13

Using Authorized IP Managers

Contents

Overview

Authorized IP Manager Features

Feature	Default	Menu	CLI	Web
Listing (Showing) Authorized Managers	n/a	page 13-5	page 13-6	page 13-9
Configuring Authorized IP Managers	None	page 13-5	page 13-6	page 13-9
Building IP Masks	n/a	page 13-9	page 13-9	page 13-9
Operating and Troubleshooting Notes	n/a	page 13-12	page 13-12	page 13-12

The Authorized IP Managers feature uses IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This covers access through the following means:

- Telnet and other terminal emulation applications
- The switch's web browser interface
- SNMP (with a correct community name)

Also, when configured in the switch, the Authorized IP Managers feature takes precedence over local passwords, TACACS+, RADIUS, Port-Based Access Control (802.1x), and Port Security. This means that the IP address of a networked management device must be authorized before the switch will attempt to authenticate the device by invoking any other access security features. If the Authorized IP Managers feature disallows access to the device, then access is denied. Thus, with authorized IP managers configured, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch's Authorized IP Managers configuration.

You can use Authorized IP Managers along with other access security features to provide a more comprehensive security fabric than if you use only one or two security options. Refer to

Options

You can configure:

- Up to 10 authorized manager *addresses*, where each address applies to either a single management station or a group of stations
- Manager or Operator access privileges (for Telnet, SNMPv1, and SNMPv2c access only)

Caution

Configuring Authorized IP Managers does not protect access to the switch through a modem or direct connection to the Console (RS-232) port. Also, if an unauthorized station "spoofs" an authorized IP address, it can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the username/password and other security features available in the switch, and preventing unauthorized access to data on your management stations.

Access Levels

Note

The Authorized IP Manager feature can assign an access level to stations using Telnet, SNMPv1, or SNMPv2c for switch access. The access level the switch allows for authorized stations using SSH, SNMPv3, or the web browser interface is determined by the access application itself, and not by the Authorized IP Manager feature.

For each authorized manager address using Telnet, SNMPv1, or SNMPv2c, you can configure either of these access levels:

- **Manager:** Enables full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces.
- **Operator:** Allows read-only access from the web browser and console interfaces. (This is the same access that is allowed by the switch's operator-level password feature.)

Defining Authorized Management Stations

- **Authorizing Single Stations:** The table entry authorizes a single management station to have IP access to the switch. To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP column, and leave the IP Mask set to **255.255.255.255**. This is the easiest way to use the Authorized Managers feature. (For more on this topic, see "Configuring One Station Per Authorized Manager IP Entry" on page 13-9.)
- **Authorizing Multiple Stations:** The table entry uses the IP Mask to authorize access to the switch from a defined group of stations. This is useful if you want to easily authorize several stations to have access to the switch without having to type in an entry for every station. All stations in the group defined by the one Authorized Manager IP table entry and its associated IP mask will have the same access level—Manager or Operator. (For more on this topic, refer to "Configuring Multiple Stations Per Authorized Manager IP Entry" on page 13-10.)

To configure the switch for authorized manager access, enter the appropriate *Authorized Manager IP* value, specify an *IP Mask*, and select either **Manager** or **Operator** for the *Access Level*. The IP Mask determines how the Authorized Manager IP value is used to allow or deny access to the switch by a management station.

Overview of IP Mask Operation

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter value. ("255" in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of **255.255.255.0** and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 254 IP addresses for IP management access (excluding 0 for the network and 255 for broadcasts). A mask of **255.255.255.252** uses the 4th octet of a given Autho-

rized Manager IP address to authorize four IP addresses for management station access. The details on how to use IP masks are provided under "Building IP Masks" on page 13-9.

Note

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

Menu: Viewing and Configuring IP Authorized Managers

From the console Main Menu, select:

2. Switch Configuration …

7. IP Authorized Managers

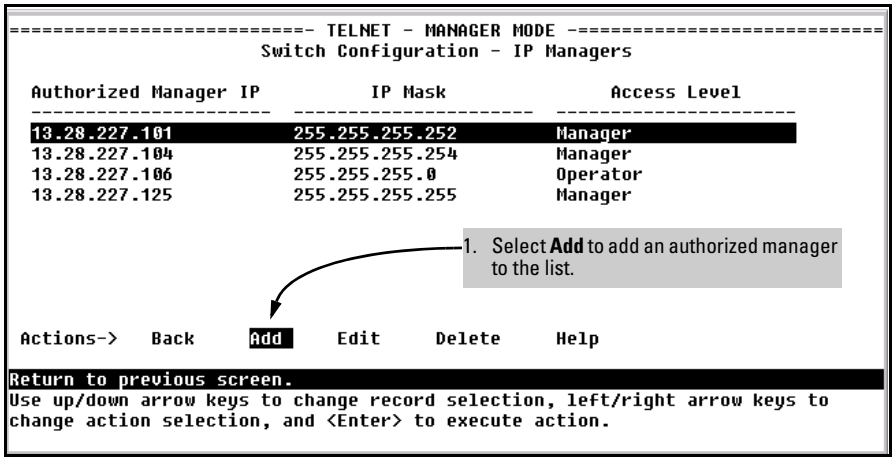

Figure 13-1. Example of How To Add an Authorized Manager Entry

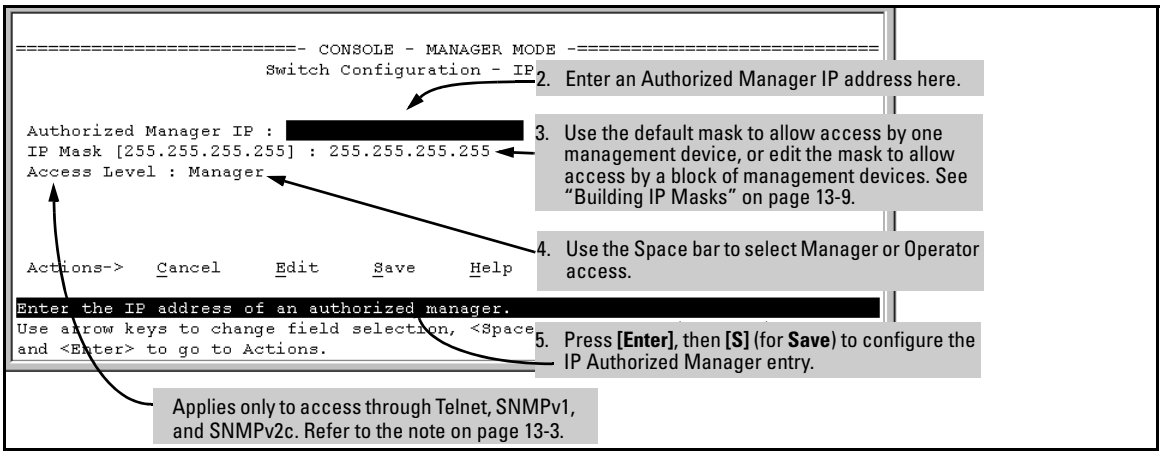

Figure 13-2. Example of How To Add an Authorized Manager Entry (Continued)

Editing or Deleting an Authorized Manager Entry. Go to the IP Managers List screen (figure 13-1), highlight the desired entry, and press **[E]** (for **Edit**) or **[D]** (for **Delete**).

CLI: Viewing and Configuring Authorized IP Managers

Authorized IP Managers Commands Used in This Section

Command	Page
show ip authorized-managers	below
ip authorized-managers	13-7
<ip-address>	13-8
mask *<mask-bits>*	13-8
<operator | manager>	

Listing the Switch's Current Authorized IP Manager(s)

Use the **show ip authorized-managers** command to list IP stations authorized to access the switch. For example:

```
ProCurve# show ip authorized-managers
 IP Managers
  Authorized Manager IP  IP Mask                 Access Level
  ---------------------- ---------------------- -------------
  10.28.227.101          255.255.255.252        Manager
  10.28.227.104          255.255.255.254        Manager
  10.28.227.125          255.255.255.255        Manager
  10.28.227.106          255.255.255.0          Operator
```

Figure 13-3.Example of the Show IP Authorized-Manager Display

The above example shows an Authorized IP Manager List that allows stations to access the switch as shown below:

IP Mask	Authorized Station IP Address:	Access Mode:
255.255.255.252	10.28.227.100 through 103	Manager
255.255.255.254	10.28.227.104 through 105	Manager
255.255.255.255	10.28.227.125	Manager
255.255.255.0	10.28.227.0 *through* 255	Operator

Configuring IP Authorized Managers for the Switch

Syntax: ip authorized-managers *<ip address>*

Configures one or more authorized IP addresses.

[*<ip-mask-bits>*]

Configures the IP mask for < ip address >

[access <operator | manager>]

Configures the privilege level for < ip address>. Applies only to access through Telnet, SNMPv1, and SNMPv2c. Refer to the Note on page 13-3.

To Authorize Manager Access. This command authorizes manager-level access for any station with an IP address of 10.28.227.0 through 10.28.227.255:

```
ProCurve(config)# ip authorized-managers 10.28.227.101
255.255.255.0 access manager
```

Similarly, the next command authorizes manager-level access for any station having an IP address of 10.28.227.101 through 103:

```
ProCurve(config)# ip authorized-managers 10.28.227.101
255.255.255.252 access manager
```

If you omit the < *mask bits* > when adding a new authorized manager, the switch automatically uses **255.255.255.255**. If you do not specify either Manager or Operator access, the switch assigns the Manager access. For example:

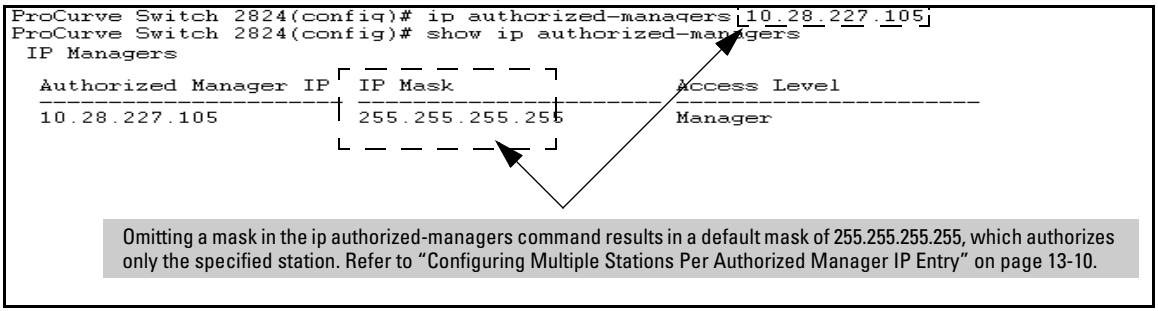

Figure 13-4. Example of Specifying an IP Authorized Manager with the Default Mask

To Edit an Existing Manager Access Entry. To change the mask or access level for an existing entry, use the entry's IP address and enter the new value(s). (Notice that any parameters not included in the command will be set to their default.):

```
ProCurve(config)# ip authorized-managers
      10.28.227.101 255.255.255.0 access operator
```

The above command replaces the existing mask and access level for IP address 10.28.227.101 with `255.255.255.0` and `operator`.

The following command replaces the existing mask and access level for IP address 10.28.227.101 with `255.255.255.255` and `manager` (the defaults) because the command does not specify either of these parameters.

```
ProCurve(config)# ip authorized-managers 10.28.227.101
```

To Delete an Authorized Manager Entry. This command uses the IP address of the authorized manager you want to delete:

```
ProCurve(config)# no ip authorized-managers 10.28.227.101
```

Web: Configuring IP Authorized Managers

In the web browser interface you can configure IP Authorized Managers as described below.

To Add, Modify, or Delete an IP Authorized Manager address:

1. Click on the **Security** tab.
2. Click on [Authorized Addresses].
3. Enter the appropriate parameter settings for the operation you want.
4. Click on [Add], [Replace], or [Delete] to implement the configuration change.

For web-based help on how to use the web browser interface screen, click on the **[?]** button provided on the web browser screen.

Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them by adding the address of each to the Authorized Manager IP list with **255.255.255.255** for the corresponding mask. For example, as shown in figure 13-3 on page 13-7, if you configure an IP address of **10.28.227.125** with an IP mask of **255.255.255.255**, only a station having an IP address of **10.28.227.125** has management access to the switch.

Figure 13-5. Analysis of IP Mask for Single-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	255	The "255" in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 10.33.248.5.
Authorized Manager IP	10	28	227	125	

Configuring Multiple Stations Per Authorized Manager IP Entry

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if **255** is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than **255**).

If a bit in an octet of the mask is "on" (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is "off" (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a "255" in an IP Mask octet (*all* bits in the octet are "on") means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorized Manager IP list. A "0" (all bits in the octet are "off") means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

Table 13-1. Analysis of IP Mask for Multiple-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	0	The "255" in the first three octets of the mask specify that only the exact value in the octet of the corresponding IP address is allowed. However, the zero (0) in the 4th octet of the mask allows any value between 0 and 255 in that octet of the corresponding IP address. This mask allows switch access to any device having an IP address of 10.28.227.*xxx*, where *xxx* is any value from 0 to 255.
Authorized Manager IP	10	28	227	125	
IP Mask	255	255	255	249	In this example (figure 13-2, below), the IP mask allows a group of up to 4 management stations to access the switch. This is useful if the only devices in the IP address group allowed by the mask are management stations. The "249" in the 4th octet means that bits 0 and 3 - 7 of the 4th octet are fixed. Conversely, bits 1 and 2 of the 4th octet are variable. Any value that matches the authorized IP address settings for the fixed bits is allowed for the purposes of IP management station access to the switch. Thus, any management station having an IP address of 10.28.227.121, 123, 125, or 127 can access the switch.
Authorized IP Address	10	28	227	125	

Table 13-2. Example of How the Bitmap in the IP Mask Defines Authorized Manager Addresses

4th Octet of IP Mask:	**249**							
4th Octet of Authorized IP Address:	**5**							
Bit Numbers	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
Bit Values	128	64	32	16	8	4	2	1
4th Octet of IP Mask (249)	■	■	■	■	■	□	□	■
4th Octet of IP Authorized Address (125)	□	■	■	■	■	■	□	■

Bits 1 and 2 in the mask are "off", and bits 0 and 3 - 7 are "on", creating a value of 249 in the 4th octet.

Where a mask bit is "on", the corresponding bit setting in the address of a potentially authorized station must match the IP Authorized Address setting for that same bit. Where a mask bit is "off" the corresponding bit setting in the address can be either "on" or "off". In this example, in order for a station to be authorized to access the switch:

- The first three octets of the station's IP address must match the Authorized IP Address.
- Bit 0 and Bits 3 through 6 of the 4th octet in the station's address must be "on" (value = 1).
- Bit 7 of the 4th octet in the station's address must be "off" (value = 0).
- Bits 1 and 2 can be either "on" or "off".

This means that stations with the IP address 13.28.227.*X* (where *X* is 121, 123, 125, or 127) are authorized.

Additional Examples for Authorizing Multiple Stations

	Entries for Authorized Manager List				**Results**
IP Mask	255	255	0	255	This combination specifies an authorized IP address of 10.33.*xxx*.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of "1" in the fourth octet of the station's IP address.
Authorized Manager IP	10	33	248	1	
IP Mask	255	238	255	250	Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet.
Authorized Manager IP	10	247	100	195	

Operating Notes

- **Network Security Precautions:** You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, using the additional security features described in this manual, and preventing unauthorized access to data on your management stations.
- **Modem and Direct Console Access:** Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.
- **Duplicate IP Addresses:** If the IP address configured in an authorized management station is also configured (or "spoofed") in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.
- **Web Proxy Servers:** If you use the web browser interface to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. *This reduces security by opening switch access to anyone who uses the web proxy server.* The following two options outline how to eliminate a web proxy server from the path between a station and the switch:
  - Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or "Exceptions" list in the web browser interface you are using on the authorized station.
  - If you don't need proxy server access at all on the authorized station, then just disable the proxy server feature in the station's web browser interface.