8

Configuring IP Addressing

Contents

Overview

You can configure IP addressing through all of the switch's interfaces. You can also:

- Easily edit a switch configuration file to allow downloading the file to multiple switches without overwriting each switch's unique gateway and VLAN 1 IP addressing.
- Assign up to 32 IP addresses to a VLAN (multinetting).
- Select an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Why Configure IP Addressing? In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by the ports on the switch. However, to enable specific management access and control through your network, you will need IP addressing. Table 8-1 on page 8-12 shows the switch features that depend on IP addressing to operate.

IP Configuration

IP Configuration Features

Feature	Default	Menu	CLI	Web
IP Address and Subnet Mask	DHCP/Bootp	page 8-5	page 8-7	page 8-11
Multiple IP Addresses on a VLAN	n/a	—	page 8-9	—
Default Gateway Address	none	page 8-5	page 8-7	page 8-11
Packet Time-To-Live (TTL)	64 seconds	page 8-5	page 8-7	—
Time Server (Timep)	DHCP	page 8-5	page 8-7	—
Single Source IP Addressing	outgoing IP address	—	page 8-25	—

IP Address and Subnet Mask. Configuring the switch with an IP address expands your ability to manage the switch and use its features. By default, the switch is configured to automatically receive IP addressing on the default VLAN from a DHCP/Bootp server that has been configured correctly with information to support the switch. (Refer to "DHCP/Bootp Operation" on page 8-12 for information on setting up automatic configuration from a server.) However, if you are not using a DHCP/Bootp server to configure IP addressing, use the menu interface or the CLI to manually configure the initial IP values. After you have network access to a device, you can use the web browser interface to modify the initial IP configuration if needed.

For information on how IP addressing affects switch operation, refer to "How IP Addressing Affects Switch Operation" on page 8-11.

Multinetting: Assigning Multiple IP Addresses to a VLAN. For a given VLAN you can assign up to 32 IP addresses. This allows you to combine two or more subnets on the same VLAN, which enables devices in the combined subnets to communicate normally through the network without needing to reconfigure the IP addressing in any of the combined subnets.

Default Gateway Operation. The default gateway is required when a router is needed for tasks such as reaching off-subnet destinations or forwarding traffic across multiple VLANs. The gateway value is the IP address of the next-hop gateway node for the switch, which is used if the requested destination address is not on a local subnet/VLAN. If the switch does not have a manually-configured default gateway and DHCP/Bootp is configured on the primary VLAN, then the default gateway value provided by the DHCP or Bootp server will be used. If the switch has a manually configured default gateway, then the switch uses his gateway, even if a different gateway is received via DHCP or Bootp on the primary VLAN. This is also true for manually configured TimeP, SNTP, and Time-To-Live(TTL). (In the default configuration, VLAN 1 is the Primary VLAN.) Refer to the information on Primary VLANs in the *Advanced Traffic Management Guide* for your switch.

Packet Time-To-Live (TTL) . This parameter specifies the maximum number of routers (hops) through which a packet can pass before being discarded. Each router decreases a packet's TTL by 1 before forwarding the packet. If decreasing the TTL causes the TTL to be 0, the router drops the packet instead of forwarding it. In most cases, the default setting (64) is adequate.

Just Want a Quick Start with IP Addressing?

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, ProCurve recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

- Enter `setup` at the CLI Manager level prompt.

```
ProCurve# setup
```

- Select **8. Run Setup** in the Main Menu of the menu interface.

For more on using the Switch Setup screen, refer to the *Installation and Getting Started Guide* you received with the switch.

IP Addressing with Multiple VLANs

In the factory-default configuration, the switch has one, permanent default VLAN (named DEFAULT_VLAN) that includes all ports on the switch. Thus, when only the default VLAN exists in the switch, if you assign an IP address and subnet mask to the switch, you are actually assigning the IP addressing to the DEFAULT_VLAN.

Notes

- If multiple VLANs are configured, then each VLAN can have its own IP address. This is because each VLAN operates as a separate broadcast domain and requires a unique IP address and subnet mask. A default gateway (IP) address for the switch is optional, but recommended.
- In the factory-default configuration, the default VLAN (named DEFAULT_VLAN) is the switch's *primary* VLAN. The switch uses the primary VLAN for learning the default gateway address. The switch can also learn other settings from a DHCP or Bootp server, such as (packet) Time-To-Live (TTL), and Timep or SNMP settings. (Other VLANs can also use DHCP or BootP to acquire IP addressing. However, the switch's gateway, TTL, and TimeP or SNTP values, which are applied globally, and not per-VLAN, will be acquired through the primary VLAN only, unless manually set by using the CLI, Menu, or web browser interface.(If these parameters are manually set, they will *not* be overwritten by alternate values received from a DHCP or Bootp server.) For more on VLANs, refer to the chapter titled "Static Virtual LANs" in the *Advanced Traffic Management Guide* for your switch.

- The IP addressing used in the switch should be compatible with your network. That is, the IP address must be unique and the subnet mask must be appropriate for your IP network.
- If you change the IP address through either Telnet access or the web browser interface, the connection to the switch will be lost. You can reconnect by either restarting Telnet with the new IP address or entering the new address as the URL in your web browser.

Menu: Configuring IP Address, Gateway, and Time-To-Live (TTL)

Do one of the following:

- To manually enter an IP address, subnet mask, set the **IP Config** parameter to **Manual** and then manually enter the IP address and subnet mask values you want for the switch.
- To use DHCP or Bootp, use the menu interface to ensure that the **IP Config** parameter is set to **DHCP/Bootp**, then refer to "DHCP/Bootp Operation" on page 8-12.

To Configure IP Addressing.

1. From the Main Menu, Select.

   2. Switch Configuration ...

   5. IP Configuration

Notes

If multiple VLANs are configured, a screen showing all VLANs appears instead of the following screen.

The Menu interface displays the IP address for any VLAN. If you use the CLI to configure the IP address on a VLAN, use the CLI **show ip** command to list them. (Refer to "Viewing the Current IP Configuration" on page 8-7.)

For descriptions of these parameters, see the online Help for this screen.

Before using the DHCP/ Bootp option, refer to "DHCP/Bootp Operation" on page 8-12.

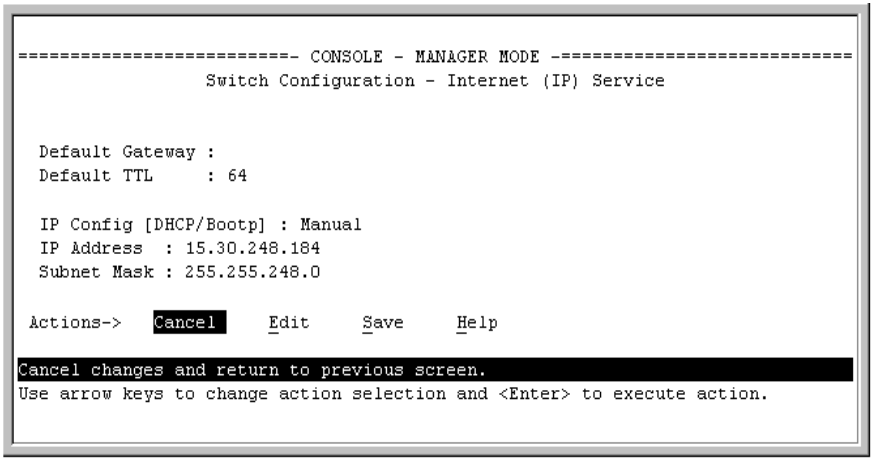

Figure 8-1. Example of the IP Service Configuration Screen without Multiple VLANs Configured

2. Press **[E]** (for **Edit**).
3. If the switch needs to access a router, for example, to reach off-subnet destinations, select the **Default Gateway** field and enter the IP address of the gateway router.
4. If you need to change the packet Time-To-Live (TTL) setting, select **Default TTL** and type in a value between 2 and 255.
5. To configure IP addressing, select **IP Config** and do one of the following:
   - If you want to have the switch retrieve its IP configuration from a DHCP or Bootp server, at the **IP Config** field, keep the value as **DHCP/ Bootp** and go to step 8.
   - If you want to manually configure the IP information, use the Space bar to select **Manual** and use the **[Tab]** key to move to the other IP configuration fields.
6. Select the **IP Address** field and enter the IP address for the switch.
7. Select the **Subnet Mask** field and enter the subnet mask for the IP address.
8. Press **[Enter]**, then **[S]** (for **Save**).

CLI: Configuring IP Address, Gateway, and Time-To-Live (TTL)

IP Commands Used in This Section	Page
show ip	8-7
ip address < *mask-length* >	8-8, 8-9
ip address /< *mask-bits* >	8-8, 8-9
ip default-gateway	8-10
ip ttl	8-11

Viewing the Current IP Configuration.

Syntax: show ip

This command displays the IP addressing for each VLAN configured in the switch. If only the DEFAULT_VLAN exists, then its IP configuration applies to all ports in the switch. Where multiple VLANs are configured, the IP addressing is listed per VLAN. The display includes switch-wide packet time-to-live, and (if configured) the switch's default gateway and Timep configuration.

(You can also use the **show management** command to display the IP addressing and time server IP addressing configured on the switch. Refer to figure 9-6 on page 9-11.)

For example, in the factory-default configuration (no IP addressing assigned), the switch's IP addressing appears as:

The Default IP Configuration

```
ProCurve> show ip
 Internet (IP) Service
  Default Gateway :
  Default TTL     : 64
  Arp Age         : 20

  TimeP Config : DHCP    TimeP Poll Interval (min) : 720

  VLAN         | IP Config  IP Address      Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | DHCP/Bootp
```

Figure 8-2. Example of the Switch's Default IP Addressing

With multiple VLANs and some other features configured, **show ip** provides additional information:

A Switch with IP Addressing and VLANs Configured

```
ProCurve> show ip
 Internet (IP) Service
  IP Routing : Disabled
  Default Gateway : 10.28.227.1
  Default TTL     : 64
  VLAN         | IP Config  IP Address      Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | Manual     10.28.227.101   255.255.248.0
  VLAN_2       | Disabled
```

Figure 8-3. Example of Show IP Listing with Non-Default IP Addressing Configured

Configure an IP Address and Subnet Mask. The following command includes both the IP address and the subnet mask. You must either include the ID of the VLAN for which you are configuring IP addressing or go to the context configuration level for that VLAN. (If you are not using VLANs on the switch—that is, if the only VLAN is the default VLAN—then the VLAN ID is always "1".)

Note

The default IP address setting for the DEFAULT_VLAN is **DHCP/Bootp**. On additional VLANs you create, the default IP address setting is **Disabled**.

Syntax: [no] vlan < *vlan-id* > ip address *<ip-address/mask-length>*
or
[no] vlan < *vlan-id* > ip address < *ip-address* > < *mask-bits* >
or
vlan < *vlan-id* > ip address *dhcp-bootp*

This example configures IP addressing on the default VLAN with the subnet mask specified in mask bits.

```
ProCurve(config)# vlan 1 ip address 10.28.227.103 255.255.255.0
```

This example configures the same IP addressing as the preceding example, but specifies the subnet mask by mask length.

```
ProCurve(config)# vlan 1 ip address 10.28.227.103/24
```

This example deletes an IP address configured in VLAN 1.

```
ProCurve (config) no vlan 1 ip address 10.28.227.103/24
```

Configure Multiple IP Addresses on a VLAN (Multinetting). The following is supported:

- Up to 2000 IP addresses for the switch
- Up to 32 IP addresses for the same VLAN
- Up to 512 IP VLANs, that is, VLANs on which you can configure IP addresses
- Each IP address on a VLAN must be for a separate subnet, whether on the same VLAN or different VLANs.

Syntax: [no] vlan < *vlan-id* > ip address < *ip-address/mask-length* >
[no] vlan < *vlan-id* > ip address < *ip-address* > < *mask-bits* >

For example, if you wanted to multinet VLAN_20 (VID = 20) with the IP addresses shown below, you would perform steps similar to the following. (For this example, assume that the first IP address is already configured.)

IP Address	VID	IP Address	Subnet Mask
1st address	20	10.25.33.101	255.255.240.0
2nd address	20	10.26.33.101	255.255.240.0
3rd address	20	10.27.33.101	255.255.240.0

1. Go to VLAN 20.
2. Configure two additional IP addresses on VLAN 20.
3. Display IP addressing.

```
ProCurve(config)# vlan 20
ProCurve(vlan-20)# ip address 10.26.33.101/20
ProCurve(vlan-20)# ip address 10.27.33.101/20

ProCurve(vlan-20)# show ip
 Internet (IP) Service
  IP Routing : Disabled

  Default Gateway :
  Default TTL     : 64
  Arp Age         : 20

  VLAN          | IP Config  IP Address       Subnet Mask
  ------------- + ---------- --------------- ---------------
  DEFAULT_VLAN  | Manual     10.20.30.100     255.255.240.0
  VLAN_20       | Manual     10.25.33.101     255.255.240.0
                | Manual     10.26.33.101     255.255.240.0
                | Manual     10.27.33.101     255.255.240.0
```

Figure 8-4. Example of Configuring and Displaying a Multinetted VLAN

If you then wanted to multinet the default VLAN, you would do the following:

```
ProCurve(vlan-20)# vlan 1
ProCurve(vlan-1)# ip address 10.21.30.100/20
ProCurve(vlan-1)# show ip

 Internet (IP) Service

  IP Routing : Disabled

  Default Gateway :
  Default TTL     : 64
  Arp Age         : 20

  VLAN          | IP Config  IP Address       Subnet Mask
  ------------- + ---------- --------------- ---------------
  DEFAULT_VLAN  | Manual     10.20.30.100    255.255.240.0
                | Manual     10.21.30.100    255.255.240.0
  VLAN_20       | Manual     10.25.33.101    255.255.240.0
                | Manual     10.26.33.101    255.255.240.0
                | Manual     10.27.33.101    255.255.240.0
```

Figure 8-5. Example of Multinetting on the Default VLAN

Note

The Internet (IP) Service screen in the Menu interface (figure 8-1 on page 8-6) displays the first IP address for each VLAN. You must use the CLI **show ip** command to display the full IP address listing for multinetted VLANs.

Removing or Replacing IP Addresses in a Multinetted VLAN. To remove an IP address from a multinetted VLAN, use the **no** form of the IP address command shown on page 8-9. Generally, to replace one IP address with another, you should first remove the address you want to replace, and then enter the new address.

Configure the Optional Default Gateway. Using the Global configuration level, you can manually assign one default gateway to the switch. (The switch does *not* allow IP addressing received from a DHCP or Bootp server to replace a manually configured default gateway.)

Syntax: ip default-gateway < *ip-address* >

For example:

```
ProCurve(config)# ip default-gateway 10.28.227.115
```

Note

The switch uses the IP default gateway only while operating as a Layer 2 device. While routing is enabled on the switch, the IP default gateway is not used. Thus, to avoid loss of Telnet access to off-subnet management stations, you should use the **ip route** command to configure a static (default) route before enabling routing. For more information, refer to the chapter titled "IP Routing Features" in the *Multicast and Routing Guide* for your switch.

Configure Time-To-Live (TTL). The maximum number of routers (hops) through which a packet can pass before being discarded. (The default is 64.) Each router decreases a packet's TTL by 1 before forwarding the packet. If a router decreases the TTL to 0, the router drops the packet instead of forwarding it.

Syntax: ip ttl *<number-of-hops>*

```
ProCurve(config)# ip ttl 60
```

In the CLI, you can execute this command only from the global configuration level. The TTL default is 64, and the range is 2 - 255.

Web: Configuring IP Addressing

You can use the web browser interface to access IP addressing only if the switch already has an IP address that is reachable through your network.

1. Click on the Configuration tab.
2. Click on **[IP Configuration]**.
3. If you need further information on using the web browser interface, click on **[?]** to access the web-based help available for the switch.

How IP Addressing Affects Switch Operation

Without an IP address and subnet mask compatible with your network, the switch can be managed only through a direct terminal device connection to the Console RS-232 port. You can use direct-connect console access to take advantage of features that do not depend on IP addressing. However, to realize the full capabilities ProCurve proactive networking offers through the switch, configure the switch with an IP address and subnet mask compatible with your network. The following table lists the general features available with and without a network-compatible IP address configured.

Table 8-1. Features Available With and Without IP Addressing on the Switch

Features Available Without an IP Address	Additional Features Available with an IP Address and Subnet Mask
• Direct-connect access to the CLI and the menu interface. • DHCP or Bootp support for automatic IP address configuration, and DHCP support for automatic Timep server IP address configuration • Multiple Spanning Tree Protocol • Port settings and port trunking • Switch meshing • Console-based status and counters information for monitoring switch operation and diagnosing problems through the CLI or menu interface. • VLANs and GVRP • Serial downloads of software updates and configuration files (Xmodem) • Link test • Port monitoring • Password authentication • Quality of Service (QoS) • Authorized IP manager security	• Web browser interface access, with configuration, security, and diagnostic tools, plus the Alert Log for discovering problems detected in the switch along with suggested solutions • SNMP network management access such as ProCurve Manager for network configuration, monitoring, problem-finding and reporting, analysis, and recommendations for changes to increase control and uptime • TACACS+, RADIUS, SSH, SSL, and 802.1X authentication • Multinetting on VLANs • Telnet access to the CLI or the menu interface • IGMP • TimeP and SNTP server configuration • TFTP download of configurations and software updates • Access Control Lists (ACLs) • IP routing, Multicast Routing • VRRP router redundancy • PIM-DM and PIM-SM • Radius • Ping test

DHCP/Bootp Operation

Overview. DHCP/Bootp is used to provide configuration data from a DHCP or Bootp server to the switch. This data can be the IP address, subnet mask, default gateway, Timep Server address, and TFTP server address. If a TFTP server address is provided, this allows the switch to TFTP a previously saved configuration file from the TFTP server to the switch. With either DHCP or Bootp, the servers must be configured prior to the switch being connected to the network.

Note The switches covered in this guide are compatible with both DHCP and Bootp servers.

The DHCP/Bootp Process. Whenever the **IP Config** parameter in the switch or in an individual VLAN in the switch is configured to **DHCP/Bootp** (the default), or when the switch is rebooted with this configuration:

1. DHCP/Bootp requests are automatically broadcast on the local network. (The switch sends one type of request to which either a DHCP or Bootp server can respond.)
2. When a DHCP or Bootp server receives the request, it replies with a previously configured IP address and subnet mask for the switch. The switch also receives an IP Gateway address if the server has been configured to provide one. In the case of Bootp, the server must first be configured with an entry that has the switch's MAC address. (To determine the switch's MAC address, refer to Appendix D, "MAC Address Management".) The switch properly handles replies from either type of server. If multiple replies are returned, the switch tries to use the first reply.)

Note

If you manually configure default gateway, TTL, TimeP, and/or SNTP parameters on the switch, it ignores any values received for the same parameters via DHCP or Bootp.

If the switch is initially configured for DHCP/Bootp operation (the default), or if it reboots with this configuration, it begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process immediately.

DHCP Operation. A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic. Depending on how the DHCP server is configured, the switch may receive an IP address that is temporarily leased. Periodically the switch may be required to renew its lease of the IP configuration. Thus, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. However, you can fix the address assignment for the switch by doing either of the following:

- Configure the server to issue an "infinite" lease.
- Using the switch's MAC address as an identifier, configure the server with a "Reservation" so that it will always assign the same IP address to the switch. (For MAC address information, refer to Appendix D, "MAC Address Management".)

For more information on either of these procedures, refer to the documentation provided with the DHCP server.

Bootp Operation. When a Bootp server receives a request it searches its Bootp database for a record entry that matches the MAC address in the Bootp request from the switch. If a match is found, the configuration data in the associated database record is returned to the switch. For many Unix systems, the Bootp database is contained in the **/etc/bootptab** file. In contrast to DHCP operation, Bootp configurations are always the same for a specific receiving device. That is, the Bootp server replies to a request with a configuration previously stored in the server and designated for the requesting device.

Bootp Database Record Entries. A minimal entry in the Bootp table file **/etc/bootptab** to update an IP address and subnet mask to the switch or a VLAN configured in the switch would be similar to this entry:

```
8212switch:\
   ht=ether:\
   ha=0030c1123456:\
   ip=10.66.77.88:\
   sm=255.255.248.0:\
   gw=10.66.77.1:\
   hn:\
   vm=rfc1048
```

An entry in the Bootp table file `/etc/bootptab` to tell the switch or VLAN where to obtain a configuration file download would be similar to this entry:

```
8212switch:\
   ht=ether:\
   ha=0030c1123456:\
   ip=10.66.77.88:\
   sm=255.255.248.0:\
   gw=10.66.77.1:\
   lg=10.22.33.44:\
   T144="switch.cfg":\
   vm=rfc1048
```

where:

8212switch	is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you should use a unique symbolic name for each switch.
ht	is the "hardware type". For the switches covered in this guide, enter **ether** (for Ethernet). *This tag must precede the* ha *tag*.
ha	is the "hardware address". Use the switch's (or VLAN's) 12-digit MAC address.
ip	is the IP address to be assigned to the switch (or VLAN).
sm	is the subnet mask of the subnet in which the switch (or VLAN) is installed.
gw	is the IP address of the default gateway.

lg	TFTP server address (source of final configuration file)
T144	is the vendor-specific "tag" identifying the configuration file to download.
vm	is a required entry that specifies the Bootp report format. Use **rfc1048** for the switches covered in this guide.

Note The above Bootp table entry is a sample that will work for the switch when the appropriate addresses and file names are used.

Network Preparations for Configuring DHCP/Bootp

In its default configuration, the switch is configured for DHCP/Bootp operation. However, the DHCP/Bootp feature will not acquire IP addressing for the switch unless the following tasks have already been completed:

- For Bootp operation:
  - A Bootp database record has already been entered into an appropriate Bootp server.
  - The necessary network connections are in place
  - The Bootp server is accessible from the switch
- For DHCP operation:
  - A DHCP scope has been configured on the appropriate DHCP server.
  - The necessary network connections are in place
  - A DHCP server is accessible from the switch

Note Designating a primary VLAN other than the default VLAN affects the switch's use of information received via DHCP/Bootp. For more on this topic, refer to the chapter describing VLANs in the *Advanced Traffic Management Guide* for your switch.

After you reconfigure or reboot the switch with DHCP/Bootp enabled in a network providing DHCP/Bootp service, the switch does the following:

- Receives an IP address and subnet mask and, if configured in the server, a gateway IP address and the address of a Timep server.
- If the DHCP/Bootp reply provides information for downloading a configuration file, the switch uses TFTP to download the file from the designated source, then reboots itself. (This assumes that the switch or VLAN has connectivity to the TFTP file server specified in the reply, that the configuration file is correctly named, and that the configuration file exists in the TFTP directory.)

Loopback Interfaces

This section describes how to configure and use user-defined loopback interfaces on the switch.

Introduction

By default, each switch has an internal loopback interface (**lo0**) with the IP address 127.0.0.1. This IP address is used only for internal traffic transmitted within the switch and is not used in packet headers in egress traffic sent to network devices.

You can configure up to seven other loopback interfaces (**lo1**, **lo2**, **lo3**, and so on) on the switch to use to transmit network across the network. Each loopback interface can have multiple IP addresses. Routing protocols, such as RIP and OSPF, advertise the configured loopback addresses throughout a network or autonomous system.

User-defined loopback addresses provide the following benefits:

- A loopback interface is a virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. As a result, a loopback interface is useful for debugging tasks since its IP address can always be pinged if any other switch interface is up.
- You can use a loopback interface to establish a Telnet session, ping the switch, and access the switch through SNMP, SSH, and HTTP (web interface).
- A loopback IP address can be used by routing protocols. For example, you can configure the loopback IP address as the router ID used to identify the switch in an OSPF area. Because the loopback interface is always up, you ensure that the switch's router ID remains constant and that the OSPF network is protected from changes caused by downed interfaces.

Note

OSPF does not require that you use an IP address as the router ID. OSPF only requires the router ID to be a unique value within the autonomous system (AS). However, if you configure the loopback IP address as the router ID, OSPF can reach the switch if any switch interface is up. (Normally, OSPF automatically configures the router ID with the IP address of a switch interface. The disadvantage is that if the interface goes down, OSPF can no longer ping the switch using the router ID even if other interfaces are operational.)

For more information about how to configure a loopback IP address to participate in an OSPF broadcast area, refer to the section titled "(Optional) Assigning Loopback Addresses to an Area" in the *Multicast and Routing Guide*.

Configuring a Loopback Interface

To configure a loopback interface, enter the **interface loopback** command at the global configuration level of the CLI:

Syntax: [no] interface loopback <*number*>

Creates a loopback interface, where <number> is a value from 1 to 7. Use the **no** *form of the command to remove the loopback interface.*

Note: *You cannot remove the default loopback interface (number 0) with IP address 127.0.0.1.*

You can configure up to thirty-two IP addresses on a loopback interface. To configure an IP address for the loopback interface, enter the **ip address < *ip-address* >** command at the loopback interface configuration level as shown in the following example.

Note that when you configure an IP address for a loopback interface, you do not specify a network mask. The default subnet mask 255.255.255.255 is used.

```
ProCurve(config)# interface loopback 1
ProCurve (lo1)# ip address 10.1.1.1
```

Figure 8-6. Example of a Loopback Interface Configuration

Notes

- You can configure a loopback interface only from the CLI; you cannot configure a loopback interface from the web management or Menu interface.
- Loopback interfaces share the same IP address space with VLAN configurations. The maximum number of IP addresses supported on a switch is 2048, which includes all IP addresses configured for both VLANs and loopback interfaces (except for the default loopback IP address 127.0.0.1).
- Each IP address that you configure on a loopback interface must be unique in the switch. This means that the address cannot be used by a VLAN interface or another loopback interface.

For example, if you configure a VLAN with IP address 172.16.100.8/24, you cannot configure a loopback interface with IP address 172.16.100.8. In the same way, if you configure a loopback interface (**lo1**) with IP address 172.16.101.8, you cannot configure another loopback interface (**lo2**) with IP address 172.16.101.8.

- You can configure multiple IP addresses on a loopback interface (**lo0** to **lo7**). Up to thirty-two IP addresses are supported on a loopback interface. The following example shows valid IP address configurations on two loopback interfaces.

```
ProCurve(config)# interface loopback 0
ProCurve (lo0)# ip address 172.16.101.8
ProCurve (lo0)# ip address 172.16.101.9
ProCurve (lo0)# exit
ProCurve (config)# interface loopback 1
ProCurve (lo1)# ip address 172.16.102.1
ProCurve (lo1)# ip address 172.16.102.2
```

Displaying Loopback Interface Configurations

To display the list of loopback interfaces which have been assigned IP addresses, enter the **show ip** command.

In the **show ip** command output, information about configured loopback interfaces is displayed below other IP configuration parameters, such as packet time-to-live (TTL) and ARP age-out values, and VLAN IP configurations. The following example displays the IP addresses configured for two user-defined loopback interfaces (**lo1** and **lo2**).

```
ProCurve> show ip

Internet (IP) Service

IP Routing : Enabled
Default TTL : 64
ARP Age : 20


 VLAN        IP Config IP Address Subnet Mask Proxy ARP
--------     --------- ---------- ----------  -------
DEFAULT_VLAN   Manual 10.0.8.121   255.255.0.0    No
VLAN2          Manual 192.168.12.1 255.255.255.0  No
VLAN3          Disabled

              Loopback Addresses
Loopback     IP Config   IP Address   Subnet Mask
--------    ----------  ----------    --------------
lo1          Manual      172.16.110.2  255.255.255.255
lo2          Manual      172.16.112.2  255.255.255.255
lo2          Manual      172.16.114.1  255.255.255.255
```

Figure 8-7. Example of show ip Command Output

Note

The default loopback interface (**lo0**) with IP address 127.0.0.1 is not displayed in the **show ip** command output because it is permanently configured on the switch. To display the default loopback address, enter the **show ip route** command as shown in figure 8-8.

To display the loopback interfaces configured on the switch in a list of IP routing entries displayed according to destination IP address, enter the **show ip route** command.

The following example displays the configuration of the default loopback interface (**lo0**) and one user-defined loopback interface (**lo2**).

```
ProCurve> show ip route

IP Route Entries

IP Routing : Enabled
Default TTL : 64
ARP Age : 20


Destination     Gateway      VLAN Type     Metric  Dist
-----------     ----------   ---- ------   -----   ---
10.0.0.0/16     DEFAULT_VLAN  1   connected   1     0
127.0.0.0/8      reject           static      0     0
127.0.0.1/32     lo0              connected   1     0
172.16.10.121/32 lo2              static      1     0
172.16.100.0/24  10.0.8.11    1   ospf        1     1
172.16.102.0/24  VLAN2        2   connected   1     0
```

Figure 8-8. Example of show ip route Command Output

IP Preserve: Retaining VLAN-1 IP Addressing Across Configuration File Downloads

For the switches covered in this guide, IP Preserve enables you to copy a configuration file to multiple switches while retaining the individual IP address and subnet mask on VLAN 1 in each switch, and the Gateway IP address assigned to the switch. This enables you to distribute the same configuration file to multiple switches without overwriting their individual IP addresses.

Operating Rules for IP Preserve

When **ip preserve** is entered as the last line in a configuration file stored on a TFTP server:

- If the switch's current IP address for VLAN 1 was not configured by DHCP/Bootp, IP Preserve retains the switch's current IP address, subnet mask, and IP gateway address when the switch downloads the file and reboots. The switch adopts all other configuration parameters in the configuration file into the startup-config file.
- If the switch's current IP addressing for VLAN 1 is from a DHCP server, IP Preserve is suspended. In this case, whatever IP addressing the configuration file specifies is implemented when the switch downloads the file and reboots. If the file includes DHCP/Bootp as the IP addressing source for VLAN 1, the switch will configure itself accordingly and use DHCP/Bootp. If instead, the file includes a dedicated IP address and subnet mask for VLAN 1 and a specific gateway IP address, then the switch will implement these settings in the startup-config file.
- The **ip preserve** statement does not appear in **show config** listings. To verify IP Preserve in a configuration file, open the file in a text editor and view the last line. For an example of implementing IP Preserve in a configuration file, see figure 8-9, below.

Enabling IP Preserve

To set up IP Preserve, enter the **ip preserve** statement at the end of a configuration file. (Note that you do not execute IP Preserve by entering a command from the CLI).

```
; J8697A Configuration Editor; Created on release #K.12.00
hostname "ProCurve"
time daylight-time-rule None
  .
  .
  .
  .
password manager
password operator
ip preserve
```

Entering "ip preserve" in the last line of a configuration file implements IP Preserve when the file is downloaded to the switch and the switch reboots.

Figure 8-9. Example of Implementing IP Preserve in a Configuration File

For example, consider figure 8-10:

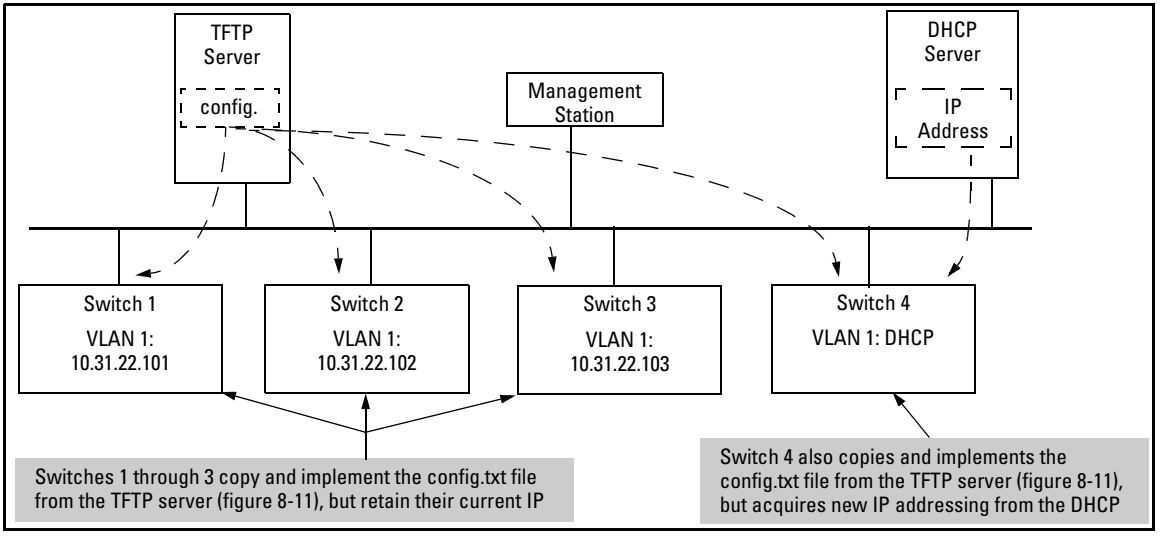

Figure 8-10. Example of IP Preserve Operation with Multiple Series Switches

If you apply the following configuration file to figure 8-10, switches 1 - 3 will retain their manually assigned IP addressing and switch 4 will be configured to acquire its IP addressing from a DHCP server.

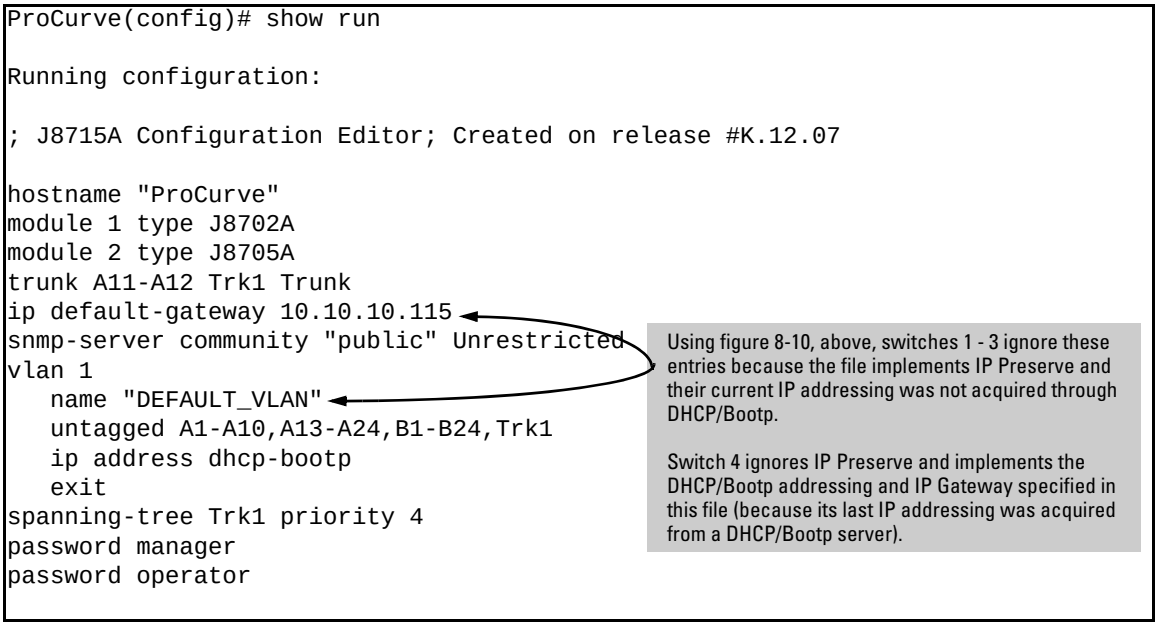

Figure 8-11. Configuration File in TFTP Server, with DHCP/Bootp Specified as the IP Addressing Source

If you apply this configuration file to figure 8-10, switches 1 - 3 will still retain their manually assigned IP addressing. However, switch 4 will be configured with the IP addressing included in the file.

```
ProCurve# show run

Running configuration:

; J8715A Configuration Editor; Created on release #K.12.07

hostname "ProCurve"
module 1 type J8702A
module 2 type J8705A
trunk A11-A12 Trk1 Trunk
ip default-gateway 10.10.10.115
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1,A7-A10,A13-A24,B1-B24,Trk1
   ip address 10.12.17.175 255.255.255.0
   tagged A4-A6
   no untagged A2-A3
   exit
vlan 2
   name "VLAN2"
   untagged A2-A3
   no ip address
   exit
spanning-tree Trk1 priority 4
password manager
password operator
```

Because switch 4 (figure 8-10) received its most recent IP addressing from a DHCP/Bootp server, the switch ignores the **ip preserve** command and implements the IP addressing included in this file.

Figure 8-12. Configuration File in TFTP Server, with Dedicated IP Addressing Instead of DHCP/Bootp

To summarize the IP Preserve effect on IP addressing:

- If the switch received its most recent VLAN 1 IP addressing from a DHCP/Bootp server, it ignores the IP Preserve command when it downloads the configuration file, and implements whatever IP addressing instructions are in the configuration file.
- If the switch did not receive its most recent VLAN 1 IP addressing from a DHCP/Bootp server, it retains its current IP addressing when it downloads the configuration file.
- The content of the downloaded configuration file determines the IP addresses and subnet masks for other VLANs.

Configuring a Single Source IP Address

Overview

This feature applies to the following software applications:

- TACACS
- RADIUS
- System Logging applications

The above IP-based software applications use a client-server communication model, that is, the client's source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Specifying the Source IP Address

The CLI command **ip source-interface** is used to specify the source IP address for an application. Different source IP addresses can be used for different software applications, but only one source IP address can be specified for each application.

.

Syntax: [no] ip source-interface <radius | tacacs | logging | all> <loopback <*id*> | vlan <*vlan-id*> address <*ip-address*>>

Determines the source IP address used by the specified software application when transmitting IP packets. The **all** *parameter can be used to set one IP address for all the listed applications, in this case, RADIUS, TACACS, and System Logging.*

The **no** *version of the command cancels the configuration and the application reverts to its default behavior. The system determines the source IP address of outgoing application-specific IP packets at packet transmission time.*

loopback <*id*>: *Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

vlan <*vlan-id*>: *Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

address <*ip-address*>: *Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.*

The Source IP Selection Policy

The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- Outgoing Interface—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.

- Configured IP Address—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- Configured IP Interface—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed. The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy (See figure 8-13).

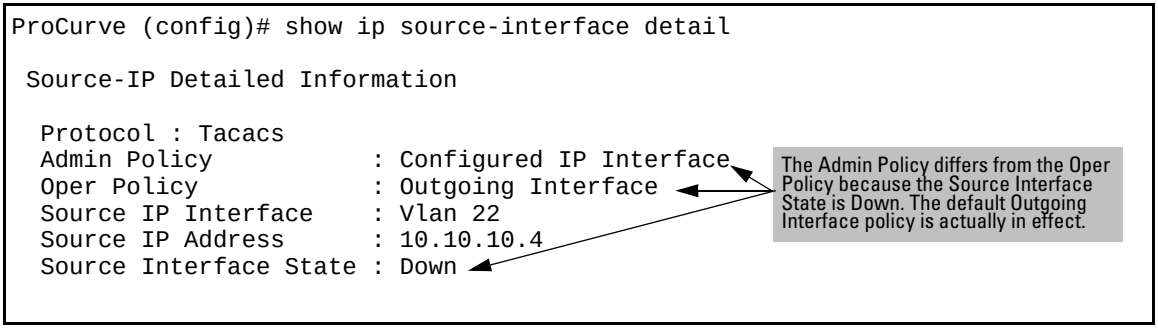

Figure 8-13. Example of the Administratively-assigned Source IP Selection Policy Differing From the Operational Policy

The **no** form of the **ip source-interface** command reverts the application protocols to the default behavior. The Outgoing Interface policy is used.

Figure 8-14 is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

```
ProCurve(config)# ip source-interface radius address 10.10.10.2

ProCurve(config)# show ip source-interface radius

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Radius   | Configured IP Address   vlan 3         10.10.10.2
```

Figure 8-14. Example of a Specific IP Address Assigned for the RADIUS Application Protocol

In figure 8-15, a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface tacacs vlan 22

ProCurve(config)# show ip source-interface tacacs

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22        10.10.10.4
```

Figure 8-15. Example of Using a VLAN Interface as the Source IP Address for TACACS

Figure 8-16 shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface syslog vlan 10

ProCurve(config)# show ip source-interface syslog

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 8-16. Example of Using a VLAN Interface as the Source IP Address for Logging (Syslog)

Displaying the Source IP Interface Information

There are several **show** commands that can be used to display information about the source IP interface status.

Syntax: show ip source-interface status [radius | tacacs | syslog]

Displays the operational status information for the source IP address selection policy. Both the administratively-assigned source IP selection policy and the operational source IP selection policy are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface status

 Source-IP Status Information

  Protocol | Admin Selection Policy  Oper Selection Policy
  -------- + ---------------------- ----------------------
  Tacacs   | Configured IP Interface Configured IP Interface
  Radius   | Configured IP Address   Configured IP Address
  Syslog   | Configured IP Interface Outgoing Interface
```

Figure 8-17. Example of the Data Displayed for Source IP Interface Status

When executing the **show ip source-interface** command without parameters, the configured IP interfaces (VLANs) and IP addresses are displayed for each protocol.

```
ProCurve(config)# show ip source-interface

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ---------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 22        10.10.10.4
  Radius   | Configured IP Address   vlan 3         10.10.10.2
  Syslog   | Configured IP Interface vlan 10        10.10.10.10
```

Figure 8-18. Example of show ip source-interface Command Output

The **show ip source-interface detail** command displays detailed information about the configured policies, source IP address, and interface state for each protocol.

Syntax: show ip source-interface detail [radius | tacacs | syslog]

Displays detailed operational status information for the source IP address selection policy. Information about the configured policies, source IP address and interface state are displayed.

When no parameters are specified, policy information for all protocols is displayed.

```
ProCurve(config)# show ip source-interface detail

 Source-IP Detailed Information

  Protocol : Tacacs
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 22
  Source IP Address      : 10.10.10.4
  Source Interface State : Up

  Protocol : Radius
  Admin Policy           : Configured IP Address
  Oper Policy            : Configured IP Address
  Source IP Interface    : vlan 3
  Source IP Address      : 10.10.10.2
  Source Interface State : Up

  Protocol : Syslog
  Admin Policy           : Configured IP Interface
  Oper Policy            : Configured IP Interface
  Source IP Interface    : vlan 10
  Source IP Address      : 10.10.10.10
  Source Interface State : Up
```

Figure 8-19. Example of Detailed Information Displayed for Each Protocol

The **show** command can also be used with the application to display the source IP address selection information in effect for the application protocol.

```
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Configured IP address
```

Source IP Selection for the specified application protocol is displayed.

Figure 8-20. Example of show radius Command Displaying Source IP Selection Information

```
ProCurve(config)# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : Configured IP Interface
  Encryption Key :
```

Source IP Selection for the specified application protocol is displayed.

Figure 8-21. Example of show tacacs Command Displaying Source IP Selection Information

```
ProCurve(config)# show debug

Debug Logging

  Source IP Selection: Configured IP interface
  Destination:    None

  Enabled debug types:
   None are enabled.
```

Source IP Selection for the specified application protocol is displayed.

Figure 8-22. Example of show debug Command Displaying Source IP Selection Information for Syslog

Error Messages

The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down.	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.