2.132 IPv4 address:

```
switch(config-acl)# permit icmp host 192.168.2.132 any
```

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 192.168.2.23 and 192.168.2.37 networks to the 192.168.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# permit udp 192.168.2.23/16 192.168.0.0/16
switch(config-acl)# permit tcp 192.168.2.37/16 192.168.0.0/16
switch(config-acl)# permit udp 192.168.2.37/16 192.168.0.0/16
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.
object-group ip address	Configures an IPv4 address group object.
object-group ip port	Configures an IPv4 port group object.
remark	Configures a remark in an IPv4 or MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

permit (MAC)

To create a MAC ACL rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit** *source destination* [*protocol* [**cos** *cos-value* | **vlan** *vlan-id*]]

no permit *source destination* [*protocol* [**cos** *cos-value* | **vlan** *vlan-id*]]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. Use the format EEEE.EEEE.EEEE. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
destination	Destination MAC addresses that the rule matches. Use the format EEEE.EEEE.EEEE. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see "MAC Protocols" in the "Usage Guidelines" section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.
vlan *vlan-id*	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The *vlan-id* argument can be an integer from 1 to 4094.

Command Default

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the switch assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

Mac acl configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the switch applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

```
MAC-address MAC-mask
```

The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
```

The following example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

```
switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—Ethertype 0x6000 (0x6000)
- **etype-8042**—Ethertype 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-list	Configures a MAC ACL.
remark	Configures a remark in an IPv4 or MAC ACL.
show mac access-lists	Displays all MAC ACLs or one MAC ACL.

permit interface

To allow access to interfaces for a user role interface policy, use the **permit interface** command. To remove the allowed interfaces, use the **no** form of this command.

permit interface {**ethernet** *slot* | **port-channel** *number*}

no permit interface {**ethernet** *slot* | **port-channel** *number*}

Syntax Description

ethernet *slot*	Specifies the Ethernet interface slot number and port number in the format 1/1.
port-channel *number*	Specifies the EtherChannel number. Valid EtherChannel numbers are from 1 to 576.

Command Default

All interfaces.

Command Modes

Interface policy configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

For permit interface statements to work, you need to configure a command rule to allow interface access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

Examples

This example shows how to configure a range of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

This example shows how to configure an allowed list of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
```

This example shows how to remove an interface from a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
```

Related Commands

Command	Description
interface policy deny	Enters interface policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vlan

To specify the range of VLANs that the role can access, use the **permit vlan** command. To remove VLAN access, use the **no** form of this command.

permit vlan *vlan-list*

no permit vlan

Syntax Description

vlan-list	List of VLANs that the user role has permission to access.

Command Default

All VLANs.

Command Modes

Vlan policy configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

For **permit vlan** statements to work, you need to configure a command **rule** to allow VLAN access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

Examples

This example shows how to configure a range of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

This example shows how to configure a list of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

This example shows how to remove a VLAN from a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
vlan policy deny	Enters VLAN policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vrf

To specify the range of Virtual Private Network (VPN) routing and forwarding (VRF) instances the role can access, use the **permit vrf** command. To remove VRFs, use the **no** form of this command.

permit vrf *vrf-list*

no permit vrf

Syntax Description

vrf-list	List of VRFs that the user role has permission to access. The default VRFs include the following: • **chassis-management** • **default** • **management**

Command Default

All VRFs.

Command Modes

Vrf policy configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Use the **show vrf** command to display a list of VRFs in the system. You can also create VRFs using the **vrf context** command.

Examples

This example shows how to configure a range of VRFs for a user role VRF policy:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
switch(config-role-vrf)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
vrf policy deny	Enters vrf policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

Command	Description
show vrf	Displays the list of VRFs.
vrf context	Creates a VRF instance.

radius-server deadtime

To configure the global dead-time interval for all RADIUS servers on a switch, use the **radius-server deadtime** command. To restore the default dead-time interval of 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Command Default

0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the switch checks a RADIUS server that was previously unresponsive.

Note When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to specify five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

```
switch(config)# radius-server deadtime 5
```

This example shows how to revert to the default global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
switch(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To disable the directed-request feature, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

The **no radius-server directed-request** command causes the entire username string, both before and after the "@" symbol, to be passed to the default RADIUS server.

Examples

This example shows how to enable directed requests to a specific RADIUS server:

```
switch(config)# radius-server directed-request
```

This example shows how to disable directed requests to a specific RADIUS server:

```
switch(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server	Displays the directed request configuration in a RADIUS server.

radius-server host

To define a RADIUS server host to be used for authentication, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address*}
[**accounting [retransmit** *count* | **timeout** *seconds*]]
[**acct-port** *port-number*]
[**auth-port** *port-number*]
[**authentication** [**accounting** [**transmit** | **timeout** *seconds*]]]
[**key** {**0** | **7** | *key-value*}]
[**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address*}
[**accounting [retransmit** *count* | **timeout** *seconds*]]
[**acct-port** *port-number*]
[**auth-port** *port-number*]
[**authentication** [**accounting** [**transmit** | **timeout** *seconds*]]]
[**key** {**0** | **7** | *key-value*}]
[**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name System (DNS) name. The maximum length is 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
key	(Optional) Configures a preshared key for a single RADIUS server host. This preshared key is used instead of the global preshared key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
key-value	Configures a preshared key to authenticate communication between the RADIUS client and server. The maximum length is 63 characters.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.

idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The maximum size is 32 characters.
username *name*	Specifies a username in the test packets. The maximum size is 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the range is from 1 to 60 seconds.

Command Default

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: 0

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to specify host1 as the RADIUS server and use the default ports for both accounting and authentication:

```
switch(config)# radius-server host host1
```

This example shows how to specify port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
switch(config)# radius-server host host1 auth-port 1612 acct-port 1616
```

This example shows how to configure the host with IP address 192.168.2.1 as the RADIUS server, ports 2003 and 2004 as the authorization and accounting ports, enable accounting services on the RADIUS server, set the clear text and encrypted shared keys, set the idle time value to 10 minutes, and set the username and password for test packets on the RADIUS server:

```
switch(config)# radius-server host 192.168.2.1 key HostKey
switch(config)# radius-server host 192.168.2.1 auth-port 2003
```

```
switch(config)# radius-server host 192.168.2.1 acct-port 2004
switch(config)# radius-server host 192.168.2.1 accounting
switch(config)# radius-server host 192.168.2.1 key 0 MyKeyClr
switch(config)# radius-server host 192.168.2.1 key 7 MyKeyEnc
switch(config)# radius-server host 192.168.2.1 test idle-time 10
switch(config)# radius-server host 192.168.2.1 test username testuser
switch(config)# radius-server host 192.168.2.1 test password 2B9ka5
```

This example shows how to restore the default idle time for a specific RADIUS server:

```
switch(config)# no radius-server host 192.168.2.1 idle-time 10
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure the global secret key that is used by all RADIUS servers to authenticate with the switch, use the **radius-server key** command. To disable the global key, use the **no** form of this command.

radius-server key [**0** | **7**] *key-value*

no radius-server key [**0** | **7**] *key-value*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
key-value	Preshared key. The maximum length is 63 characters.

Command Default

Clear text authentication.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **radius-server host** command.

Examples

This example shows how to set the authentication key to AnyWord:

```
switch(config)# radius-server key AnyWord
```

This example shows how to set the authentication and encryption key to AnyWord. The 7 specifies that a hidden key will follow.

```
switch(config)# radius-server key 7 AnyWord
```

This example shows how to remove the encryption key from RADIUS authentication:

```
switch(config)# no radius-server key 7 AnyWord
```

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.
show radius-server	Displays RADIUS server information.

radius-server retransmit

To configure the maximum number of times for the switch to retry transmitting to a RADIUS server before reverting to local authentication, use the **radius-server retransmit** command. To restore the default configuration, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times.

Command Default

1 attempt.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The retransmit configuration is applied to all RADIUS servers.

Examples

This example shows how to specify a retransmit counter value of 3 times:

```
switch(config)# radius-server retransmit 3
```

This example shows how to restore the default retransmission count:

```
switch(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.
show radius-server	Displays RADIUS server information.

radius-server timeout

To configure the global timeout interval specifying how long to wait for a response from a RADIUS server before declaring a timeout failure, use the **radius-server timeout** command. To restore the default timeout value, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Command Default

1 second.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to how to set the interval timer to 30 seconds:

```
switch(config)# radius-server timeout 30
```

This example shows how to restore the default interval:

```
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

remark

To enter a comment into an IPv4 or MAC access control list (ACL), use the **remark** command. To remove a remark command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. The remark text can be up to 100 characters.

Command Default

No ACL contains a remark by default.

Command Modes

Ipv4 acl configuration

Mac acl configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the switch accepts the first 100 characters and drops any additional characters.

If you do not specify a sequence number, the switch adds the remark to the end of the ACL and assigns it a sequence number that is 10 greater than the sequence number of the preceding rule.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark This ACL denies the marketing department access to the lab
switch(config-acl)# show access-lists
```

This example shows how to remove a remark in an IPv4 ACL:

```
switch(config-acl)# no remark This ACL denies the marketing department access to the lab
switch(config-acl)#
```

This example shows how to remove a remark in an IPv4 ACL using only the sequence number:

```
switch(config-acl)# no 100
switch(config-acl)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.

resequence

To reassign sequence numbers to all rules in an access control list (ACL), use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **ip** • **mac**
access-list *access-list-name*	Specifies the name of the ACL. The name can be maximum 64 characters.
starting-number	Sequence number for the first rule in the ACL or time range.
increment	Number that the switch adds to each subsequent sequence number.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL. The new sequence number for the first rule is determined by the *starting-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp 128.0.0.0/16 any eq www
        10 permit udp 128.0.0.0/16 any
        13 permit icmp 128.0.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01
```

```
IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

role feature-group name

To create a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch(config)# no role feature-group name MyGroup
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
feature	Configures features in a user role feature group.
show role feature-group	Displays the user role feature groups.

role name

To create or specify a user role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name *role-name*

no role name *role-name*

Syntax Description

role-name	User role name. The *role-name* has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

A Cisco Nexus 4001I and Cisco Nexus 4005I switch provides the following default user roles:

- Network Administrator—Complete read-and-write access to the entire switch
- Complete read access to the entire switch

You cannot change or remove the default user roles.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to remove a user role:

```
switch(config-role)# no role name MyRole
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
interface policy deny	Configures the interface policy for the role.
show role	Displays the user roles.
username	Configures a user account.

Command	Description
vlan policy deny	Configures the VLAN policy for the role.
vrf policy deny	Configures the Virtual Private Network (VPN) routing and forwarding instance (VRF) policy for the role.

rule

To configure rules for a user role, use the **rule** command. To delete a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

Syntax Description

number	Sequence number for the rule. Valid values are 1 to 256. The switch applies the rule with the highest value first and then the rest in descending order.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string.
read	Specifies read access.
read-write	Specifies read and write access.
feature *feature-name*	(Optional) Configures a read-only or read-and-write rule for a feature. The feature name can be 32 characters. **Note** Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
feature-group *group-name*	(Optional) Configures a read-only or read-and-write rule for a feature group. The group name can be 32 characters. **Note** Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.

Command Default

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

To separate two or more commands in the *command-string*, press the **Space** key, and then press **;**. Example, config t ; role *.

Examples

This example shows how to add rules to a user role:

```
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to remove rule from a user role:

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
role feature-group name	Configures a user role feature group.
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.

server

To add a server to a RADIUS or TACACS+ server group, use the **server** command. To delete a server from a server group, use the **no** form of this command.

server {*ipv4-address* | *hostname*}

no server {*ipv4-address* | *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
hostname	Server name. The maximum length is 256 characters.

Command Default

No default behavior or values.

Command Modes

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter radius server group configuration mode or **aaa group server tacacs+** command to enter tacacs+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to add a server to a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.2.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.2.1
```

This example shows how to add a server to a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 192.168.2.2
```

This example shows how to delete a server from a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

show aaa accounting

To display AAA accounting configuration, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show aaa accounting** command and displays information about the AAA configuration:

```
switch# show aaa accounting
default: local
switch(config)#
```

Related Commands

Command	Description
aaa accounting default	Configures AAA methods for accounting.

show aaa authentication

To display AAA authentication configuration information, use the **show aaa authentication** command.

show aaa authentication login [**error-enable** | **mschap**]

Syntax Description

error-enable	(Optional) Displays the authentication login error message enable configuration. Displays the configuration information when authentication login error message is enabled.
mschap	(Optional) Displays the authentication login Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) enable configuration.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show aaa authentication** command and displays information about the configured authentication parameters:

```
switch# show aaa authentication
         default: local
         console: group TacServer
switch(config)#
```

The following is sample output from the **show aaa authentication login error-enable** command and displays information about the authentication login error enable configuration:

```
switch# show aaa authentication login error-enable
disabled
switch(config)#
```

The following is sample output from the **show aaa authentication login mschap** command and displays information about the authentication login MS-CHAP configuration:

```
switch# show aaa authentication login mschap
disabled
switch(config)#
```

Related Commands

Command	Description
aaa authentication login console	Configures AAA console login authentication.
aaa authentication login default	Configures AAA default login authentication.
aaa authentication login error-enable	Enables AAA authentication failure messages to display on the console.
aaa authentication login mschap enable	Enables MS-CHAP authentication for logging in to the AAA servers.

show aaa groups

To display AAA server group configuration, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable the TACACS+ feature on the switch by using the **feature tacacs+** command before you can display TACACS+ information.

Examples

The following is sample output from the **show aaa groups** command and displays information about the AAA groups:

```
switch# show aaa groups
radius
RadServer
tacacs
TacServer
switch#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server group information.
show tacacs-server	Displays TACACS+ server group information

show access-lists

To display all IPv4 and MAC access control lists (ACLs) or a specific ACL, use the **show access-lists** command.

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

Syntax Description

access-list-name	(Optional) Name of an ACL to show. The name can be maximum 64 characters.

Command Default

The switch shows all ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show access-lists** command and displays information about the IPv4 and MAC ACLs configured on the switch:

```
switch# show access-lists

MAC access list 01-mac-acl
        10 permit any any ip cos 3
        20 permit any any vlan 5
        30 permit 00c0.4f03.0a72 0000.0000.0000 any aarp
        40 permit any 0060.3e00.0000 0000.0000.0000 ip vlan 3
        50 deny any any vines-echo cos 1
MAC access list 02-mac-acl
        10 deny any any ip vlan 2
IP access list 01-myacl
        10 deny tcp 192.168.1.37/16 192.168.1.176/16
IP access list acl2
        10 permit tcp any any
IP access list ip-acl-01
        1 remark This ACL permits UDP traffic
        21 permit udp 192.168.2.3/3 192.168.2.116/3
        41 permit tcp 192.168.3.23/12 192.168.3.176/12
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.

Command	Description
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*] [**start-time** *year month day HH*:*MM*:*SS*] [**end-time** *year month day HH*:*MM*:*SS*]

Syntax Description

size	(Optional) The amount of the log to display in bytes. The range is from 0 to 250000.
start-time *year month day HH*:*MM*:*SS*	(Optional) Specifies a start time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.
end-time *year month day HH*:*MM*:*SS*	(Optional) Specifies an end time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show accounting log** command and displays information about the accounting log:

```
switch# show accounting log
```

The following is sample output from the **show accounting log 500** command and displays 500 bytes of the accounting log:

```
switch# show accounting log 500

Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
Wed Aug  5 06:10:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; r
adius-server host myRad test username testuser password testpwd idle-time 10 (SU
CCESS)
Wed Aug  5 06:10:39 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
switch#
```

The following is sample output from the **show accounting log start-time** command and displays information about the accounting log starting at 16:00:00 on August 5, 2009:

```
switch# show accounting log start-time 2009 Aug 5 06:00:00

Wed Aug  5 06:01:06 2009:update:192.168.2.168@pts/0:root:tacacs+ disabled
```

```
Wed Aug  5 06:01:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; n
o feature tacacs+ (SUCCESS)
Wed Aug  5 06:01:24 2009:update:192.168.2.168@pts/0:root:tacacs+ enabled
Wed Aug  5 06:01:24 2009:update:192.168.2.168@pts/0:root:configure terminal ; f
eature tacacs+ (SUCCESS)
Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:updated TACACS+ parame
ters for group:TacServer
Wed Aug  5 06:01:28 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
Wed Aug  5 06:10:06 2009:update:192.168.2.168@pts/0:root:configure terminal ; r
adius-server host myRad test username testuser password testpwd idle-time 10 (SU
CCESS)
Wed Aug  5 06:10:39 2009:update:192.168.2.168@pts/0:root:configure terminal ; a
aa group server tacacs+ TacServer (SUCCESS)
switch#
```

The following is sample output from the **show accounting log** command and displays information about the accounting log starting at 15:59:59 on August 3, 2009 and ending at 16:00:00 on August 5, 2009:

```
switch# show accounting log start-time 2009 Aug 3 15:59:59 end-time 2009 Aug 5 16:00:00
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

show interface counters storm-control

To view the storm-control levels set on the interface, use the **show interface counters** command.

show interface [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control**

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface slot number and port number.
port-channel *number*	(Optional) Specifies the EtherChannel interface number.

Command Default

Displays the storm-control levels of all interfaces.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show interface counters storm-control** command and displays information about the storm-control levels set on the interfaces:

```
switch# show interface counters storm-control

--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth1/1          100.00          100.00          100.00                     0
Eth1/2           30.00          100.00          100.00                     0
Eth1/3          100.00          100.00          100.00                     0
Eth1/4          100.00          100.00          100.00                     0
Eth1/5          100.00          100.00          100.00                     0
Eth1/6          100.00          100.00          100.00                     0
Eth1/7          100.00          100.00          100.00                     0
Eth1/8          100.00          100.00          100.00                     0
Eth1/9          100.00          100.00          100.00                     0
Eth1/10         100.00          100.00          100.00                     0
Eth1/11         100.00          100.00          100.00                     0
Eth1/12         100.00          100.00          100.00                     0
Eth1/13         100.00          100.00          100.00                     0
Eth1/14         100.00          100.00          100.00                     0
Eth1/15         100.00          100.00          100.00                     0
Eth1/16         100.00          100.00          100.00                     0
Eth1/17         100.00          100.00          100.00                     0
Eth1/18         100.00          100.00          100.00                     0
Eth1/19         100.00          100.00          100.00                     0
Eth1/20         100.00          100.00          100.00                     0
switch#
```

The following is sample output from the **show interface ethernet 1/2 counters storm-control** command and displays information about the storm-control levels set on Ethernet interface 1/2:

```
switch# show interface ethernet 1/2 counters storm-control
```

```
--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Eth1/2           30.00          100.00          100.00                      0

switch#
```

Related Commands

Command	Description
storm-control	Sets the storm-control threshold value and blocks forwarding of unnecessary flooded traffic.
show running-config	Displays the configuration of the interfaces.

show ip access-lists

To display all IPv4 ACLs or a specific IPv4 ACL, use the **show ip access-lists** command.

show ip access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an IPv4 ACL to show. The name can be maximum 64 characters.

Command Default

The switch shows all IPv4 ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show ip access-lists** command and displays information about the IPv4 ACLs configured on the switch:

```
switch# show ip access-lists

IP access list test
        10 permit ip 192.168.2.1/32 192.168.2.2/32

IP access list ip-acl-01
        10 permit ip 192.168.2.1/5 any
        20 permit tcp 192.168.2.23/16 192.168.2.176/16
        30 deny udp 192.168.3.25/12 192.168.3.27/15
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

show mac access-lists

To display all Media Access Control (MAC) access control lists (ACLs) or a specific MAC ACL, use the **show mac access-lists** command.

show mac access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of a MAC ACL to show. The name can be maximum 64 characters.

Command Default

The switch shows all MAC ACLs, unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show mac access-lists** command and displays information about the MAC ACLs configured on the switch:

```
switch# show mac access-lists

MAC access list 01-mac-acl
        10 permit any any ip cos 3
        20 permit any any vlan 5
        30 permit 00c0.4f03.0a72 0000.0000.0000 any aarp
        40 permit any 0060.3e00.0000 0000.0000.0000 ip vlan 3
        50 deny any any vines-echo cos 1
MAC access list 02-mac-acl
        10 deny any any ip vlan 2
switch#
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [{*hostname* | *ipv4-address*} | **directed-request** | **groups** [*group-name*] | **sorted** | **statistics** {*hostname* | *ipv4-address*}]

Syntax Description

hostname	(Optional) RADIUS server Domain Name System (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A.B.C.D* format.
directed-request	(Optional) Displays the directed request configuration.
groups [*group-name*]	(Optional) Displays information about the configured RADIUS server groups or a specific RADIUS server group.
group-name	(Optional) Name of the RADIUS server group. The name is alphanumeric and case-sensitive. The name can be maximum 64 characters.
sorted	(Optional) Displays sorted-by-name information about the RADIUS servers.
statistics	(Optional) Displays RADIUS statistics for the RADIUS servers. A hostname or IP address is required.

Command Default

Displays the global RADIUS server configuration.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

RADIUS preshared keys are not visible in the **show radius-server** command output. Use the **show running-config radius** command to display the RADIUS preshared keys.

Examples

The following is sample output from the **show radius-server** command and displays information about the RADIUS servers configured on the switch:

```
switch# show radius-server
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:5
source interface:any available
total number of servers:2

following RADIUS servers are configured:
        192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
```

```
        host1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
switch#
```

The following is sample output from the **show radius-server 192.268.2.168** command and displays information about the specified RADIUS server:

```
switch# show radius-server 192.168.2.168
192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
                idle time:10
                test user:testuser
                test password:********
switch#
```

The following is sample output from the **show radius-server directed-request** command and displays information about the RADIUS directed request configuration:

```
switch# show radius-server directed-request
disabled
switch#
```

The following is sample output from the **show radius-server groups** command and displays information about the RADIUS server groups:

```
switch# show radius-server groups
total number of groups:1

following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
                deadtime is 0
switch#
```

The following is sample output from the **show radius-server groups** command and displays information about the specified RADIUS server group:

```
switch# show radius-server groups RadServer
group RadServer:
                server: host1 on auth-port 1812, acct-port 1813
                deadtime is 5
switch#
```

The following is sample output from the **show radius-server sorted** command and displays information about the RADIUS servers configured on the switch, sorted by radius server names:

```
switch# show radius-server sorted
timeout value:5
retransmission count:1
deadtime value:5
source interface:any available
total number of servers:2

following RADIUS servers are configured:
        192.168.2.168:
                available for authentication on port:1812
                available for accounting on port:1813
        host1:
                available for authentication on port:1812
                available for accounting on port:1813
```

```
switch#
```

The following is sample output from the **show radius-server statistics** command and displays the statistics for a specified RADIUS servers:

```
switch# show radius-server statistics 192.168.2.168
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
switch#
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

show role

To display the user role configuration, use the **show role** command.

show role [**name** *role-name*]

Syntax Description

name *role-name*	(Optional) Displays information for a specific user role name. The name can be maximum 16 characters.

Command Default

Displays information for all user roles.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role name** command and displays information about the specified user role:

```
switch# show role name MyRole
```

The following is sample output from the **show role** command and displays information about all user roles:

```
switch# show role
Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: myRole
  Description: User-defined user who can operate the switch
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 3,5
  Interface policy: deny
  Permitted interfaces:
  Ethernet1/3,Ethernet1/5
  Vrf policy: deny
```

```
  Permitted vrfs: management
  --------------------------------------------------------------------
  Rule    Perm    Type         Scope               Entity
  --------------------------------------------------------------------
  5       permit  command                          configure terminal ; vlan *
  4       permit  read-write   feature-group       myGroup
  3       deny    read-write   feature             arp
  2       deny    command                          clear users
  1       permit  read         feature             ping

switch#
```

Related Commands

Command	Description
role name	Configures user roles.

show role feature

To display the user role features, use the **show role feature** command.

show role feature [**detail** | **name** *feature-name*]

Syntax Description

detail	(Optional) Displays detailed information for all features.
name *feature-name*	(Optional) Displays detailed information for a specific feature. The name can be maximum 16 characters.

Command Default

Displays a list of user role feature names.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role feature** command and displays information about the user role features:

```
switch# show role feature
feature: aaa
feature: access-list
feature: arp
feature: callhome
feature: cdp
feature: install
feature: l3vm
feature: license
feature: ping
feature: platform
feature: radius
feature: snmp
feature: syslog
feature: tacacs
feature: eth-span
feature: ethanalyzer
feature: spanning-tree
feature: vlan
switch#
```

The following is sample output from the **show role feature detail** command and displays detailed information about the user role features:

```
switch# show role feature detail
feature: aaa
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
```

```
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
feature: access-list
  show ip access-lists *
  show ipv6 access-lists *
  show mac access-lists *
  show arp access-lists *
  show vlan access-map *
  show vlan access-list *
  show vlan filter *
  config t ; ip access-list *
  config t ; ipv6 access-list *
  config t ; mac access-list *
  config t ; arp access-list *
  config t ; vlan access-map *
  config t ; time-range *
  config t ; resequence *
  config t ; errdisable detect cause acl-exception
  config t ; object-group *
  config t ; interface * ; ip access-group *
  config t ; interface * ; ip port access-group *
  config t ; interface * ; ipv6 traffic-filter *
  config t ; interface * ; ipv6 port traffic-filter *
  config t ; interface * ; errdisable port detect cause acl-exception
  config s ; ip access-list *
  config s ; ipv6 access-list *
  config s ; mac access-list *
--More--
switch#
```

The following is sample output from the **show role feature name** command and displays detailed information about the specific user role feature:

```
switch# show role feature name vlan
feature: vlan
  show vlan *
  config t ; vlan *
  vlan *
  clear vlan *
  debug vlan *
  show vlan-mgr *
  config t ; vlan-mgr *
  vlan-mgr *
  clear vlan-mgr *
  debug vlan-mgr *
  show pvlan *
  config t ; pvlan *
  pvlan *
  clear pvlan *
  debug pvlan *
switch#
```

Related Commands

Command	Description
feature (user role)	Configures a feature in a user role feature group.

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show role feature-group

To display the user role feature groups, use the **show role feature-group** command.

show role feature-group [**detail** | **name** *group-name*]

Syntax Description

detail	(Optional) Displays detailed information for all feature groups.
name *group-name*	(Optional) Displays detailed information for a specific feature group.

Command Default

Displays a list of user role feature groups.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show role feature-group** command and displays information about the user role feature groups:

```
switch# show role feature-group

feature group: myGroup
feature: aaa
feature: radius
feature: tacacs
switch#
```

The following is sample output from the **show role feature-group detail** command and displays detailed information about the user role feature groups:

```
switch# show role feature-group detail
```

The following is sample output from the **show role feature-group name** command and displays information about a specific user role feature group:

```
switch# show role feature-group name SecGroup
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show running-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the running configuration, use the **show running-config aaa** command.

show running-config aaa [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config aaa** command and displays the configured AAA information in the running configuration:

```
switch# show running-config aaa
version 4.1(2)E1(1)
aaa authentication login default group radius
radius-server directed-request
tacacs-server directed-request

switch#
```

The following is sample output from the **show running-config aaa all** command and displays the detailed AAA configuration information in the running configuration:

```
switch# show running-config aaa all
version 4.1(2)E1(1)
no snmp-server enable traps aaa server-state-change
aaa authentication login default group radius
aaa accounting default local
aaa user default-role
no aaa authentication login error-enable
no aaa authentication login mschap enable
no aaa authentication login ascii-authentication
radius-server directed-request
no tacacs-server directed-request
tacacs-server directed-request

switch#
```

Related Commands

Command	Description
show aaa accounting	Displays AAA accounting configuration information.
show aaa authentication	Displays AAA authentication configuration information.
show startup-config aaa	Displays AAA configuration in the startup configuration.

show running-config radius

To display RADIUS server information in the running configuration, use the **show running-config radius** command.

show running-config radius [**all**]

Syntax Description

all	(Optional) Displays default RADIUS configuration information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config radius** command and displays information about the RADIUS server configuration:

```
switch# show running-config radius
version 4.1(2)E1(1)
radius-server host 192.168.2.168 authentication accounting
radius-server host host1 key 7 "MyKeyEnc" authentication accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" authentication accounting
aaa group server radius RadServer
    server host1
    deadtime 5

switch#
```

The following is sample output from the **show running-config radius all** command and displays detailed information about RADIUS server groups and host configurations:

```
switch# show running-config radius all
version 4.1(2)E1(1)
radius-server timeout 5
radius-server retransmit 1
radius-server deadtime 0
no ip radius source-interface
radius-server host 192.168.2.168 auth-port 1812 acct-port 1813 authentication acco
unting
radius-server host 192.168.2.168 test username test password test idle-time 0
radius-server host host1 key 7 "MyKeyEnc" auth-port 1812 acct-port 1813 authenti
cation accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" auth-port 1812 acct-port 1813 authentica
tion accounting
radius-server host myRad test username test password test idle-time 0
aaa group server radius radius
```

```
    server 192.168.2.168
    server host1
    server myRad
    deadtime 0
    use-vrf default
    no source-interface
aaa group server radius RadServer
    server host1
    deadtime 5
    use-vrf default
    no source-interface

switch#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.
show startup-config radius	Displays RADIUS server in the startup configuration.

show running-config security

To display user account, SSH server, and Telnet server information in the running configuration, use the **show running-config security** command.

show running-config security [**all**]

Syntax Description

all	(Optional) Displays default user account, SSH server, and Telnet server configuration information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config security** command and displays the running configuration information about the user account, SSH server, and Telnet server:

```
switch# show running-config security
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role networ
-operator
username admin password 5 $1$zkTYLs/y$sOecMEkhsnJT8Lu8rbPAQ/  role network-admi
username USERID password 5 $1$8UHo5rdt$6zLdUqn4dr3Aqk0DFyBlq.  role network-ope
ator

banner motd #Nexus 4000 Switch#

switch#
```

The following is sample output from the **show running-config security all** command and displays the detailed security information available in the running configuration.

```
switch# show running-config security all
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network
-operator
username admin password 5 $1$qBkDwg9Y$JLTReKR3IWscqEAXpPLb5/  role network-admin
username USERID password 5 $1$fDVBuiJu$MQ3JiBFO7AAFqnzSwMhEE.  role network-oper
ator
password strength-check
```

```
banner motd #Nexus 4000 Switch#

ssh key rsa 1024
no ssh key dsa

switch#
```

Related Commands

Command	Description
show startup-config security	Displays user accounts, SSH server, and Telnet server configuration information in the startup configuration.

show running-config tacacs+

To display TACACS+ configuration information in the running configuration, use the **show running-config tacacs+** command.

show running-config tacacs+ [**all**]

Syntax Description

all	(Optional) Displays default TACACS+ configuration information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable the TACACS+ feature on the switch by using the **feature tacacs+** command before you can display TACACS+ information.

Examples

The following is sample output from the **show running-config tacacs+** command and displays information about the TACACS+ configuration:

```
switch# show running-config tacacs+
version 4.1(2)E1(1)
feature tacacs+

tacacs-server deadtime 5
tacacs-server host tacacs2 key 7 "DjcPwy" timeout 5
tacacs-server host tacacs2 test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy"
aaa group server tacacs+ tacacs
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20
switch#
```

The following is sample output from the **show running-config tacacs+ all** command and displays detailed information about the TACACS+ configuration:

```
switch# show running-config tacacs+ all
version 4.1(2)E1(1)
feature tacacs+

tacacs-server timeout 5
tacacs-server deadtime 5
no ip tacacs source-interface
tacacs-server host tacacs2 key 7 "DjcPwy" port 49 timeout 5
tacacs-server host tacacs2 test username test password test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy" port 49
```

```
tacacs-server host tacacs3 test username test password test idle-time 0
aaa group server tacacs+ tacacs
    use-vrf default
    no source-interface
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20
    use-vrf default
    no source-interface

switch#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+ on the switch.
show startup-config tacacs+	Displays TACACS+ server information in the startup configuration.
show tacacs-server	Displays TACACS+ server information.

show ssh key

To display the Secure Shell (SSH) server key, use the **show ssh key** command.

show ssh key

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **ssh server enable** command.

Examples

The following is sample output from the **show ssh key** command and displays information about the SSH server keys:

```
switch# show ssh key
**************************************
rsa Keys generated:Tue Aug  4 22:18:57 2009

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAop9LIBbT2mydCBOpt8PZ9jYZuUiVqyLBcL7ogcOpuN4M
Ju+Y6pa7v3nvwcUQ8LRxq6pVL5lFO5heU/RV0sU4vaWLY1lMWuAIgIcLY7YX2zv7Pte6gW2Y8jVVI3ce
jt09OffM2JiHc/KJbPfchzC7+FJJ+s5ivKodYG4bnL1gBw0=

bitcount:1024
fingerprint:
c1:e4:a1:27:ea:01:52:fd:b1:a9:a1:ca:c4:aa:53:53
**************************************
dsa Keys generated:Wed Aug  5 09:23:37 2009

ssh-dss AAAAB3NzaC1kc3MAAACBAKQrOK6RvuQ9NvUnXU8xnmmZkguTjT84RlE9piyRMcTNWYsLsRi9
TJS1mHNnEk5h8+4Cfi16BRFgsoI952tzff4j+YunmuxXxuvZ3t37L8j8wB/gTIU2QAcSOM8A3d2pjcMj
d7VMW1vilkJfGDfTJHmToTR5vCHka+yZbLqEn7/tAAAAFQCGcIm8L9EozxDNGcZUA4D2C3120wAAAIBs
7oVB5ESlmYKcIWUbear54nqnbD5d9KYH1rtnIUIp8k6vACYMDfnXQv/zMdZS3s/8YCqGU8XD1dl52Lw+
JVMtHVgyqL2t9O9XFe2ew61kqHh1jbJFmmTuW+iUBYZshTDn5N8Ujw2Nrpu3+j1BFsTIV//mIC5Dzcpf
D7+5pNMZ5wAAAIBASR/ooYfMPJAWTrSRwifes5ByEffUn1lnes4/NxwnqMNLnMhMuuYE3t/X2oZXNI/k
EIxNyQ0X08mIktVRdSZQ7lITkWtYYQPA/Ua91bevFzgiwWZam4aswwHOHMO4bd1guVyQGngBjON3iTs5
KvemLHjVT3yiri9aDdvBfw78XQ==

bitcount:1024
fingerprint:
1a:8a:66:44:27:35:d6:8e:93:89:5b:5b:02:31:9c:60
**************************************
switch#
```

Related Commands

Command	Description
ssh key	Configures the SSH server key.

show ssh server

To display the Secure Shell (SSH) server status, use the **show ssh server** command.

show ssh server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must enable SSH on the switch by using the **feature ssh** command.

Examples

The following is sample output from the **show ssh server** command and displays information about the SSH server status:

```
switch# show ssh server
ssh version 2 is enabled
switch#
```

Related Commands

Command	Description
feature ssh	Enables SSH on the switch.
ssh server enable	Enables the SSH server.

show startup-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the AAA running configuration to the startup configuration before you can display the AAA startup configuration information.

Examples

The following is sample output from the **show startup-config aaa** command and displays information about the AAA available in the startup configuration:

```
switch# show startup-config aaa
version 4.1(2)E1(1)
aaa authentication login default group radius
radius-server directed-request
tacacs-server directed-request

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config aaa	Displays AAA configuration information in the running configuration.

show startup-config radius

To display RADIUS configuration information in the startup configuration, use the **show startup-config radius** command.

show startup-config radius

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config radius** command and displays information about the RADIUS server available in the startup configuration:

```
switch# show startup-config radius
version 4.1(2)E1(1)
radius-server host 192.168.2.168 authentication accounting
radius-server host host1 key 7 "MyKeyEnc" authentication accounting
radius-server host host1 test username testuser password testpwd idle-time 10
radius-server host myRad key 7 "KkxPwy" authentication accounting
radius-server host myRad test username testuser password testpwd idle-time 10
aaa group server radius RadServer
    server host1
    deadtime 5

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config radius	Displays the RADIUS server information in the running configuration.

show startup-config security

To display user account, SSH server, and Telnet server configuration information in the startup configuration, use the **show startup-config security** command.

show startup-config security

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config security** command and displays information about the user account, SSH server, and Telnet server available in the startup configuration:

```
switch# show startup-config security
version 4.1(2)E1(1)
feature telnet
no feature ssh

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network
-operator
username admin password 5 $1$qBkDwg9Y$JLTReKR3IWscqEAXpPLb5/  role network-admin
username USERID password 5 $1$fDVBuiJu$MQ3JiBFO7AAFqnzSwMhEE.  role network-oper
ator

banner motd #Nexus 4000 Switch#

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config security	Displays the user account, SSH server, Telnet server information in the running configuration.

show startup-config tacacs+

To display TACACS+ configuration information in the startup configuration, use the **show startup-config tacacs+** command.

show startup-config tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must copy the changes made to the RADIUS server running configuration to the startup configuration before you can display the RADIUS server startup configuration information.

Examples

The following is sample output from the **show startup-config tacacs+** command and displays information about the TACACS+ server configuration available in the startup configuration:

```
switch# show startup-config tacacs+
version 4.1(2)E1(1)
feature tacacs+

tacacs-server deadtime 5
tacacs-server host tacacs2 key 7 "DjcPwy" timeout 5
tacacs-server host tacacs2 test idle-time 10
tacacs-server host tacacs3 key 7 "DjcPwy"
aaa group server tacacs+ tacacs
aaa group server tacacs+ TacServer
    server tacacs2
    deadtime 20

switch#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
show running-config tacacs+	Displays the TACACS+ server information in the running configuration.

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [{*hostname* | *ipv4-address*} | **directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

hostname	(Optional) TACACS+ server Domain Name System (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured TACACS+ server groups.
sorted	(Optional) Displays sorted-by-name information about the TACACS+ servers.
statistics	(Optional) Displays TACACS+ statistics for the TACACS+ servers.

Defaults

Displays the global TACACS+ server configuration.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you can display TACACS+ information.

TACACS+ preshared keys are not visible in the **show tacacs-server** command output. Use the **show running-config tacacs+** command to display the TACACS+ preshared keys.

Examples

The following is sample output from the **show tacacs-server** command and displays information about the TACACS+ servers:

```
switch# show tacacs-server
timeout value:5
deadtime value:5
source interface:any available
total number of servers:1

following TACACS+ servers are configured:
        tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
switch#
```

The following is sample output from the **show tacacs-server** command and displays information about a specified TACACS+ server:

```
switch# show tacacs-server tacacs2
tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
                idle time:10
                test user:test
                test password:********
switch#
```

The following is sample output from the **show tacacs-server directed-request** command and displays information about the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
disabled
switch#
```

The following is sample output from the **show tacacs-server groups** command and displays information about the TACACS+ server groups:

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group tacacs:
                deadtime is 0
        group TacServer:
                server tacacs2 on port 49
                deadtime is 20
                vrf is default
switch#
```

The following is sample output from the **show tacacs-server groups** command and displays information about a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
group TacServer:
                server tacacs2 on port 49
                deadtime is 20
                vrf is default
switch#
```

The following is sample output from the **show tacacs-server sorted** command and displays information about the TACACS+ servers, sorted by server name:

```
switch# show tacacs-server sorted
timeout value:5
deadtime value:5
source interface:any available
total number of servers:2

following TACACS+ servers are configured:
        tacacs2:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
        tacacs3:
                available on port:49
                TACACS+ shared secret:********
switch#
```

The following is sample output from the **show tacacs-server statistics** command and displays the statistical information for a specified TACACS+ server:

```
switch# show tacacs-server statistics tacacs2
Server is dead since 0 hrs, 0 min, 0 sec

Monitoring Statistics
        Time in previous state: 0 hrs, 10 min, 2 sec
        Number of times dead: 1
        Total time in dead state: 0 hrs, 0 min, 0 sec

Authentication Statistics
        failed transactions: 1
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
switch#
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.
show startup-config tacacs+	Displays TACACS+ server information in the startup configuration.
tacacs-server host	Configures TACACS+ server parameters.

show telnet server

To display the Telnet server status, use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show telnet server** command and displays information about the Telnet server status:

```
switch# show telnet server
telnet service enabled
switch#
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show user-account

To display information about the user accounts on the switch, use the **show user-account** command.

show show user-account [*name*]

Syntax Description		
	name	(Optional) Displays information about the specified user account only.

Command Default Displays information about all the user accounts defined on the switch.

Command Modes EXEC

Command History	Release	Modification
	4.1(2)E1(1)	This command was introduced.

Examples The following is sample output from the **show user-account** command and displays information about the user accounts defined on the switch:

```
switch# show user-account
user:root
        this user account has no expiry date
        roles:network-operator
user:adminbackup
        this user account has no expiry date
        roles:network-operator
user:admin
        this user account has no expiry date
        roles:network-admin
        ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxXkib5JVXsM/GVJtYeZS
Gah8IR20OsqnN0QZ166wtR/b0MDPv1MuMuJl1suzV2NkohuH9n55jTnwaFovuw6F238pkbhzJ6YdQjMK
67g+YDSAMjB3Ywh1lA+HYIv3juFVEiGP4daXMPFFQe5FHCZMDHWrzSFpp8oa5asfoasCI2U=
user:USERID
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-dss AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4
vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3
StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanUTBmqobVDazIVAAAAFQCJJio5hvUY
xYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AMI8IXZgD7XfGnnYPMTn
nfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc5NrR8Ias
Zbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+m
Avw7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ck
dZkj5pb9Fpx2YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==

switch#
```

The following is sample output from the **show user-account user1** command and displays information about a specific user account:

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-dss AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4
vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3
StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanUTBmqobVDazIVAAAAFQCJJio5hvUY
xYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AMI8IXZgD7XfGnnYPMTn
nfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc5NrR8Ias
Zbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+m
Avw7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ck
dZkj5pb9Fpx2YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==
switch#
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
username	Configures a user account.

show users

To display the users currently logged on the switch, use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show users** command and displays information about the users currently logged on the switch:

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Aug 10 04:49 03:43        2736
admin    pts/1        Aug 10 07:38   .          3952 (192.168.2.168) *
switch(config)#
```

Related Commands

Command	Description
clear user	Logs out a specific user.
username	Creates and configures a user account.

show vlan access-list

To display the contents of the IPv4 ACL or MAC ACL associated with a specific VLAN access map, use the **show vlan access-list** command.

show vlan access-list *map-name*

Syntax Description

map-name	VLAN access list to show.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

For the specified VLAN access map, the switch displays the access map name and the contents of the ACL associated with the map.

Examples

The following is sample output from the **show vlan access-list** command and displays information about the ACLs associated with the specified VLAN access map:

```
switch# show vlan access-list vlan-map-01

VLAN access-map vlan-map-01 1
        IP access list ip-acl-01
        1 remark This ACL permits UDP traffic
        21 permit udp 192.168.2.37/3 192.168.2.176/3
        41 permit tcp 192.168.5.23/12 192.168.5.176/12
switch#
```

Related Commands

Command	Description
mac access-list	Create or configures a MAC ACL.
show access-lists	Displays information about how a VLAN access map is applied.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
vlan access-map	Configures a VLAN access map.

show vlan access-map

To display all VLAN access maps or a VLAN access map, use the **show vlan access-map** command.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) VLAN access map to show.

Command Default

The switch shows all VLAN access maps, unless you use the *map-name* argument to select a specific access map.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

For each VLAN access map displayed, the switch shows the access map name, the ACL specified by the **match** command, and the action specified by the **action** command.

Use the **show vlan filter** command to see which VLANs have a VLAN access map applied to them.

Examples

The following is sample output from the **show vlan access-map** command and displays information about a specific VLAN access map:

```
switch# show vlan access-map vlan-map-01

Vlan access-map vlan-map-01 1
        match ip: ip-acl-01
        action: forward
        statistics per-entry

switch#
```

The following is sample output from the **show vlan access-map** command and displays information about all VLAN access maps configured on the switch:

```
switch# show vlan access-map
```

Related Commands

Command	Description
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

show vlan filter

To display information about the instances of the **vlan filter** command, including the VLAN access map and the VLAN IDs affected by the command, use the **show vlan filter** command.

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id*]

Syntax Description

access-map *map-name*	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan *vlan-id*	(Optional) Limits the output to access maps that are applied to the specified VLAN only.

Command Default

All instances of VLAN access maps applied to a VLAN are displayed, unless you use the **access-map** keyword and specify an access map or you use the **vlan** keyword and specify a VLAN ID.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

The following is sample output from the **show vlan filter** command and displays information about the instances of VLAN access maps that are applied to VLANs:

```
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    3
switch#
```

Related Commands

Command	Description
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

ssh

To start a Secure Shell (SSH) session using IPv4 to connect to remote devices, use the **ssh** command.

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Username for the SSH session.
ipv4-address	IPv4 address of the remote host.
hostname	Hostname of the remote host.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The VRF name can be one of the following: • **chassis-management** • **default** • **management**

Command Default

Default VRF.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to create an SSH session using IPv4:

```
switch# ssh root@192.168.2.168 vrf management
```

Related Commands

Command	Description
show running-config security	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.

ssh key

To create a Secure Shell (SSH) server key, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algrorithm (DSA) SSH server key.
force	(Optional) Forces the generation of a DSA SSH key even if previous ones are present.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Command Default

1024-bit length.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using RSA with the default key length:

```
switch(config)# ssh key rsa
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch(config)# ssh key rsa 768
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

```
switch(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config security	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh key	Displays the SSH server key information.
show ssh server	Displays the SSH server configuration.
ssh server enable	Enables the SSH server.

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to enable the SSH server:

```
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch(config)# no ssh server enable
```

Related Commands

Command	Description
show ssh server	Displays the SSH server configuration.

statistics per-entry

To collect statistics for each ACL entry, use the **statistics per-entry** command. To remove statistics, use the **no** form of this command.

statistics per-entry

no statistics per-entry

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are collected.

Command Modes

Vlan access-map configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to collect statistics for each ACL entry:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# statistics per-entry
switch(config-access-map)#
```

This example shows how to remove statistics:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# no statistics per-entry
switch(config-access-map)#
```

Related Commands

Command	Description
match	Specifies an access control list (ACL) for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.

storm-control

To set the storm-control threshold value and block forwarding of unnecessary flooded traffic on the interface, use the **storm-control level** command. To turn off storm control and restore the default threshold, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*]

no storm-control {broadcast | multicast | unicast} level

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level *percentage*	Percentage of the suppression level. The range is from 1 to 100 percent.
fraction	(Optional) Fraction of the suppression level. The range is from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

A traffic storm occurs when packets flood the interface, creating excessive traffic and degrading network performance. The traffic storm control (also called traffic suppression) feature prevents interface ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

The period (.) is required when you enter the fractional-suppression level.

The suppression level is a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port.

Use the **show interface counters storm-control** command to display the discard count.

Use one of the following methods to turn off suppression for the specified traffic type:

- Set the level to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable multicast traffic storm control on Ethernet interface 1/2 and how to configure the traffic storm control level at 70.5 percent:

```
switch(config)# interface ethernet 1/2
switch(config-if)# storm-control multicast level 70.5
```

This example shows how to limit the threshold of broadcast traffic to 30 percent:

```
switch(config-if)# storm-control broadcast level 30
```

This example shows how to disable the suppression mode for multicast traffic:

```
switch(config-if)# no storm-control multicast level
```

Related Commands

Command	Description
show interface counters storm-control	Displays the total number of packets discarded for all three traffic storm control modes, on all interfaces or on the specified interface.
show running-config	Displays the configuration of the interface.

tacacs-server deadtime

To set a global periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To restore the default dead-time interval, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

minutes	Specifies the time interval in minutes. The range is from 1 to 1440.

Command Default

0 minutes.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to configure the global dead-time interval and enable periodic monitoring:

```
switch(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch(config)# no tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive RADIUS or TACACS+ server group.
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured TACACS+ server groups.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

During login, the user can specify the *username@vrfname:hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# tacacs-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays a directed request TACACS+ server configuration.

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

Syntax Description

hostname	TACACS+ server Domain Name System (DNS) name. The maximum character size is 256.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
key	(Optional) Configures the shared secret key of the TACACS+ server.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Configures a preshared key to authenticate communication between the TACACS+ client and server. The maximum length is 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	(Optional) Specifies a user password in the test packets. The maximum size is 32.
username *name*	(Optional) Specifies a username in the test packets. The maximum size is 32.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Command Default

Idle time: disabled.

Server monitoring: disabled.

Timeout: 1 second.

Test username: test.

Test password: test.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

This example shows how to configure the server IP address or hostname as a TACACS+ server host:

```
switch(config)# tacacs-server host tacacs2
```

This example shows how to configure a TCP port other than port 49 (the default for TACACSS+ requests):

```
switch(config)# tacacs-server host tacacs3 port 2
```

This example shows how to configure periodic monitoring of a TACACS+ host:

```
switch(config)# tacacs-server host tacacs3 test username user1 password a3z9yjqz7
idle-time 3
switch(config)#
```

This example shows how to set the timeout interval for a specific TACACS+ host:

```
switch(config)# tacacs-server host tacacs3 timeout 10
```

This example shows TACACS+ configuration:

```
switch(config)# tacacs-server host tacacs2 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs2 test idle-time 10
switch(config)# tacacs-server host tacacs2 test username tester
switch(config)# tacacs-server host tacacs2 test password 2B9ka5
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server configuration.

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To remove a configured shared secret, use the **no** form of this command.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The maximum length is 63 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

The following example shows how to configure TACACS+ server shared keys:

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To restore the default global timeout value, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The valid range is 1 to 60 seconds.

Command Default

1 second.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to configure the TACACS+ server timeout value:

```
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch(config)# no tacacs-server timeout 3
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

telnet

To create a Telnet session using IPv4 on a switch, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv4-address	IPv4 address of the remote switch.
hostname	Hostname of the remote switch.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The VRF name can be one of the following: • **chassis-management** • **default** • **management**

Command Default

Port 23 is the default port.

Command Modes

EXEC

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to start a Telnet session using IPv4:

```
switch# telnet 192.168.2.168 vrf management
```

Related Commands

Command	Description
feature telnet	Enables Telnet on the switch.
show running-config security	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show telnet server	Displays the Telnet server status.
telnet server enable	Enables the Telnet server.

telnet server enable

To enable the Telnet server, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enable the Telnet server:

```
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch(config)# no telnet server enable
```

Related Commands

Command	Description
copy running-config startup-config	Copies thee changes made in the running configuration to the startup configuration.
show telnet server	Displays the Telnet server status.

use-vrf

To specify a virtual routing and forwarding (VRF) instance for a RADIUS or TACACS+ server group, use the **use-vrf** command. To remove the VRF instance, use the **no** form of this command.

use-vrf *vrf-name*

no use-vrf *vrf-name*

Syntax Description

vrf-name	Specifies VRF instance name.

Command Default

No default behavior or values.

Command Modes

Radius server group configuration

Tacacs+ server group configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command radius server group configuration mode or the **aaa group server tacacs+** command to enter tacacs+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to specify a VRF instance for a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
```

This example shows how to specify a VRF instance for a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf management
```

This example shows how to remove the VRF instance from a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf management
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
show vrf	Displays VRF information.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

username

To create and configure a user account, use the **username** command. To remove a user account, use the **no** form of this command.

username *user-id* [**expire** *date* | **password** [**0** | **5**] *password* | **role** *role-name* | **sshkey** {*key* | **filename** *filename*}

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters.
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password	(Optional) Specifies a password for the account. The default is no password.
0	(Optional) Specifies that the password that follows should be in clear text.
5	(Optional) Specifies that the password that follows should be encrypted.
password	Password for the user. The maximum length is 64 characters.
role *role-name*	(Optional) Specifies the role which the user is to be assigned to.
sshkey	(Optional) Specifies an SSH key for the user account for SSH authentication.
key	SSH key string.
filename *filename*	Specifies the name of a file that contains the SSH key string. The filename must be in the Cisco NX-OS file system format, *filesystem*:[/*directory*][/*filename*]. Table 1-4 lists URL prefix keywords for local writable storage file systems.

Command Default

No expiration date, password, or SSH key.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

The switch accepts only strong passwords. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words

- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Note Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, the password cannot include the quotation mark (" or '), vertical bar (|), or right angle bracket (>) characters at the beginning of the password.

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

Examples

This example shows how to create a user account:

```
switch(config)# username user1 password Ci5co@321
```

This example shows how to configure the SSH key for a user account:

```
switch(config)# username user1 sshkey ssh-dss
AAAAB3NzaC1kc3MAAACBAM694BlguDIyzxeqcry8gEu1Wke4vB+TtVO7T+oAm1KpWM0GAtSr7ANSjlcqKyNGiosNzZ
/41FDWunjBJs4xYCbAJK7/IhLYYHeaSKzPH5h3StFJD6U3u8HLHfeaMaogzAv8eUA6SLQCDBDfHJPWGcsDguItCanU
TBmqobVDazIVAAAAFQCJJio5hvUYxYxFSDUSbzdtXYWpgwAAAIASv6eEMXmR5M5hlCmyE3NPCiTHvrCWwaqROet6AM
I8IXZgD7XfGnnYPMTnnfVTPJZnaCTjL+fH06Bjl0nBLmvsDE1Hcndrn3ldeJwolVtmcjDYBmUUdqncxn48qxaxSsNc
5NrR8IasZbo02GJDa8tduhLAKRJTZ/xs9GgKUieITAAAAIA3q0tmhwnRgHJMOb3Y9A3rUewKO6fMTqBbLh14bs+mAv
w7h7kOwYJcmWpYVk58Svrqy/asMBY19PCyXn7NjaIxQZLEyA3Ep50iSvbydXqbkVyX7D1GSjV4H+ckdZkj5pb9Fpx2
YuNXvrF9vaoLUdI4Tu2FosElijrO/FI8artF8A==
```

This example shows how to configure the SSH key for a user account using a key stored in the file system:

```
switch(config)# username user1 sshkey file bootflash:key_file
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show user-account	Displays the user account configuration.

vlan access-map

To create a VLAN access map or to configure an existing VLAN access map, use the **vlan access-map** command. To remove a VLAN access map, use the **no** form of this command.

vlan access-map *map-name*

no vlan access-map *map-name*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure. The name can be maximum 64 characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

Each VLAN access map can include one **match** command and one **action** command.

Examples

This example shows how to create a VLAN access map named vlan-map-01:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)#
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan filter	Applies a VLAN access map to one or more VLANs.

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To remove a VLAN access map, use the **no** form of this command.

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure. The name can be maximum 64 characters.
vlan-list *VLAN-list*	Specifies the ID of one or more VLANs whose traffic the VLAN access map filters. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs. For example, use 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs. For example, use 20,70-100,142. **Note** When you use the **no** form of this command, the *VLAN-list* argument is optional. If you omit this argument, the switch removes the access map from all VLANs where the access map is applied.

Command Default

No default behavior or values.

Command Modes

Configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Usage Guidelines

You can apply a VLAN access map to one or more VLANs.

You can apply only one VLAN access map to a VLAN.

The **no** form of this command enables you to unapply a VLAN access map from all or part of the VLAN list that you specified when you applied the access map. To unapply an access map from all VLANs where it is applied, you can omit the *VLAN-list* argument. To unapply an access map from a subset of the VLANs where it is currently applied, use the *VLAN-list* argument to specify the VLANs where the access map should be removed.

Examples

This example shows how to apply a VLAN access map named vlan-map-01 to VLANs 20 through 45:

```
switch(config)# vlan filter vlan-map-01 20-45
```

Related Commands

Command	Description
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.

vlan policy deny

To deny access to a VLAN and enter vlan policy configuration mode for a user role, use the **vlan policy deny** command. To revert to the default VLAN policy for a user role, use the **no** form of this command.

vlan policy deny

no vlan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All VLANs.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter vlan policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

This example shows how to revert to the default VLAN policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
permit vlan	Specifies a range of VLANs that the role can access.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

vrf policy deny

To deny access to a Virtual Private Network (VPN) routing and forwarding instance (VRF) and enter vrf policy configuration mode for a user role, use the **vrf policy deny** command. To revert to the default VRF policy for a user role, use the **no** form of this command.

vrf policy deny

no vrf policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User role configuration

Command History

Release	Modification
4.1(2)E1(1)	This command was introduced.

Examples

This example shows how to enter vrf policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

This example shows how to revert to the default VRF policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
permit vrf	Specifies a range of VRFs that the role can access.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.