

Management ACL Commands

This chapter contains the following sections:

- deny (Management), on page 2
- permit (Management), on page 3
- management access-list, on page 4
- management access-class, on page 6
- show management access-list, on page 7
- show management access-class, on page 8

deny (Management)

To set permit rules (ACEs) for the management access list (ACL), use the **deny** Management Access-list Configuration mode command.

Syntax

deny [*interface-id*] [**service** *service*]

deny ip-source {*ipv4-address* | i*pv6-address*/ipv6-prefix-length} [**mask** {*mask* | *prefix-length*}] [*interface-id*] [**service** *service*]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service*—(Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ***ipv4-address***—Specifies the source IPv4 address.
- ***ipv6-address***/*ipv6-prefix-length*—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask** *mask*—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the ACL called **mlist**.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```

permit (Management)

To set permit rules (ACEs) for the management access list (ACL), use the **permit** Management Access-list Configuration mode command.

Syntax

permit *[interface-id] [service service]*

permit ip-source {*ipv4-address* | *ipv6-address*/ipv6-prefix-length} *[***mask** {mask | prefix-length}] [interface-id] [**service** service]

Parameters

- **interface-id** —(Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service* — (Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address** — Specifies the source IPv4 address.
- **ipv6-address/ipv6-prefix-length** — Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask** *mask* — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the ACL called **mlist**

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

management access-list

To configure a management access list (ACL) and enter the Management Access-list Configuration mode, use the **management access-list** Global Configuration mode command. To delete an ACL, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

Parameters

name—Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-list Configuration mode, where the denied or permitted access conditions are defined with the **deny** and **permit** commands.

If no match criteria are defined, the default value is **deny**.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the management access-class, on page 6 command to select the active access list.

The active management list cannot be updated or removed.

A management access-list configured as the access-class for the quiet-mode period (command login quiet-mode access-class in AAA Commands section) cannot be changed or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.

Example 1 - The following example creates a management access list called **mlist**, configures management gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1/0/1
switchxxxxxx(config-macl)# permit gi1/0/9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

Example 2 - The following example creates a management access list called ‘mlist’, configures all interfaces to be management interfaces except gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny gi1/0/1
switchxxxxxx(config-macl)# deny gi1/0/9
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

management access-class

To restrict management connections by defining the active management access list (ACL), use the **management access-class** Global Configuration mode command. To disable management connection restrictions, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

Parameters

- **console-only**—Specifies that the device can be managed only from the console.
- **name**—Specifies the ACL name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called **mlist** as the active management access list.

```
switchxxxxxx(config)# management access-class mlist
```

show management access-list

To display management access lists (ACLs), use the **show management access-list** Privileged EXEC mode command.

Syntax

show management access-list [*name*]

Parameters

name—(Optional) Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the **mlist** management ACL.

```
switchxxxxxx# show management access-list mlist
m1
--
deny service telnet
permit gi1/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

show management access-class

To display information about the active management access list (ACLs), use the **show management access-class** Privileged EXEC mode command.

Syntax

show management access-class

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

Example 1 -The following example displays the active management ACL information.

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```

Example 2 - The following example displays the active management ACL information, when management access class is enabled on the device, and the device is in the quiet-mode period (see commands login block-for and login quiet-mode access-class in AAA Commands section):

```
switchxxxxxx# show management access-class
Management access-class is enabled, using login quiet-mode period
access-class quiet-ACL(mlist access-list will be active when login quiet-mode
period ends
```