



Configuring the IP Permit List

This chapter describes how to configure the IP permit list on the Catalyst 6500 series switches.



Note

The functionality of the IP permit list can also be achieved with VLAN access control lists (VACLs). Because VACLs are handled by hardware (Policy Feature Card [PFC]), VACL processing is considerably faster than IP permit list processing.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How the IP Permit List Works, page 34-1](#)
- [IP Permit List Default Configuration, page 34-2](#)
- [Configuring the IP Permit List on the Switch, page 34-2](#)

Understanding How the IP Permit List Works

The IP permit list prevents inbound Telnet and SNMP access to the switch from unauthorized source IP addresses. All other TCP/IP services (such as IP traceroute and IP ping) continue to work normally when you enable the IP permit list. Outbound Telnet, 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 the IP Permit List](#)” section on page 34-3. 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 the IP Permit List](#)” section on page 34-3. Multiple access attempts from the same unauthorized host only trigger notifications every 10 minutes.

You can configure up to 100 entries in the permit list. Each entry consists of an IP address and subnet mask pair in dotted decimal format and information on whether the IP address is part of the SNMP permit list, Telnet permit list, or both lists. The bits set to one in the mask are checked for a match with the source IP address of incoming packets, while the bits set to zero are not checked. This process allows you to specify a wildcard address.

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.

If you do not specify SNMP or Telnet for the type of permit list for the IP address, the IP address is added to both the SNMP and Telnet permit lists.

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 34-1 shows the default IP permit list configuration.

Table 34-1 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 the IP Permit List on the Switch

These sections describe how to configure the IP permit list:

- [Adding IP Addresses to the IP Permit List, page 34-2](#)
- [Enabling the IP Permit List, page 34-3](#)
- [Disabling the IP Permit List, page 34-4](#)
- [Clearing an IP Permit List Entry, page 34-4](#)

Adding IP Addresses to the IP Permit List

You can add an IP address to the SNMP permit list, the Telnet permit list, or both lists.

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>] [telnet snmp ssh]
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 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable) show ip permit
Telnet permit list feature enabled.
Snmp permit list feature enabled.
Permit List      Mask                Access Type
-----
172.16.0.0      255.255.0.0        telnet
172.20.52.3
172.20.52.32   255.255.255.224   snmp
Denied IP Address  Last Accessed Time Type      Telnet Count  SNMP Count
-----
172.100.101.104  01/20/97,07:45:20 SNMP      14            1430
172.187.206.222  01/21/97,14:23:05 Telnet    7             236

Console> (enable)

```

Enabling the IP Permit List

You can enable either the SNMP permit list, the Telnet permit list, or both lists. If you do not specify a permit list, both the SNMP and Telnet permit lists are enabled.



Caution

Before enabling the IP permit list, make sure that 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 that you disable the IP permit list before clearing IP permit entries or host addresses.

To enable the 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 [telnet snmp ssh]
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 the 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
Telnet permit list feature enabled.
Snmp permit list feature disabled.

Permit List           Mask           Access-Type
-----
172.16.0.0            255.255.0.0   telnet
172.20.52.3          255.255.255.224 snmp telnet
172.20.52.32         255.255.255.224 snmp

Denied IP Address    Last Accessed Time Type    Telnet Count    SNMP Count
-----
172.100.101.104     01/20/97,07:45:20 SNMP      14              1430
172.187.206.222     01/21/97,14:23:05 Telnet     7               236

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)

```

Disabling the IP Permit List

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

	Task	Command
Step 1	Disable the IP permit list.	set ip permit disable [telnet snmp ssh]
Step 2	Verify the IP permit list configuration.	show ip permit

This example shows how to disable the IP permit list:

```

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

```

Clearing an IP Permit List Entry

You can clear an IP address from the SNMP permit list, the Telnet permit list, or both lists. If you do not specify which permit list to clear the IP address from, the IP address is deleted from both permit lists.



Caution

Disable the IP permit list before you clear IP permit entries or host addresses to prevent your connection from being dropped by the switch you are configuring (in case you clear your current IP address).

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

	Task	Command
Step 1	Disable the IP permit list.	set ip permit disable [telnet snmp ssh]
Step 2	Specify the IP address to remove from the IP permit list.	clear ip permit {ip_address [mask] all} [telnet snmp ssh]
Step 3	Verify the IP permit list configuration.	show ip permit

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

```

Console> (enable) set ip permit disable all
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable) clear ip permit all
IP permit list cleared.
Console> (enable)

```

