

Configuring IP Permit List

This chapter describes how to configure IP permit list on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding IP Permit List on page 27-1
- IP Permit List Default Configuration on page 27-2
- Configuring IP Permit List on page 27-2

Understanding IP Permit List

IP permit prevents inbound Telnet and SNMP access to the switch from unauthorized source IP addresses. All other Transmission Control Protocol/Internet Protocol (TCP/IP) services (such as IP traceroute and IP ping) continue to work normally when you enable the IP permit list. Outbound Telnet, Trivial File Transfer Protocol (TFTP), and other IP-based services are unaffected by the IP permit list.

Telnet attempts from unauthorized source IP addresses are denied a connection. SNMP requests from unauthorized IP addresses receive no response; the request times out. If you want to log unauthorized access attempts to the console or a syslog server, you must change the logging severity level for IP, as described in the “Enabling IP Permit List” section on page 27-3. If you want to generate SNMP traps when unauthorized access attempts are made, you must enable IP permit list (ippermit) SNMP traps, as described in the “Enabling IP Permit List” section on page 27-3. Multiple access attempts from the same unauthorized host only trigger notifications every ten minutes.

You can configure up to ten entries in the permit list. Each entry consists of an IP address and subnet mask pair in dotted decimal format. The bits set to one in the mask are checked for a match against the source IP address of incoming packets, while the bits set to zero are not checked. This process allows wildcard address specification.

If you do not specify the mask for an IP permit list entry, or if you enter a host name instead of an IP address, the mask has an implicit value of all bits set to one (255.255.255.255 or 0xffffffff), which matches only the IP address of that host.

You can specify the same IP address in more than one entry in the permit list if the masks are different. The mask is applied to the address before it is stored in NVRAM, so that entries that have the same effect (but different addresses) are not stored. When you add such an address to the IP permit list, the system displays the address after the mask is applied.

IP Permit List Default Configuration

Table 27-1 shows the default IP permit list configuration.

Table 27-1 IP Permit List Default Configuration

Feature	Default Value
IP permit list enable state	Disabled
Permit list entries	None configured
IP syslog message severity level	2
SNMP IP permit trap (ippermit)	Disabled

Configuring IP Permit List

These sections describe how to configure the IP permit list:

- Adding IP Addresses to the IP Permit List on page 27-2
- Enabling IP Permit List on page 27-3
- Clearing an IP Permit List Entry on page 27-4
- Disabling IP Permit List on page 27-4

Adding IP Addresses to the IP Permit List

To add IP addresses to the IP permit list, perform this task in privileged mode:

Task	Command
Step 1 Specify the IP addresses to add to the IP permit list.	set ip permit <i>ip_address</i> [<i>mask</i>]
Step 2 Verify the IP permit list configuration.	show ip permit

This example shows how to add IP addresses to the IP permit list and verify the configuration:

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0
172.16.0.0 with mask 255.255.0.0 added to IP permit list.
Console> (enable) set ip permit 172.20.52.32 255.255.255.224
172.20.52.32 with mask 255.255.255.224 added to IP permit list.
Console> (enable) set ip permit 172.20.52.3
172.20.52.3 added to IP permit list.
Console> (enable) show ip permit
IP permit list feature disabled.
Permit List      Mask
-----
172.16.0.0      255.255.0.0
172.20.52.3
172.20.52.32    255.255.255.224
```

```

Denied IP Address   Last Accessed Time   Type
-----
Console> (enable)

```

Enabling IP Permit List



Caution Before enabling the IP permit list, make sure you add the IP address of your workstation or network management system to the permit list, especially when configuring through SNMP. Failure to do so could result in your connection being dropped by the switch you are configuring. We recommend you disable the IP permit list before clearing IP permit entries or host addresses.

To enable IP permit list on the switch, perform this task in privileged mode:

Task	Command
Step 1 Enable the IP permit list.	set ip permit enable
Step 2 If desired, enable the IP permit trap to generate traps for unauthorized access attempts.	set snmp trap enable ippermit
Step 3 If desired, configure the logging level to see syslog messages for unauthorized access attempts.	set logging level ip 4 default
Step 4 Verify the IP permit list configuration.	show ip permit show snmp

This example shows how to enable IP permit list and verify the configuration:

```

Console> (enable) set ip permit enable
IP permit list enabled.
Console> (enable) set snmp trap enable ippermit
SNMP IP Permit traps enabled.
Console> (enable) set logging level ip 4 default
System logging facility <ip> set to severity 4(warnings)
Console> (enable) show ip permit
IP permit list feature enabled.
Permit List           Mask
-----
172.16.0.0            255.255.0.0
172.20.52.3           255.255.255.224
172.20.52.32         255.255.255.224

Denied IP Address   Last Accessed Time   Type
-----
171.68.180.16      07/16/98,00:00:38   Telnet
171.69.218.217    07/16/98,00:18:57   SNMP
Console> (enable) show snmp
RMON:                               Disabled
Extended Rmon:                     Extended RMON module is not present
Traps Enabled:
ippermit
Port Traps Enabled: None

Community-Access    Community-String
-----
read-only           public
read-write          private
read-write-all     secret

```

```
Trap-Rec-Address          Trap-Rec-Community
-----
Console> (enable)
```

Clearing an IP Permit List Entry



Caution We recommend you disable IP permit list before clearing IP permit entries or host addresses.

To clear an entry from the IP permit list, perform this task in privileged mode:

Task	Command
Step 1 Specify the IP address to remove from the IP permit list.	clear ip permit { <i>ip_address</i> [<i>mask</i>] all }
Step 2 Verify the IP permit list configuration.	show ip permit

This example shows how to clear an IP permit list entry:

```
Console> (enable) clear ip permit 172.16.0.0 255.255.0.0
172.16.0.0 with mask 255.255.0.0 cleared from IP permit list.
Console> (enable) clear ip permit all
IP permit list cleared.
Console> (enable)
```

Disabling IP Permit List

To disable IP permit list on the switch, perform this task in privileged mode:

Task	Command
Step 1 Disable IP permit list on the switch.	set ip permit disable
Step 2 Verify the IP permit list configuration.	show ip permit

This example shows how to disable IP permit list:

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```