CHAPTER 12

Configuring IP Services

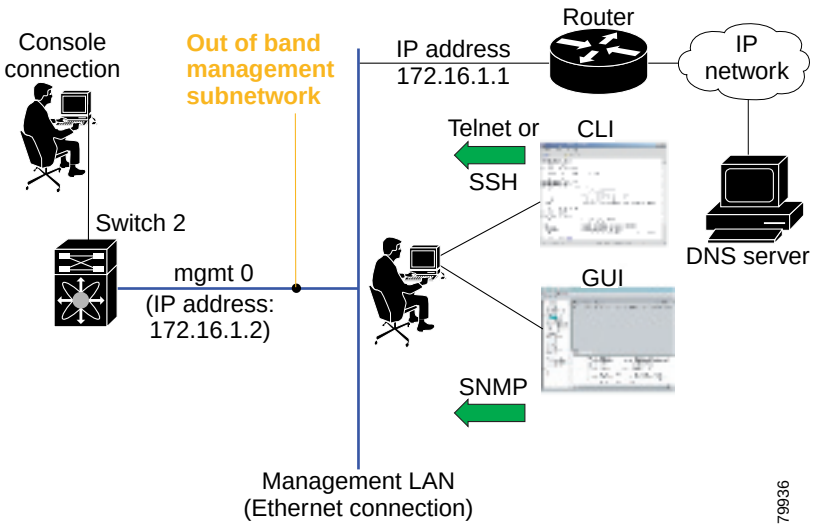
Cisco MDS 9020 Fabric Switches can route IP traffic between Ethernet and Fibre Channel interfaces.

This chapter includes the following sections:

Traffic Management Services

All traffic management is performed through the console connection or the mgmt0 Ethernet interface. (See Figure 12-1.)

Figure 12-1 Management Access to Switches



Management Interface Configuration

The management interface on the switch allows multiple simultaneous Telnet or SNMP sessions. You can remotely configure the switch through the management interface, but first you must configure some IP parameters (IP address, subnet mask) so that the switch is reachable. You can manually configure the management interface from the CLI.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

To configure the mgmt0 Ethernet interface, perform this task:

	Command	Purpose
Step 1	`switch# config terminal` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface mgmt0` `switch(config-if)#`	Enters the interface configuration mode on the management Ethernet interface (mgmt0).
Step 3	`switch(config-if)# ip address 10.1.1.1 255.255.255.0`	Enters the IP address (10.1.1.1) and IP subnet mask (255.255.255.0) for the management interface.
Step 4	`switch(config-if)# no shutdown`	Enables the interface.

Default Gateway Configuration

The default gateway IP address should be configured along with the IP static routing commands (IP default network, destination prefix, destination mask, and next hop address).

Tip If you configure the static route IP forwarding and the default-network details, these IP addresses will be used regardless of the default-gateway being enabled or disabled. If these IP addresses are configured but not available, the switch will fall back to using the default gateway IP address if you have configured it. Be sure to configure IP addresses for all entries in the switch.

See the "Initial Setup Routine" section on page 3-2 for more information on configuring the IP addresses for all entries in the switch.

Use the **IP default-gateway** command to configure the IP address for a switch's default gateway and the **show ip route** command to verify that the IP address for the default gateway is configured.

To configure default gateways, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip default-gateway 10.12.11.1`	Configures the IP address for the default gateway.

IP Access Control Lists

IP access control lists (IP-ACLs) enhance network security for Cisco MDS 9020 Fabric Switches. 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 whether the packet should be permitted or denied.

Each Cisco MDS 9020 Fabric Switch can have a maximum of 64 IP-ACLs, and each IP-ACL can have a maximum of 256 filters.

IP-ACL Configuration Guidelines

When configuring IP-ACLs in a Cisco MDS 9020 Fabric Switch, configure the order of conditions accurately. Because the IP-ACL filters are sequentially applied to the IP flows, only the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Filter Contents

An IP filter contains rules for matching an IP packet based on the protocol, address, port, ICMP type, and type of service (TOS).

Protocol Information

The protocol information is required in each filter. It identifies the IP name or number. You can specify the IP in one of two ways:

- Specify a number ranging from 0 to 255. This number represents the IP number.
- Specify the name of a protocol including, but not restricted to, Internet Protocol (IP, keyword **ip),** Transmission Control Protocol (TCP, keyword **tcp**), User Datagram Protocol (UDP, keyword **udp**), and Internet Control Message Protocol (ICMP, keyword **icmp**).

Address Information

The address information is required in each filter. It identifies the following details:

- Source: The address of the network or host from which the packet is being sent.
- Source-wildcard: The wildcard bits applied to the source.
- Destination: The number of the network or host to which the packet is being sent.
- Destination-wildcard: The wildcard bits applied to the destination.

You can specify the source and source-wildcard or the destination and destination-wildcard in one of two ways:

- Using 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 IP 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 IP address will be considered a match to this access list entry. Place ones in the bit positions that you want to ignore. 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 do not need to be contiguous in the source-wildcard. For example, a source-wildcard of 0.255.0.64 would be valid.
- Using 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).

Port Information

The port information is optional. 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. You can specify the port information in one of two ways:

- Specify the number of the port. Port numbers range from 0 to 65535. Table 12-1 displays the port numbers recognized by the Cisco MDS 9000 FabricWare software for associated TCP and UDP ports.
- Specify the name of a TCP or UDP port as follows:
  - TCP port names can only be used when filtering TCP.
  - UDP port names can only be used when filtering UDP.

Table 12-1 TCP and UDP Port Numbers

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 12-1 TCP and UDP Port Numbers (continued)

Protocol	Port	Number
TCP **Note** If the TCP connection is already established, use the **established** option to find matches. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, or URG control bit set.	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

ICMP Information

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

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

Table 12-2 displays the value for each ICMP type.

Table 12-2 ICMP Type Value

ICMP Type[1]	Code
echo	8
echo-reply	0
destination unreachable	3
traceroute	30
time exceeded	11

1. ICMP redirect packets are always rejected.

TOS Information

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

- The TOS level, as specified by a number from 0 to 15
- The TOS name: max-reliability, max-throughput, min-delay, min-monetary-cost, and normal

IP-ACL -Creation

Traffic coming into the switch is compared with IP-ACL filters based on the order that the filters occur in the switch. New filters are added to the end of the IP-ACL. The switch keeps looking until it has a match. If no matches are found when the switch reaches the end of the filter, the traffic is denied. For this reason, you should have the frequently hit filters at the top of the filter. There is an *implied deny* for traffic that is not permitted. A single-entry IP-ACL with only one **deny** entry has the effect of denying all traffic.

To configure an IP-ACL, you must complete the following tasks:

1. Create an IP-ACL by specifying a filter name and one or more access condition(s). Filters require the source and destination address to match a condition. Use optional keywords to configure finer granularity.
2. Apply the access filter to specified interfaces.

To create an IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit ip any any`	Configures an IP-ACL called List1 and permits IP traffic from any source address to any destination address.
	`switch(config)# no ip access-list List1 permit ip any any`	Removes the IP-ACL called List1.
Step 3	`switch(config)# ip access-list List1 deny tcp any any`	Updates List1 to deny TCP traffic from any source address to any destination address.

To define an IP-ACL that permits a specified network, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit udp 192.168.32.0 0.0.7.255 any`	Defines an IP-ACL that permits this network. Subtracting 255.255.248.0 (normal mask) from 255.255.255.255 yields 0.0.7.255.

To use the operand and port options, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any`	Denies TCP traffic from 10.2.3.0 through source port 5 to any destination.

Adding filters to an Existing IP-ACL

After you create an IP-ACL, you place subsequent additions at the end of the IP-ACL. You cannot insert filters in the middle of an IP-ACL. Each configured entry is automatically added to the end of an IP-ACL.

To add entries to an existing IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port telnet`	Permits TCP for Telnet traffic.
	`switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port http`	Permits TCP for HTTP traffic.
	`switch(config)# ip access-list List1 permit udp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0`	Permits UDP for all traffic.

Removing Entries from an Existing IP-ACL

To remove configured entries from an IP-ACL, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# no ip access-list List2 deny tcp 10.2.3.0 0.0.0.255 eq port 5 any`	Removes this entry from the IP-ACL.
	`switch(config)# no ip access-list x3 deny ip any any`	Removes this entry from the IP-ACL.
	`switch(config)# no ip access-list x3 permit ip any any`	Removes this entry from the IP-ACL.

Reading the IP-ACL Log Dump

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.

For the input ACL, the log displays the raw MAC information. The keyword **MAC=** does not refer to showing an Ethernet MAC frame with MAC address information. It refers to the Layer 2 MAC-layer information dumped to the log. For the output ACL, the raw Layer 2 information is not logged.

The following example shows an input ACL log dump:

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00:45:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

The following example is an output ACL log dump:

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

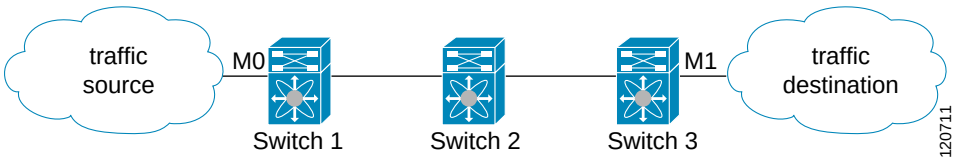
IP-ACL Interface Application

You can define IP-ACLs without applying them. However, the IP-ACLs will have no effect until they are applied to the switch's interface.

Tip Apply the IP-ACL on the interface closest to the source of the traffic.

When you are trying to block traffic from source to destination, you can apply an inbound IP-ACL to M0 on Switch 1 instead of an outbound filter to M1 on Switch 3. (See Figure 12-2.)

Figure 12-2 Denying Traffic on the Inbound Interface



The **access-group** option controls access to an interface. Each interface can only be associated with one access filter per direction. The ingress direction can have a different ACL than the egress direction. The access group becomes active on creation.

Tip Create all conditions in an access filter before creating the access group that uses this filter.

Caution If you create an access group before an access-filter, all packets in that interface are dropped because the access filter is empty.

The terms *in*, *out*, *source*, and *destination* are used as referenced by the switch.

- In—Traffic that is arriving on the interface and which will go through the switch; the source would be where it's been and the destination is where it's going (on the other side of the router).

Tip The access-group configuration for the ingress traffic applies to both local and remote traffic.

- Out—Traffic that has already been through the switch and is leaving the interface; the source would be where it's been (on the other side of the router) and the destination is where it's going.

Tip The access-group configuration for the egress traffic applies only to local traffic.

To create an access group, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch (config)# interface mgmt0`	Configures the management interface (mgmt0).
Step 3	`switch (config-if)#ip access-group SampleName`	Creates an access group called SampleName for both the ingress and egress traffic (default).
	`switch(config-if)# no ip access-group NotRequired`	Deletes the access group called NotRequired.
Step 4	`switch(config-if)# ip access-group SampleName1 in`	Creates an access group called SampleName (if it does not already exist) for ingress traffic.
	`switch(config-if)# no ip access-group SampleName1 in`	Deletes the access group called SampleName for ingress traffic.
	`switch(config-if)# ip access-group SampleName2 out`	Creates an access group called SampleName (if it does not already exist) for local egress traffic.
	`switch(config-if)# no ip access-group SampleName2 out`	Deletes the access group called SampleName for local egress traffic.

IP-ACL Configuration Verification

Use the **show ip access-list** command to view the contents of configured access filters. Each access filter can have several conditions. (See Examples 12-1 and 12-2.)

Example 12-1 Displays Configured IP-ACLs

```
switch# show ip access-list usage
Access List Name/Number          Filters IF   Status    Creation Time
-------------------------------- ------- ---- --------- -------------
abc                               3       7    active    Tue Jun 24 17:51:40 2003
x1                                3       1    active    Tue Jun 24 18:32:25 2003
x3                               0       1    not-ready Tue Jun 24 18:32:28 2003
```

Example 12-2 Displays a Summary of the Specified IP-ACL

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

IP-ACL Counter Cleanup

Use the **clear** command to clear the counters for a specified IP-ACL entry.

Note You cannot use this command to clear the counters for each individual filter.

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

Displaying IP Interface Information

Use the following **show** commands to view configured IP interface information. (See Examples 12-3 and 12-4.)

Example 12-3 Displays the Interface

```
switch# show interface mgmt0
mgmt0 is up
    Hardware is FastEthernet
    Internet address is 10.20.83.122/24
```

Example 12-4 Displays the Connected and Static Route Details

```
switch# show ip route
Codes: C - connected, S - static

Default gateway is 10.20.83.1

C 10.20.83.0/24 is directly connected, mgmt0
```