CHAPTER 21

# Troubleshooting IP Access Lists

This chapter describes how to troubleshoot IPv4 and IPv6 access lists (IP-ACLs) created and maintained in the Cisco MDS 9000 Family. It includes the following sections:


- Overview, page 21-1
- Initial Troubleshooting Checklist, page 21-4
- IP-ACL Issues, page 21-4


## Overview

IP-ACLs provide basic network security to all switches in the Cisco MDS 9000 Family. IP-ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

Each switch in the Cisco MDS 9000 Family can have a maximum of 64 IP-ACLs and each IP-ACL can have a maximum of 256 filters.

An IP filter contains rules for matching an IP packet based on the protocol, address, and port. IPv4 filters can also match on an ICMP type and type of service (ToS).

This section includes the following topics:


- Protocol Information, page 21-1
- Address Information, page 21-2
- Port Information, page 21-2
- ICMP Information, page 21-3
- ToS Information, page 21-3


### Protocol Information

You can specify the IP protocol in one of two ways:

- Specify an integer ranging from 0 to 255. This number represents the IP protocol.
- Specify the name of a protocol, restricted to Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

# Address Information

For IPv4, specify the source and source-wildcard or the destination and destination-wildcard in one of two ways:

- Use the 32-bit quantity in four-part, dotted decimal format (10.1.1.2 0.0.0.0 is the same as host 10.1.1.2).
  - Each wildcard bit set to zero indicates that the corresponding bit position in the packet's IPv4 address must exactly match the bit value in the corresponding bit position in the source.
  - Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's IPv4 address will be considered a match to this access list entry. Place ones in the binary bit positions you want to ignore and then convert to decimal. For example, use 0.0.255.255 to require an exact match of only the first 16 bits of the source. Wildcard bits set to one must be contiguous and at the end of the prefix. For example, a wildcard of 0.255.0.64 would not be valid.
- Use the **any** option as an abbreviation for a source and source-wildcard or destination and destination-wildcard (0.0.0.0 255.255.255.255)

For IPv6, specify the source or the destination IPv6 addresses in one of two ways:

- Use the 128-bit quantity in colon-separated hexadecimal <prefix>/<length> format. For example, use 2001:0DB8:800:200C::/64 to require an exact match of the first 64 bits of the source.
- Use the **any** option as an abbreviation for a source or destination.

# Port Information

To compare the source and destination ports, use the **eq** (equal) option, the **gt** (greater than) option, the **lt** (less than) option, or the **range** (range of ports) option. Table 21-1 displays the port numbers recognized by the Cisco SAN-OS software for associated TCP and UDP ports for IPv4.

**Note** IPv6-ACL CLI commands do not support TCP or UDP port names.

*Table 21-1 TCP and UDP Port Numbers for IPv4*

| Protocol | Port | Number |
|---|---|---|
| UDP | dns | 53 |
| | tftp | 69 |
| | ntp | 123 |
| | radius accounting | 1646 or 1813 |
| | radius authentication | 1645 or 1812 |
| | snmp | 161 |
| | snmp-trap | 162 |
| | syslog | 514 |

*Table 21-1 TCP and UDP Port Numbers for IPv4 (continued)*

| Protocol | Port | Number |
|---|---|---|
| TCP[1] | ftp | 20 |
| | ftp-data | 21 |
| | ssh | 22 |
| | telnet | 23 |
| | smtp | 25 |
| | tasacs-ds | 65 |
| | www | 80 |
| | sftp | 115 |
| | http | 143 |
| | wbem-http | 5988 |
| | wbem-https | 5989 |

1. If the TCP connection is already established, use the **established** option to find matches. A match occurs if the SYN flag is not set in the TCP datagram.

# ICMP Information

IP packets can be filtered based on the following optional ICMP conditions:

- The icmp-type: The ICMP message type is a number from 0 to 255.
- The icmp-code: The ICMP message code is a number from 0 to 255.

Table 21-2 displays the value for each ICMP type.

*Table 21-2 ICMP Type Value*

| ICMP Type | Code |
|---|---|
| echo | 8 |
| echo-reply | 0 |
| unreachable | 3 |
| redirect | 5 |
| time exceeded | 11 |
| traceroute | 30 |

# ToS Information

IPv4 packets can be filtered based on the ToS conditions—delay, monetary-cost, normal-service, reliability, and throughput.

# Initial Troubleshooting Checklist

Begin troubleshooting IP-ACLs by checking the following issues:

| Checklist | Check off |
|---|---|
| Verify licensing requirements. See *Cisco MDS 9000 Family Fabric Manager Configuration Guide*. | ❑ |
| Verify that the access list has been applied to the interface. | ❑ |
| Verify that the access list is not empty. | ❑ |
| Verify the order of the rules in the access list. | ❑ |

## Common Troubleshooting Tools in Fabric Manager

Choose **Switches > Security > IP ACL** to access IP-ACL configuration.

## Common Troubleshooting Commands in the CLI

The following commands may be useful in troubleshooting IP-ACL issues:

- **show ip access-list**
- **show ipv6 access-list**
- **show interface**
- Use the **log-deny** option at the end of a filter condition to log information about packets that match dropped entries. The log output displays the ACL number, permit or deny status, and port information. Use the following CLI commands to ensure that the debug messages are logged to the logfile for the kernel and ipacl facilities:
  - **logging logfile SyslogFile 7**
  - **logging level kernel 7**
  - **logging level ipacl 7**

# IP-ACL Issues

This section describes troubleshooting ACLs and includes the following topics:

- All Packets Are Blocked, page 21-5
- No Packets Are Blocked, page 21-7
- PortChannel Not Working with ACL, page 21-8
- Cannot Remotely Connect to Switch, page 21-8

# All Packets Are Blocked

**Symptom** All packets are blocked.

*Table 21-3 All Packets Are Blocked*

| Symptom | Possible Cause | Solution |
|---|---|---|
| All packets are blocked. | Access list is empty. | Remove the access list from the interface. Choose **Switches > Security > IP ACL** in Fabric Manager, select the **Interfaces** tab, and remove the ACL name from the ProfileName field. Click **Apply Changes**.<br>Or use the **no ip access-group** or the **no ipv6 traffic-filter** CLI command in interface mode. |
| | A deny filter is too broad. | Delete the deny filter. Choose **Security > IP ACL** in Device Manager, right-click the access list, and click **Rules**. Right-click the filter you want to delete and click **Delete**.<br>Or use the **no ip access-list** for IPv4-ACLs or **no ipv6 access-list** for IPv6, and use the **no deny** CLI command in IP-ACL configuration submode. |
| | Deny filter is too high in the access list order. | Delete the access list and re-create. See the "Re-creating IP-ACLs Using Fabric Manager" section on page 21-5 or the "Re-creating IP-ACLs Using the CLI" section on page 21-6. |
| | No existing permit filters match the packets. | Add an appropriate permit filter. Choose **Security > IP ACL** in Device Manager, right-click the access list, and click **Rules**. Click **Create.**<br>Or use the **ip access-list** for IPv4-ACLs or **ipv6 access-list** for IPv6, and use the **permit** CLI command in IP-ACL configuration submode. |

## Re-creating IP-ACLs Using Fabric Manager

To re-create an IP-ACL using Fabric Manager, follow these steps:

**Step 1** Choose **Switches > Security > IP ACL** and select the **Interfaces** tab.

**Step 2** Right-click all interfaces that have the IP-ACL you need to modify and remove the IP-ACL name from the ProfileName field.

**Step 3** Click **Apply Changes** to save these changes.

**Step 4** Click the **IP ACL wizard** icon. You see the IP-ACL wizard dialog box.

**Step 5** Add the IP-ACL name in the name field and click **Add**.

**Step 6** Set the IP address, subnet mask, and protocol.

**Step 7** Select **permit** or **deny** from the Action drop-down menu and click **Next**.

**Step 8** Check the switches that you want to apply this ACL to and click **Finish.**

## Re-creating IP-ACLs Using the CLI

To r-create an IP-ACL using the CLI, follow these steps:

**Step 1** Use the **show interface** command to determine which interfaces use the ACL.

```
switch# show interface gigabitethernet 2/1
GigabitEthernet2/1 is up
    Hardware is GigabitEthernet, address is 0005.3001.a706
    Internet address(es):
        4000::1/64
        fe80::205:30ff:fe01:a706/64
    MTU 2300  bytes
    Port mode is IPS
    Speed is 1 Gbps
    Beacon is turned off
    Auto-Negotiation is turned on
    ip access-group TCPAlow in
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1916 packets input, 114960 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    0 packets output, 0 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

**Step 2** Use the **no ip access-group** or the **no ipv6 traffic-filter** command in interface mode to remove the ACL from the interface. Repeat this step for all interfaces found in Step 1.

```
switch(config)# interface gigabitethernet 2/1
switch(config-if)# no ip access-group TCPAlow
```

**Step 3** Use the **no ip access-list** or the **no ipv6 access-list** command to delete the access list and all filters associated with it.

```
switch(config)# no ip access-list TCPAlow
```

**Note** We recommend deleting an ACL and re-creating it because you cannot change the order of filters in an ACL.

**Step 4** Use the **ip access-list** or the **ipv6 access-list** command to create an access list.

```
switch(config)# ip access-list List1 permit ip any any
```

**Tip** Add the filters in priority order. Add a fall-through filter in the case where no filter matches an incoming packet.

**Step 5** Use the **ip access-group** or the **ipv6 traffic-filter** command in interface mode to add the ACL to the interface. Repeat this step for all interfaces found in Step 1.

```
switch(config)# interface gigabitethernet 2/1
switch(config-if)# ip access-group List1

switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 traffic-filter IPAlow
```

# No Packets Are Blocked

**Symptom** No packets are blocked.

*Table 21-4 No Packets Are blocked*

| Symptom | Possible Cause | Solution |
|---|---|---|
| No packets are blocked. | A permit filter is too broad. | Delete the permit filter. Add an appropriate permit filter. Choose **Security > IP ACL** in Device Manager, right- click the access list and click **Rules**. Right-click the rule and click **Delete.**<br><br>Or use the **no ip access-list** for IPv4-ACLs or **no ipv6 access-list** for IPv6, and use the **no permit** CLI command in IP-ACL configuration submode. |
| | Permit filter is too high in the access list order. | Delete the access list and re-create. See the "Re-creating IP-ACLs Using Fabric Manager" section on page 21-5 or the "Re-creating IP-ACLs Using the CLI" section on page 21-6. |

# PortChannel Not Working with ACL

**Symptom** PortChannel not working with ACL.

*Table 21-5 PortChannel Not Working with ACL*

| Symptom | Possible Cause | Solution |
|---|---|---|
| PortChannel not working with ACL | ACL not applied to all interfaces in the PortChannel. | Add the ACL to all interfaces in the PortChannel. Choose **Switches > ISLs > Port Channels** to view the Members Admin field to find out which interfaces are part of the PortChannel. Choose **Switches > Security > IP ACL** on Fabric Manager, select the **Interfaces** tab, and add the ACL name to the ProfileName field. Click **Apply Changes**.<br><br>Or use the **show port-channel database** CLI command to find out which interfaces are part of the PortChannel and then use the **ip access-group** or the **ipv6 traffic-filter** CLI command in interface mode to add the ACL to all interfaces in the PortChannel. |

# Cannot Remotely Connect to Switch

**Symptom** Cannot remotely connect to switch.

*Table 21-6 Cannot Remotely Connect to Switch*

| Symptom | Possible Cause | Solution |
|---|---|---|
| Cannot remotely connect to switch. | Incorrect ACL on mgmt0 interface. | Connect to console port locally and delete the ACL. Use the **no ip access-group** or the **no ipv6 traffic-filter** CLI command in interface mode. |