14

Using the Web Browser Interface for Basic Configuration Tasks

Contents

Configuring Access to the Web Browser Interface

You can use the Web browser interface to configure interfaces on your router. To access the Web browser interface, you must first use the command line interface (CLI) to enable the HTTP server on the ProCurve Secure Router and to configure a username and password for HTTP access.

You must also configure at least one interface on the ProCurve Secure Router and establish a connection through which you can send HTTP traffic. For example, if you want to access the router from a workstation on your WAN, you must configure the Ethernet interface and establish a connection between it and your LAN. (For information about setting up an Ethernet interface, see *Chapter 3: Configuring Ethernet Interfaces*.)

Enabling Access to the Web Browser Interface

From the global configuration mode context, enter:

```
ProCurve(config)# ip http server
```

If you want to use Secure Sockets Layer (SSL) to protect the communication between your workstation and the router, enter:

```
ProCurve(config)# ip http secure-server
```

In either case, you must then configure a username and password, which will also be used for HTTP, Secure Shell (SSH), and FTP access. From the global configuration mode context, enter:

Syntax: username <*username*> password <*password*>

Both the username and password can be an alphanumeric string up to 30 characters in length. In addition, both are case-sensitive.

After configuring the ProCurve Secure Router for HTTP access, open an Internet browser and enter the IP address assigned to the router interface through which you want to establish an HTTP session. For example, if you want to access the router from your LAN and the IP address of the Ethernet 0/1 interface is 192.168.1.1, you would enter: http://192.168.1.1.You will be prompted to enter the username and password that you configured for HTTP access.

The Web Browser Interface Navigation Bar

The Web browser interface features a navigation bar, containing available commands grouped by category. (See Figure 14-1.) The navigation bar is always visible on the left side of the browser screen. Selecting a command takes you to the associated screen(s) where you can view or modify settings on your ProCurve Secure Router. Although the instructions in this guide often refer to the navigation bar, it is not included in the illustrations.

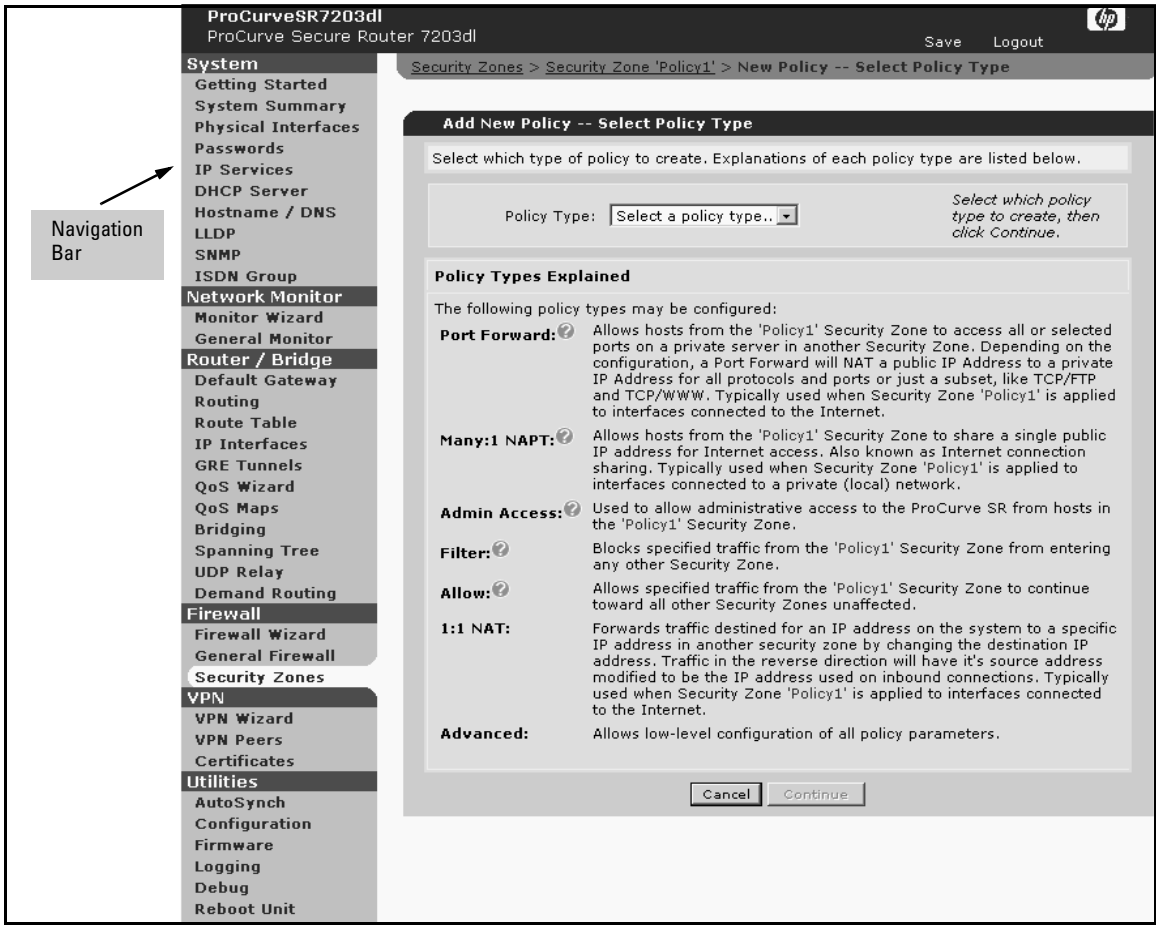

Figure 14-1. Navigation Bar in the Web Browser Interface

Managing Files, Firmware, Boot Software, and the AutoSynch™ Function

In the *Utilities* section of the Web browser interface, you can do basic file management tasks, manage the AutoSynch function, and set the router's firmware and boot software using the Web browser interface.

The *Utilities* section of the Web browser interface includes the following subsections:

- AutoSynch
- Configuration
- Firmware
- Logging
- Debug
- Reboot Unit
- Telnet to Unit

The *AutoSynch* section allows you to enable the AutoSynch technology and force synchronization. For more information about AutoSynch functions, see *Chapter 1: Overview*.

The *Configuration* section allows you to create and manage configuration files.

In the *Firmware* section, you can configure the router's primary and backup firmware files, view the drive space that is used and free on the router's internal flash and compact flash memories, upload, and delete firmware files.

The *Logging* section lets you configure the event-history log of events logged by the Secure Router OS firewall.

The *Debug* section lets you activate debug messages that provide real-time troubleshooting information about the activity of certain interfaces, protocols, and operations on the router.

The *Reboot Uni*t section provides two options for rebooting the router: save and reboot or reboot without saving.

The *Telnet to Unit* section opens a terminal session on your PC and begins to negotiate a Telnet session between your PC and the router.

The AutoSynch™ Feature

1. To manage the AutoSynch™ feature in the Web browser interface, click *AutoSynch* in the *Utilities* section of the navigation bar. The *AutoSynch Mode* window is displayed. From this window, you can enable the AutoSynch function, force synchronization, and troubleshoot AutoSynch operation.
2. To enable the AutoSynch™ technology, click the *AutoSynch Mode* box.
3. Click *Apply*. This will signal the AutoSynch™ function to begin synchronization efforts.

Note

The AutoSynch™ function is a feature that allows the router to maintain exact, up-to-date copies of the boot code and startup-config files on the router's internal flash and a mounted compact flash card. The AutoSynch feature is not available for routers without a mounted compact flash card.

AutoSynch technology will work only if you have a copy of the router's boot code file (SROS.BIZ) and a startup-config file on your compact flash card.

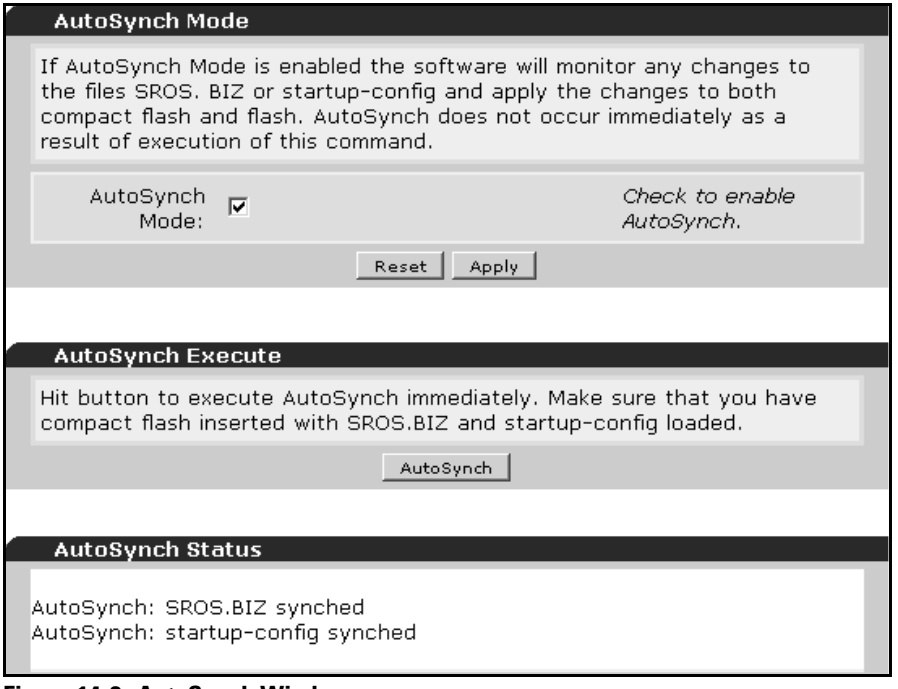

Figure 14-2. AutoSynch Window

4. When the AutoSynch™ function is enabled, you can force synchronization by clicking the *AutoSynch* button in the *AutoSynch Execute* window. The following dialog box is displayed:

   "You are about to activate AutoSynch. Continue?"

5. Click the *OK* button. The boot code file and the startup-config file will be copied from internal flash to compact flash, and synchronization will begin.

The *AutoSynch Status* window displays AutoSynch™ messages, such as the current synchronization status of the software (SROS.BIZ) file and startup-config file and any AutoSynch™ error messages. For a list of AutoSynch™ error messages and troubleshooting methods, see "AutoSynch™ Technology" on page 1-34.

Configuration

The configuration section supports basic configuration file management.

Startup-Config. The *Startup-Config* section allows you to set the primary and secondary startup-config files. The startup-config file contains your router's saved configurations. If you have more than one startup configuration on internal flash or compact flash, you can set the router to boot from the file you want and from the location you specify.

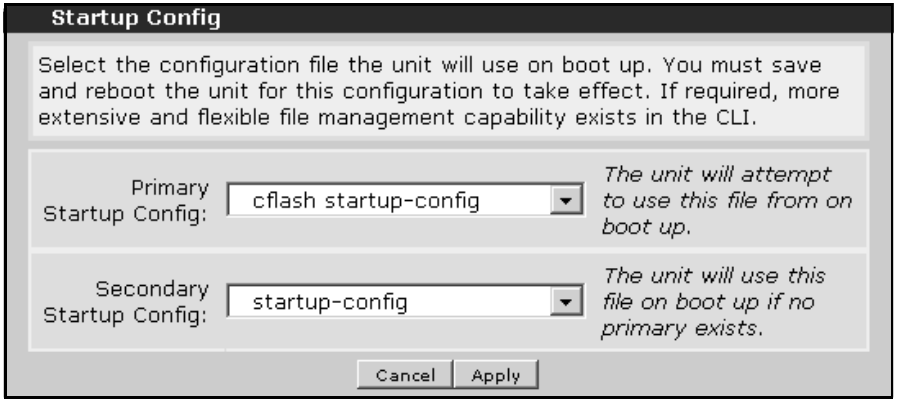

Figure 14-3. Startup Config Window

When the ProCurve Secure Router boots, it looks for the boot code software on the internal flash. After the ProCurve Secure Router locates the boot code and begins to boot, it looks on compact flash for a valid startup-config file. If the router cannot find a valid startup-config on compact flash, it looks on the internal flash memory for a valid file.

1. To set the primary startup config file, click the pull-down menu. A list of configuration files on the internal flash memory (and compact flash if installed) is displayed.
2. Click the file you want the router to use to boot.
3. To set the secondary startup config file, click the desired configuration file from the pull-down menu.
4. To save these changes to the running-config file, click *Apply*.

Note

If the AutoSynch function is enabled, the primary and backup startup-config files and locations are automatically set and cannot be changed.

Save-Config. The *Save-Config* window allows you to save the running-config file to the startup-config file. The current configurations will be saved, and the router can then boot with these configurations after it is powered down.

Click the *Save* button. If the AutoSynch feature is enabled, the running-config is saved as startup-config on both the internal flash memory and the compact flash card.

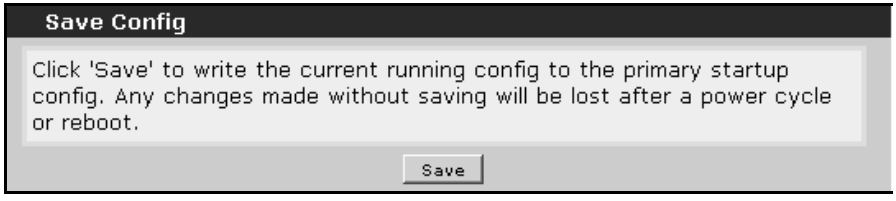

Figure 14-4. Save Config

Download Config. The *Download Config* section allows you to save the startup-config to a file on your PC. This feature is particularly useful when you must configure several routers with similar settings and you need to edit the configuration to tailor it to another router.

Figure 14-5. Download Config

1. Click the *Download* button. The *File Download* window with the *Open*, *Save*, *Cancel*, and *More Info* buttons is displayed. The file is automatically named <*hostname*>-<*date*>.cfg. For example, if you configured your router's hostname as HQRouter and today's date were May 5, 2007, the filename would be HQRouter-05-05-2007.cfg.
2. Click *Save*. The *Save As* dialog box is displayed.
3. Locate the folder where you want to save the file and click *Save*.

After you have downloaded the configuration file onto your PC, you can open and edit it in a text editor program such as Notepad.

Upload Config. The *Upload Config* section allows you to upload a configuration file from your PC.

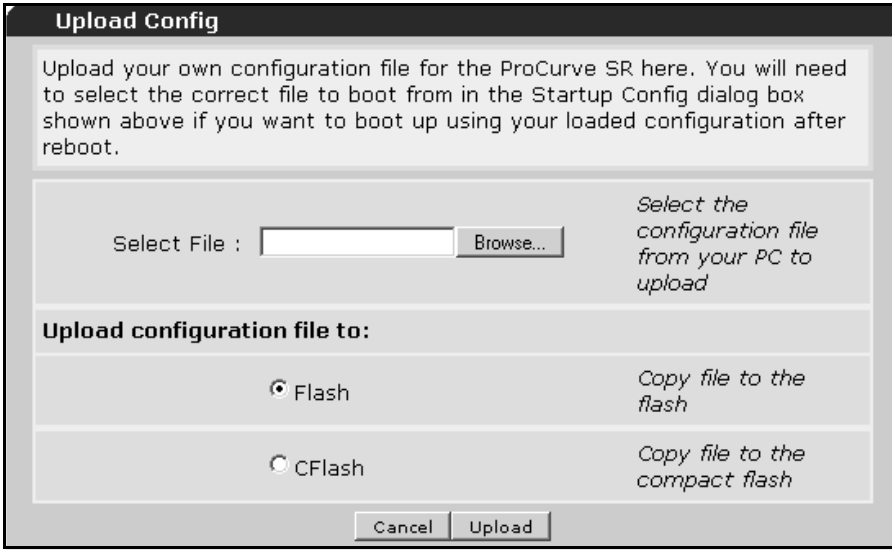

Figure 14-6. Upload Config

1. Click the *Browse…* button next to the *Select File* box and choose the file you want to upload.
2. Select either *Flash* or *CFlash* to specify the destination location for the file.
3. To upload the file, click the *Upload* button at the bottom of the window. The file is uploaded to your router.

Delete Config File. If you have an old or outdated configuration file or if you need the room on your router's flash or cflash memory, you can delete the file.

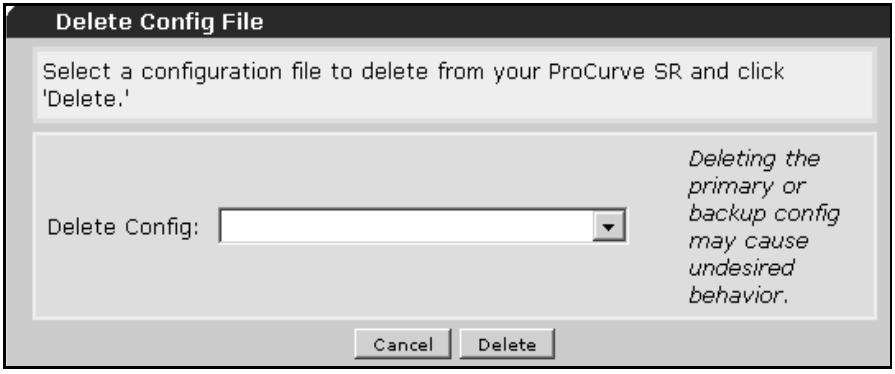

Figure 14-7. Delete Config File

1. In the *Delete Config File* section, use the pull-down menu to display all the files on flash and cflash and select the file you want to delete.
2. Click the *Delete* button to erase the file. A confirmation dialog box is displayed.
3. Click *OK* to delete the file.

For information about advanced file management functions such as renaming, uploading, or downloading files, see *Chapter 1: Overview*.

Firmware

The *Firmware* section allows you to manage Secure Router OS files. You can select the Secure Router OS file that is loaded when the ProCurve Secure Router boots. You can also upload new OS files and delete old files.

Be careful when setting and managing router firmware; setting the wrong file may prevent your router from booting with the proper configuration or even from booting at all.

Set Primary/Backup Firmware. The Secure Router OS, or firmware, files have the .biz extension. The primary firmware file is always named SROS.BIZ. From the Web browser interface, you can select the firmware file that the router loads when it is booted.

1. Click *Utilities* > *Firmware* in the navigation bar. The *Set Primary / Backup Firmware* window is displayed.

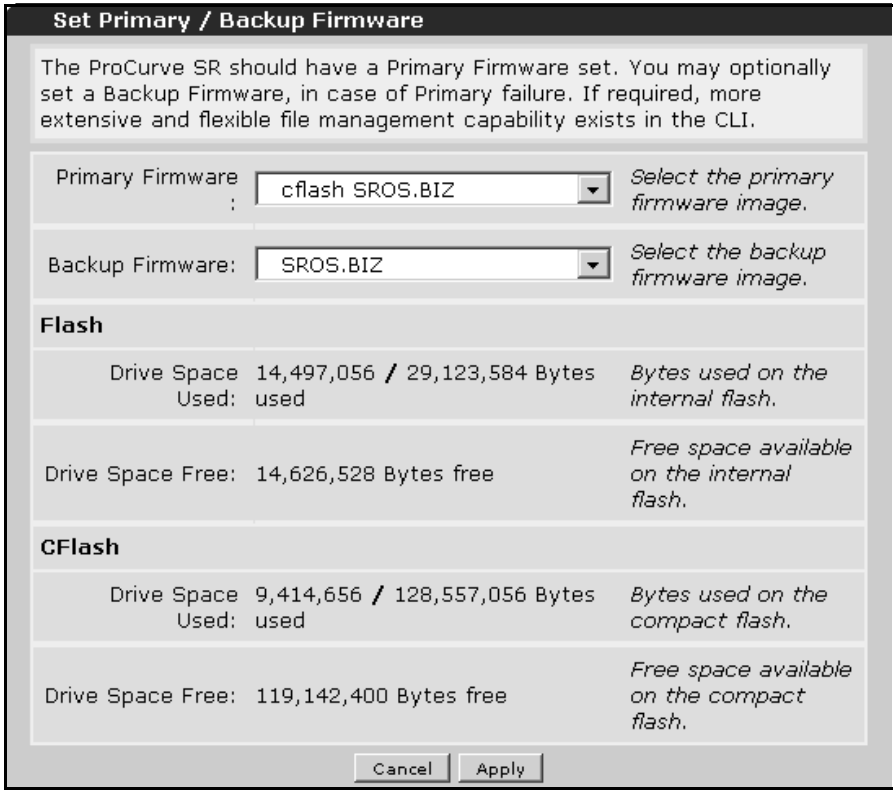

Figure 14-8. Set Primary/Backup Firmware

2. Use the pull-down menu for the *Primary Firmware* box to select the file you want for your primary firmware. This file should be cflash SROS.BIZ.

3. To set the backup firmware, use the pull-down menu for the *Backup Firmware* box to select the file you want for your backup software. This file should be SROS.BIZ.

This window also shows the current memory statistics for the internal flash and cflash drives. The Flash memory statistics are displayed as the bytes used, the total memory, and the drive space free. The CFlash memory statistics are displayed below the Flash statistics in the same format.

It is always a good idea to keep track of the amount of memory you have available when saving multiple configurations to your router. For information about deleting files, see "Delete Config File" on page 14-12.

Upload Firmware. This section allows you to upload boot code and OS updates to your router. To get these updates, go to www.procurve.com and download the new firmware files to your PC.

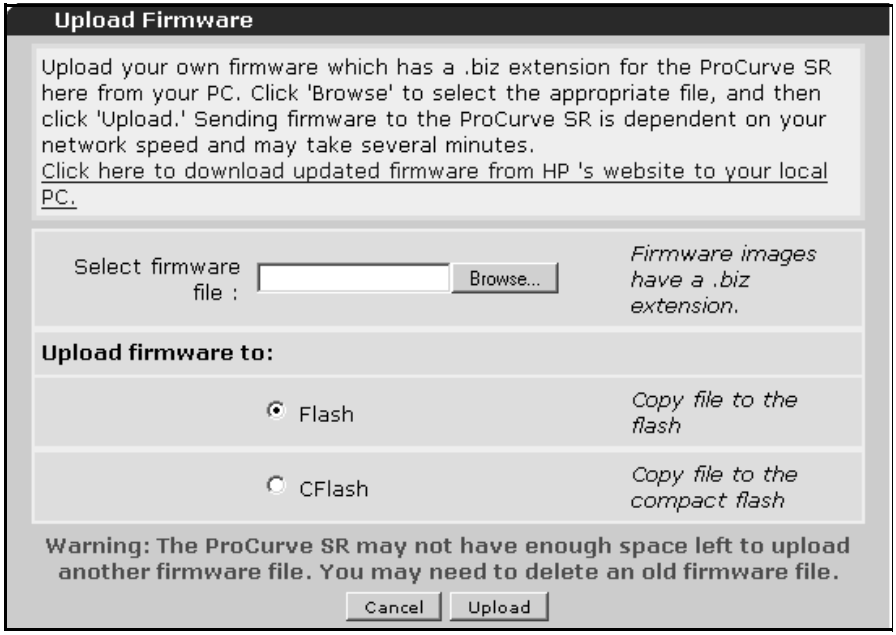

Figure 14-9. Upload Firmware

1. To upload the file from your PC or terminal to the router, click the *Browse* button next to the *Select Firmware File:* box.

Note

All firmware files have a .biz extension.

2. After you have selected the new firmware file, select either *Flash* or *CFlash* to specify the router memory location you are saving the file to.
3. Click the *Upload* button.

Delete Firmware. This window allows you to delete old firmware versions. Firmware files are usually the largest files in memory, and if you need to free up memory for configuration files, you may want to delete older firmware.

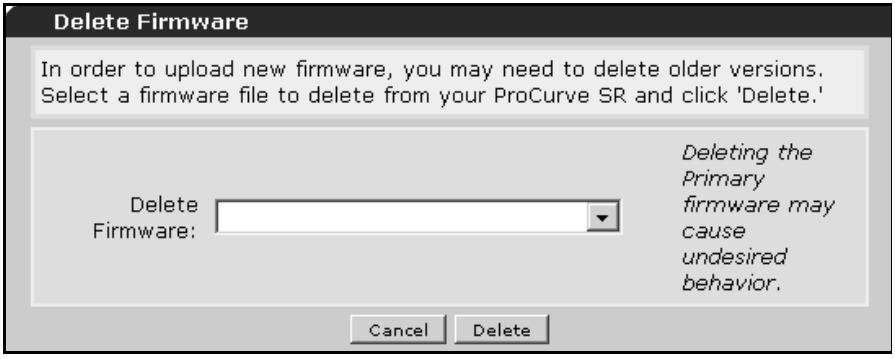

Figure 14-10.Delete Firmware

1. Use the pull-down menu for the *Delete Firmware* box to select the file that you want to delete.
2. Click the *Delete* button.

Caution

Deleting the current firmware version or deleting all firmware from the router's memory may prevent the router from booting. Be very careful when deleting your router's firmware. You may want to keep a backup copy of the current firmware version.

Debug

The *Debug* section allows you to activate debug messages that provide real-time information about processes and protocols that are running on the router. Debug messages are displayed as the router receives and sends packets related to the process you are debugging, providing useful information for troubleshooting or testing your router's operation.

The debug messages generated using the Web interface are equivalent to the corresponding CLI **debug** commands. For example, to view detailed messages about the AAA subsystem in real time, if you select the *AAA* filter in the Web browser interface, you will see the same messages that you will see if you enter the CLI **debug aaa** command from the enable mode context.

You can generate messages using one or more debug filters. For example, you can enable Point-to-Point Protocol (PPP) and track debug messages at the same time. Some debug filters have subcategories, such as the *PPP* filter's *Authentication* subcategory (equivalent to running the CLI **debug ppp authentication** command). Other debug filters may require additional information, such as an access control list (ACL) name for the *Access-List* filter (as in the CLI **debug access-list *<listname>*** command).

When you enable debug messages from the Web browser interface, the ProCurve Secure Router will continue displaying these messages until you exit the Web browser interface or explicitly stop the debug messages (as explained in Step 8 in the instructions that follow).

Note

As you use the debug commands in the Web browser interface to troubleshoot your router, be aware that debug operations are processor-intensive and could seriously degrade network performance.

To enable debug messages from the Web browser interface, complete the following steps:

1. Click *Debug* in the *Utilities* section of the navigation bar.
2. To add a debug filter, click the *Add Debug Filter* button.
3. From the *Category* pull-down menu, select the desired debug filter.

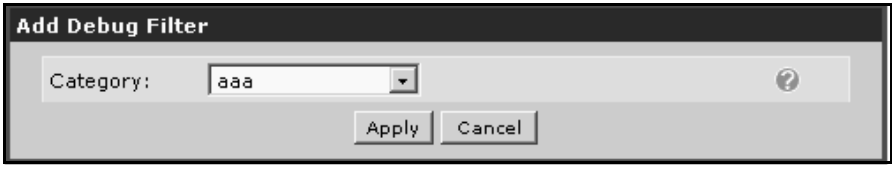

Figure 14-11. Add Debug Filter Category

   a. If the debug filter that you select has subcategories, select the subcategory that you want from the *Subcategory* pull-down menu.

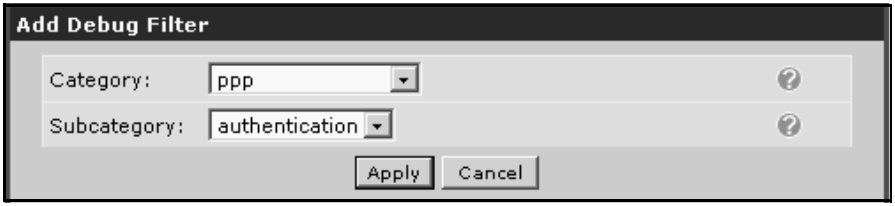

Figure 14-12. Add Debug Filter Subcategory

b. Or, if the debug filter that you select requires other information, enter the information in the field provided.

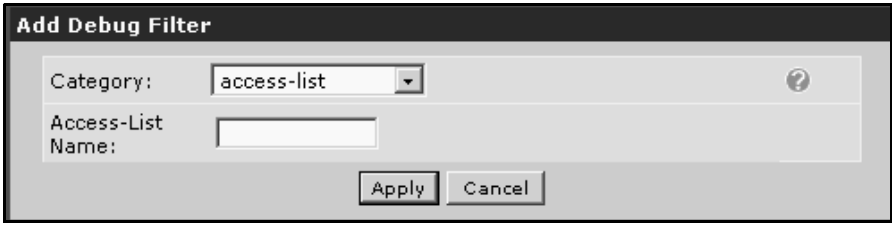

Figure 14-13. Add Debug Filter Specifics

4. Click the *Apply* button.
5. Repeat steps 2 through 4 for all other debug filters that you want to add.
6. If you want to delete one or more debug filters that you have selected, check the box for each filter you want to delete. You can check or uncheck *all* listed categories by clicking the *Debug Category* box (and you can then still check or uncheck individual boxes as needed). Then click the *Remove Selected Events* button to delete all checked filters.

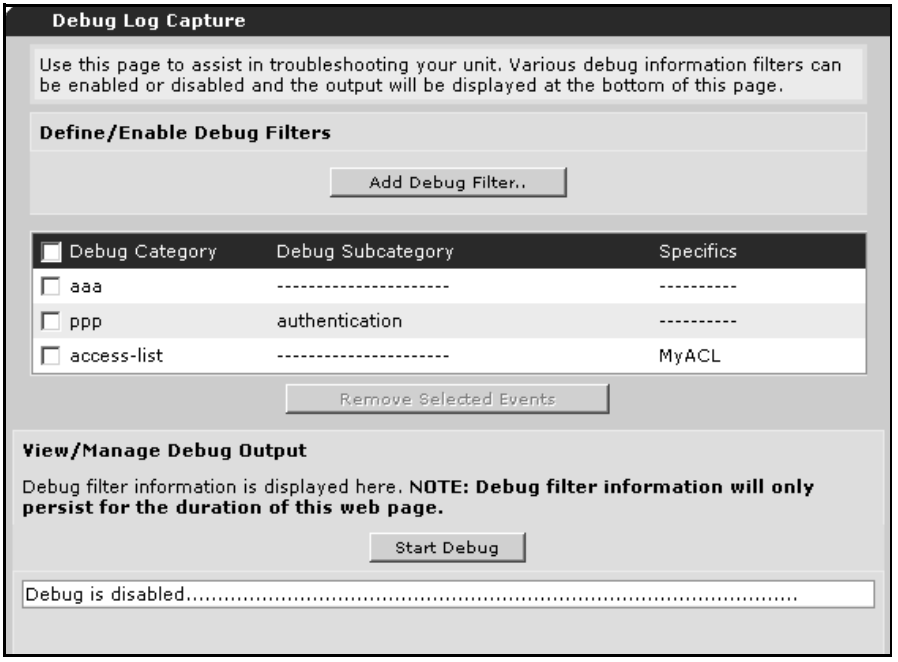

Figure 14-14. Start Debug

7. When you have selected all of the debug filters that you want, click the *Start Debug* button. Messages generated for the selected debug filters will then be displayed on the screen.

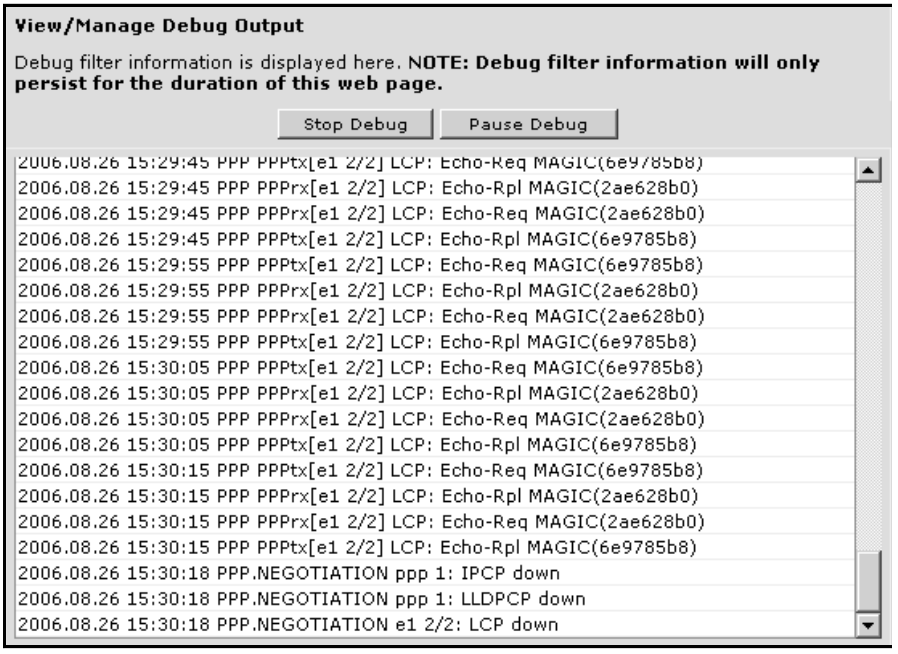

Figure 14-15. View/Manage Debug Output

For a complete explanation of the output for each debug filter in the Web browser interface, see the corresponding CLI **debug** command in the troubleshooting section of the applicable chapter in this manual or the *ProCurve Secure Router Advanced Management and Configuration Guide*.

8. You can click the following buttons on the screen while debug is running:
   - *Pause Debug* and *Restart Debug*—to pause and then restart the debug output on the screen. While the output is paused, you can examine the existing debug messages, but no new messages will be generated until you restart the output.
   - *Stop Debug*—to stop the debug output. If you want, you can then add or delete debug filters and start the debug output again (see Steps 2 through 7).

Note

If you click the *Stop Debug*, *Add Debug Filter*, or *Remove Selected Events* button while debug is running, the current debug output on the screen will be lost.

Reboot Unit

After you have uploaded new firmware or done some configuration work, you may need to reboot the router to make the changes active. Select *Reboot Unit* under *Utilities* in the navigation bar.

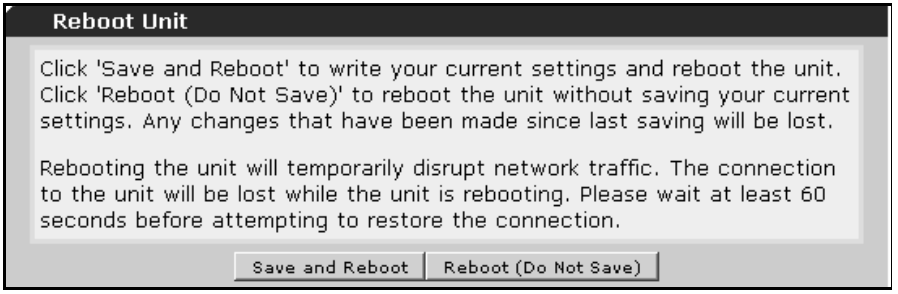

Figure 14-16. Reboot Unit

1. Click the *Save and Reboot* button to save a copy of the current configuration to a startup-config file. If you are running the AutoSynch feature, a copy is saved to both internal flash and compact flash. This option allows you to keep the current configuration and reboot the router.

Caution

If you have made changes to the Ethernet or WAN interface that you are using to access the Web browser interface, or if you have made changes to any security policies, saving and rebooting may lock you out of the router.

2. Click the *Reboot (Do Not Save)* button to immediately reboot the router without keeping any changes made to the configuration since the last save. If you have made experimental changes to the router or if you have made changes that are causing operation problems, you may want to reboot the router and have it revert to a previous working configuration.

Telnet to Unit

To open a Telnet session between your router and your PC, select *Telnet to Unit* under *Utilities* in the navigation bar.

In order to successfully establish a Telnet session to your router, you first need to configure the router to allow Telnet access.

1. Set an enable mode password.
   a. On the left panel of the Web browser interface, click *Passwords*.
   b. Scroll to the *Service Authentication* window and click the *Enable* tab.
   c. Select *Use Password* and enter an enable password. Enter the password again in the *Confirm Password* box.
   d. Click *Apply*.
2. Set a Telnet password.
   a. In the *Service Authentication* window, click the *Telnet* tab.
   b. Select *Use Password* and enter the password in the box. Re-enter the password in the *Confirm Password* box.
3. In the navigation bar, click *Telnet to Unit*. The PC will open a terminal session and begin to establish a Telnet session.
4. When the terminal session software begins, it will prompt you for a password. Enter the Telnet password.
5. The session software will display the CLI in the basic mode context. To enter the enable mode context, enter **enable**. When the router prompts you for the enable mode password, enter the password you configured. From this Telnet session, you can configure the router using the CLI.

Enabling IP Services on the Router

In the *IP Services* section, you can enable or disable the following servers on the router:

- FTP
- TFTP
- HTTP
- HTTPS
- secure copy
- Telnet
- SSH

You can also configure settings for the Web browser interface.

In addition to enabling these servers, you must configure passwords for them so that users can access the router. To configure passwords for management access, see "Configuring Passwords to Control Management Access to the Router" on page 14-26.

1. Click *System* > *IP Services* in the navigation bar. The *IP Services Enable/Disable* window is displayed.

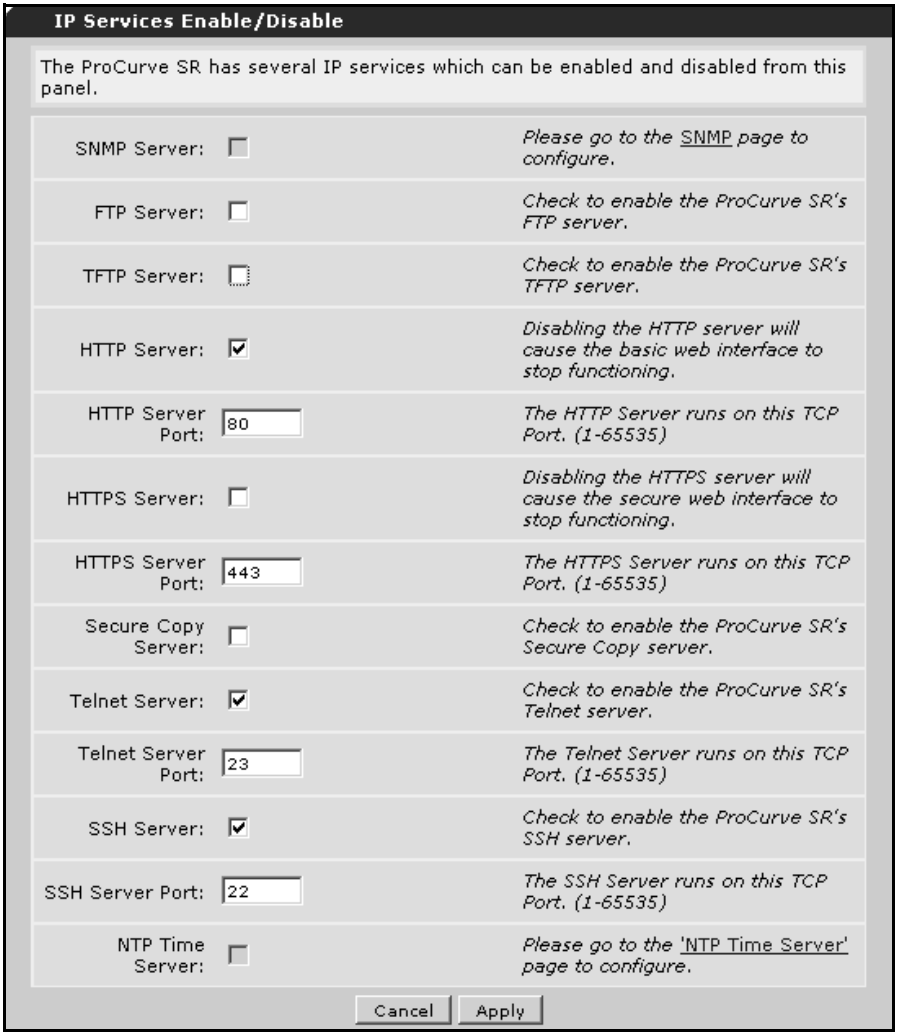

Figure 14-17. IP Services Enable/Disable

2. To enable the router as an FTP Server, check the box.
3. To enable the router as a TFTP server, check the box.
4. To access the Web browser interface, you enabled the router's HTTP Server from the CLI. To disable the HTTP Server, uncheck the box.

Caution

Disabling the HTTP Server will cause the Web browser interface to stop functioning.

5. To change the HTTP Server Port, enter the desired port number in the box. The default port is 80.
6. To enable the HTTPS Server, check the box.
7. To change the HTTPS Server Port, enter the desired port number in the box. The default is 443.
8. To enable the router's Secure Copy Server, check the box.
9. To enable the router as a Telnet server, check the box.
10. To change the Telnet Server Port, enter the desired port number in the box. The default port is 23.
11. To enable the router as an SSH server, check the box.
12. To change the SSH Server Port, enter the desired port number in the box. The default port is 22.
13. To make the changes effective, click *Apply*. If you want to return to the previously configured settings, click *Cancel* to reset to the defaults.

Web Access Configuration

Web sessions with the ProCurve Secure Router have a default timeout of 10 minutes, after which you must log in again for continued access to the Web browser interface.

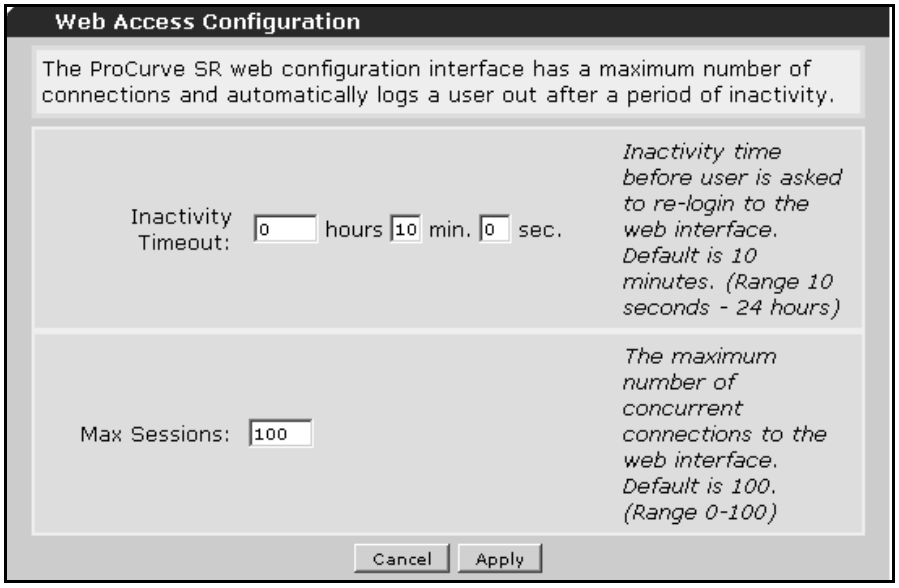

Figure 14-18. Web Access Configuration

1. To change the *Inactivity Timeout*, enter the number of hours, minutes, and seconds in the boxes.
2. You can set the maximum number of concurrent connections to the Web browser interface by entering the number in the *Max Sessions:* box.
3. To make the changes effective, click *Apply.* Click *Cancel* to reset to the previously configured settings.

Configuring Passwords to Control Management Access to the Router

The ProCurve Secure Router uses usernames and passwords to control management access to the router. In addition to configuring usernames and passwords for each access method, you can enable the Authentication, Authorization, and Accounting (AAA) subsystem, which allows you to configure multiple access methods in case an access method fails. The AAA subsystem also supports Remote Authentication Dial-In User Service (RADIUS) servers for authentication and Terminal Access Controller Access-Control System Plus (TACACS+) servers for authentication, authorization, and accounting.

Encrypting All the Passwords

You can encrypt all passwords that you establish on the ProCurve Secure Router. These include

- enable mode password
- telnet and console line passwords
- passwords for SSH, HTTP, and FTP access
- passwords in the router's local username database

The Secure Router OS can perform an MD5 hashing function on these passwords so that they are encrypted in the running-config and when they are sent over the line.

To enable password encryption globally, complete these steps:

1. Select *Passwords* under *System* in the navigation bar.
2. Check the *Encryption Enabled* box in the *Password Encryption* window. See Figure 14-19.

Figure 14-19. Add/Modify/Delete Users Window

Configuring a Local User List: Passwords for Web, SSH, and FTP Access

When you configured the router for HTTP or HTTPS access, you entered a username and password. You can use this username and password to access the ProCurve Secure Router through Secure Shell (SSH) and FTP.

All of the usernames and passwords that you configure using the **username** command from the global configuration mode context in the CLI are stored in the local user list. The Web browser interface simplifies management of this local user list. You can view all of the usernames and passwords that have been configured in the local user list, and you can add or delete usernames and passwords.

1. To view the local user list from the Web browser interface, select *Passwords* in the navigation bar. The *Add/Modify/Delete Users* window is displayed, and the usernames that have been configured are listed under the *Modify/Delete User* heading.

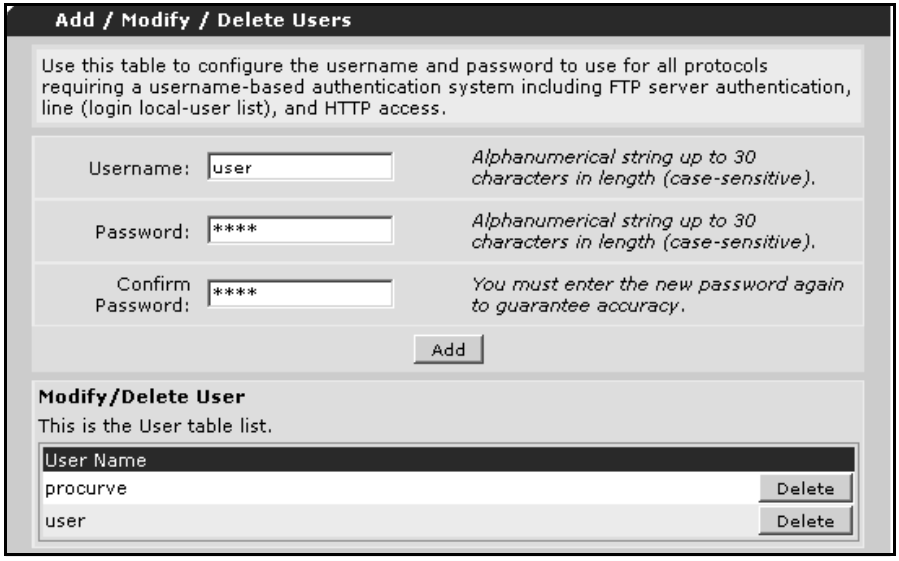

Figure 14-20. Add/Modify/Delete Users Window

2. To add a new user, enter the username in the space provided.
3. Enter the password for the username in the *Password* box.
4. Re-enter the password in the *Confirm Password* box.

5. Click *Add*. The username is now listed under the *Modify/Delete User* heading.
6. To remove a username, select it and click *Delete*.

Configuring an Enable Mode Password

To configure an enable mode password, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *Enable* tab.

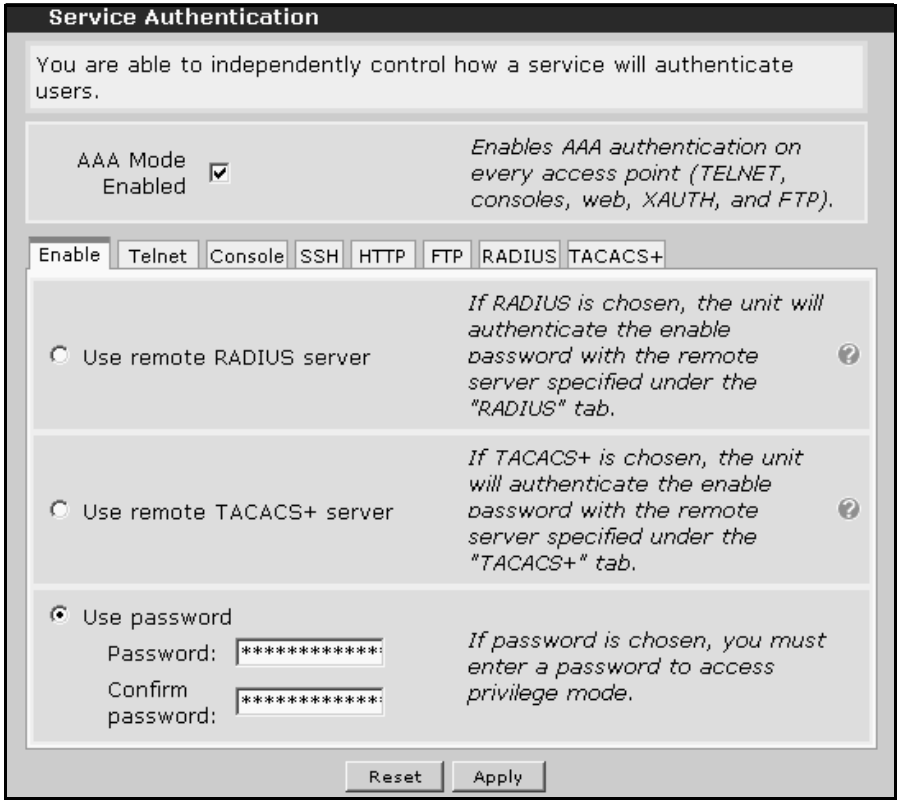

Figure 14-21. Configuring a Password for the Enable Mode

3. Select *Use Password* and then enter and confirm the password you want to use.

4. If you want to use a RADIUS or TACACS+ server to control enable mode access, then you must enable the AAA subsystem. See "Using the AAA Subsystem to Control Management Access" on page 14-35 for instructions on configuring these options.
5. Click *Apply*.

Configuring a Password for Telnet Access

To configure a password for Telnet access, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *Telnet* tab.

Figure 14-22. Configuring Passwords for Telnet Access

3. Select the *Use Local User List* option if you want to use the usernames and passwords configured in this list for Telnet access.
4. Select the *Use password* option if you want to configure a separate password for Telnet access.
5. If you want to use a RADIUS or TACACS+ server to control Telnet access, then you must enable the AAA subsystem. See “Using the AAA Subsystem to Control Management Access” on page 14-35 for instructions on configuring these options.
6. Click *Apply*.

Configuring a Password for Console Access

To configure a password for console access, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *Console* tab.

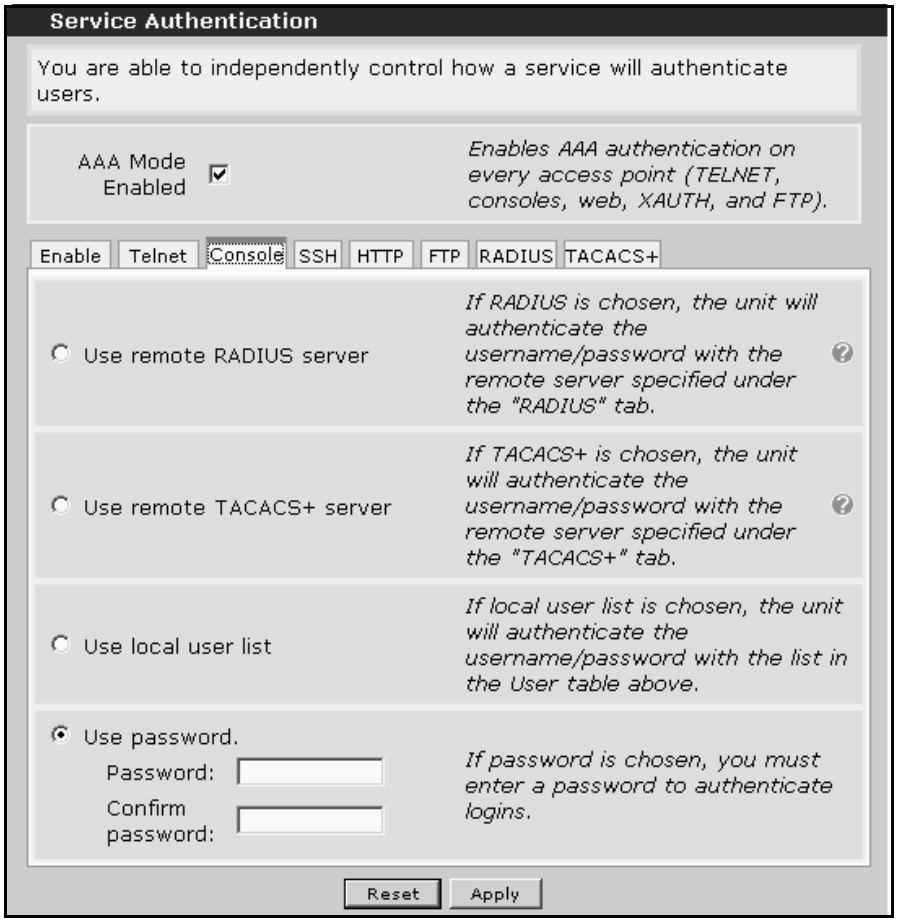

Figure 14-23. Configuring Passwords for Console Access

3. Select the *Use local user list* option if you want to use the usernames and passwords configured in this list for console access.
4. Select the *Use password* option if you want to configure a separate password for console access.

5. If you want to use a RADIUS or TACACS+ server to control console access, then you must enable the AAA subsystem. See "Using the AAA Subsystem to Control Management Access" on page 14-35 for instructions on configuring these options.
6. Click *Apply*.

Configuring a Password for SSH Access

To configure a password for SSH access, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *SSH* tab.

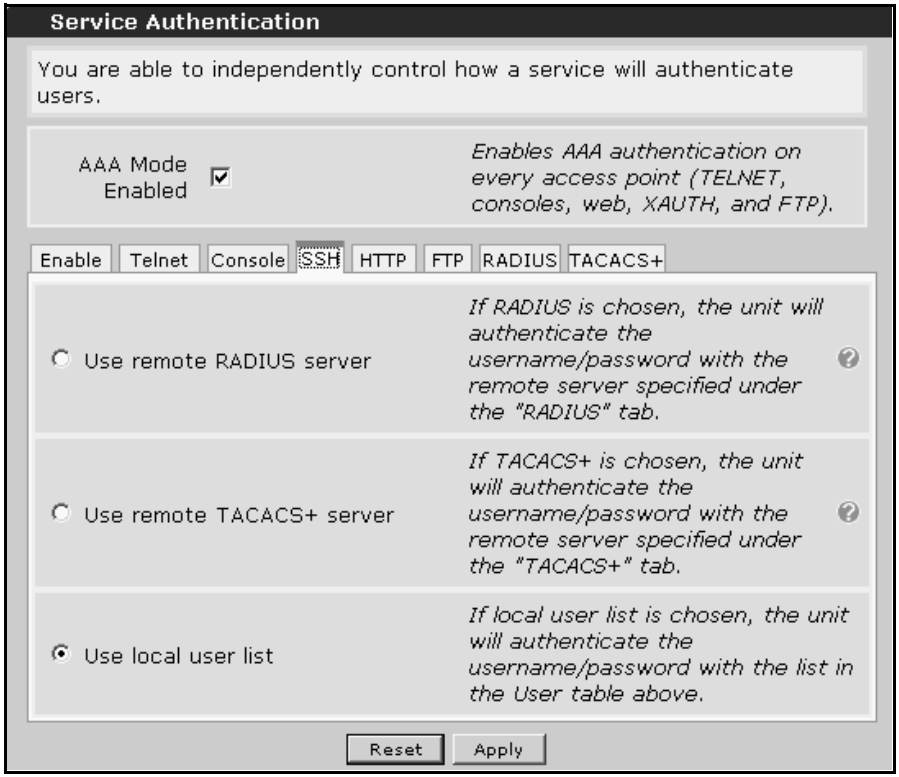

Figure 14-24. Configuring Passwords for SSH Access

3. Select the *Use Local User List* option if you want to use the usernames and passwords configured in this list for SSH access. (This is the default option.)
4. If you want to use a RADIUS or TACACS+ server to authenticate users attempting to initiate an SSH session with the router, then you must enable the AAA subsystem. See "Using the AAA Subsystem to Control Management Access" on page 14-35 for instructions on configuring these options.
5. Click *Apply*.

Configuring a Password for HTTP Access

To configure a password for Web access, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *HTTP* tab.

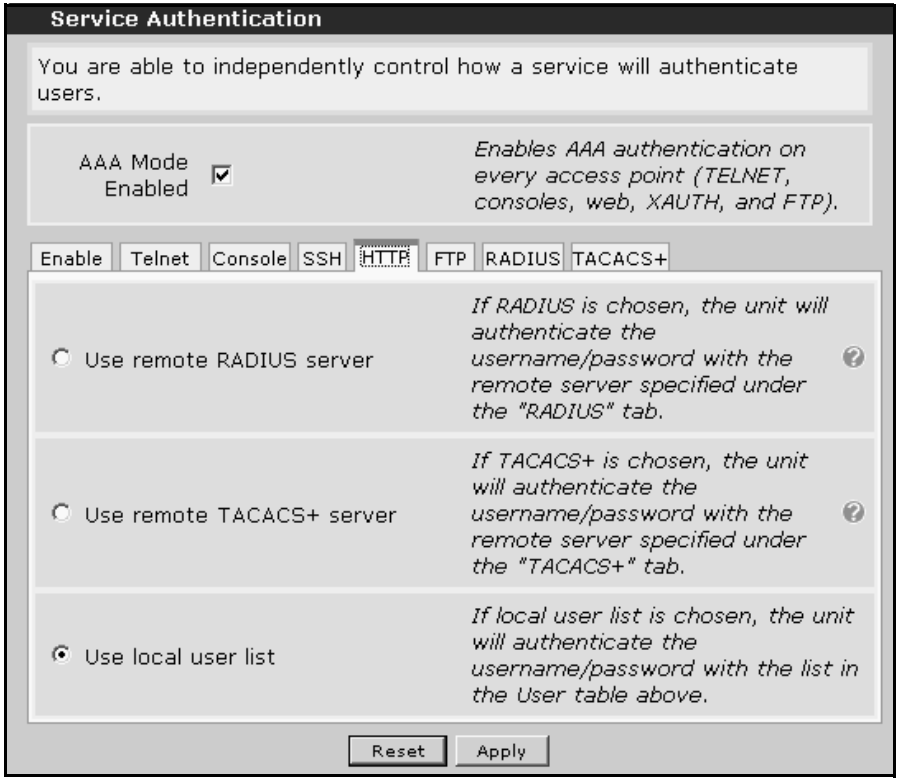

Figure 14-25. Configuring Passwords for Web Access

3. Select the *Use Local User List* option if you want to use the usernames and passwords configured in this list for access to the router's Web server. (This is the default setting.)
4. If you want to use a RADIUS or TACACS+ server to control access to the Web browser, then you must enable the AAA subsystem. See "Using the AAA Subsystem to Control Management Access" on page 14-35 for instructions on configuring these options.
5. Click *Apply*.

Configuring a Password for FTP Access

To configure a password for FTP access, complete these steps:

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. Select the *FTP* tab.

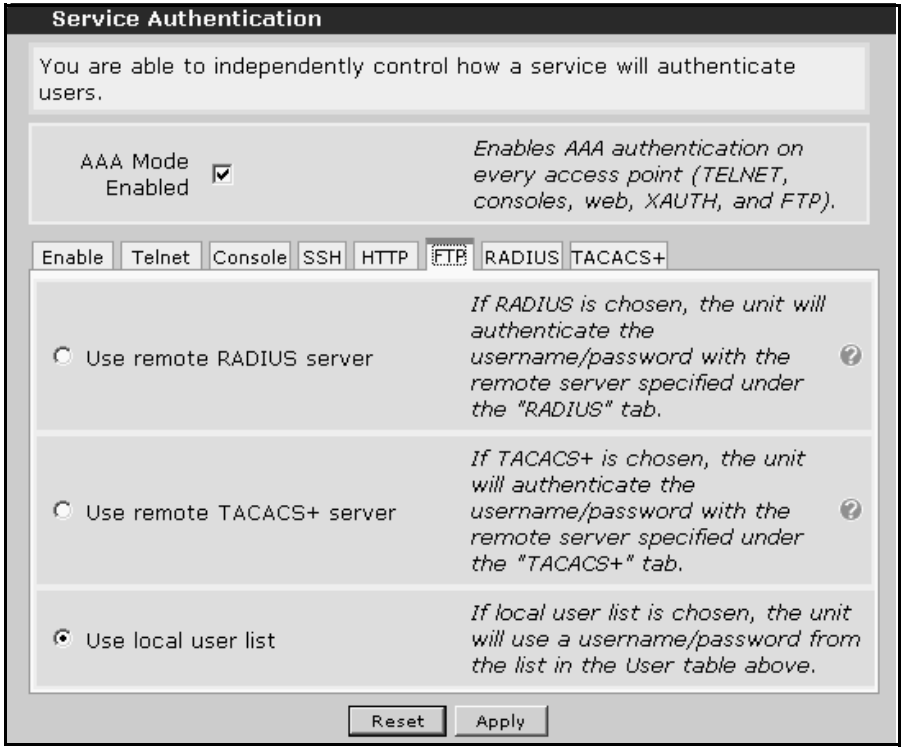

Figure 14-26. Configuring Passwords for FTP Access

3. Select the *Use Local User List* option if you want to use the usernames and passwords configured in this list for FTP access. (This is the default setting.)
4. If you want to use a RADIUS or TACACS+ server to control FTP access, then you must enable the AAA subsystem. See "Using the AAA Subsystem to Control Management Access" on page 14-35 for instructions on configuring these options.
5. Click *Apply*.

Using the AAA Subsystem to Control Management Access

Authentication, authorization, and accounting (AAA) is an industry standard for controlling:

- which users can access a system (authentication)
- what they can do once they are granted access (authorization)
- what is recorded about their activities (accounting)

The AAA subsystem on the ProCurve Secure Router currently supports authentication using a remote RADIUS server. The ProCurve Secure Router also supports authentication, authorization, and accounting using a remote TACACS+ server.

When you enable the AAA subsystem, you can specify a list of authentication methods for each type of access. If one authentication method fails, the ProCurve Secure Router will allow the user to try another access method.

The ProCurve Secure Router has specific criteria for failure:

- Line and enable passwords fail if there are no line or enable passwords configured.
- RADIUS and TACACS+ servers fail if the ProCurve Secure Router cannot reach the server on the network.
- The local user list fails if the given user is not in the database.

For example, if you configure the authentication methods with RADIUS as the first option and the RADIUS server goes down, the AAA subsystem tries the next authentication method you configured. If you listed the local user list after the RADIUS server, the AAA subsystem will use that authentication method next.

However, if a user enters the wrong username or the wrong password for a particular username, the user failed to authenticate to the router; the access method did not fail. In this case, the user will be denied access to the router.

You can use the Web browser interface to specify the RADIUS and TACACS+ servers that the ProCurve Secure Router can contact. You can also configure authentication using RADIUS or TACACS+ from the Web browser interface. However, you must configure authorization and accounting using TACACS+ from the CLI.

Configuring Authentication Using a RADIUS Server

If you want to use a RADIUS server to authenticate users who access the router, you must enable the AAA subsystem.

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. In the *Service Authentication* section, select *AAA Mode Enabled*.
3. Click *Apply* to enable the AAA subsystem.
4. Configure the settings for a RADIUS server.
   a. Select the *Radius* tab.

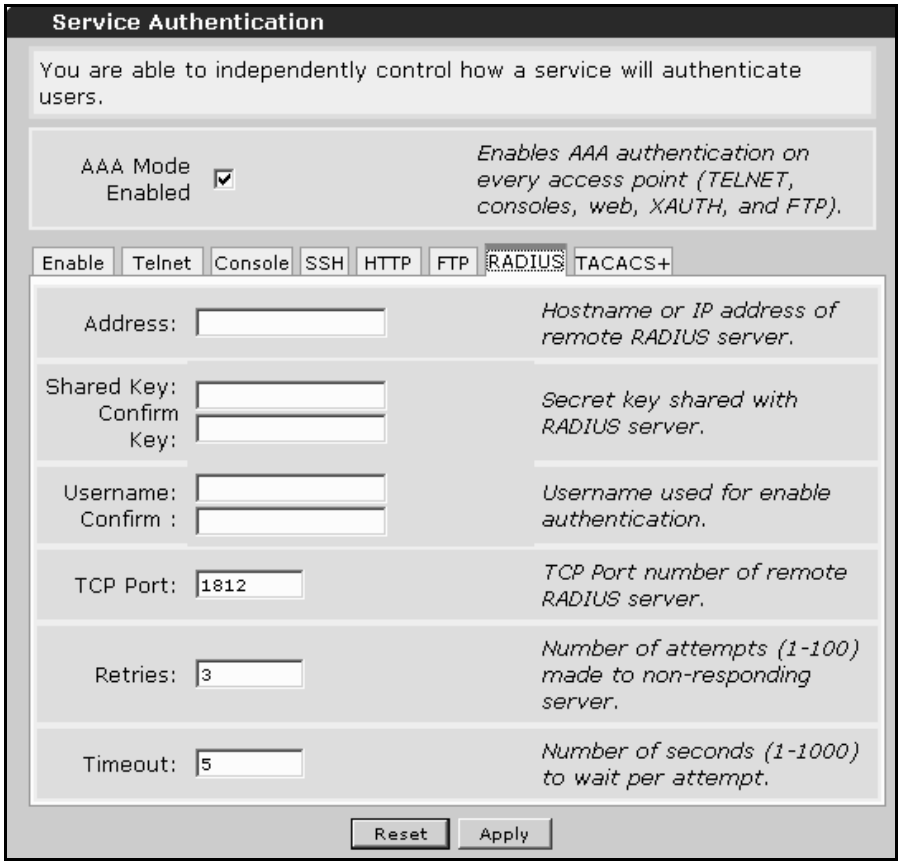

Figure 14-27. Configure the Settings for a RADIUS Server

b. For *Address*, enter the IP address of the RADIUS server.

c. For *Shared Key*, enter the shared key. Re-enter the key to confirm it.

d. For *Username*, enter and confirm the username that the router should use to authenticate itself to the RADIUS server.

e. For *TCP Port*, accept the default port unless the RADIUS server is operating on a different port.

f. For *Retries*, configure the number of attempts that the ProCurve Secure Router will make to contact the RADIUS server.

g. For *Timeout*, configure the number of seconds that the ProCurve Secure Router will wait to receive a reply from the RADIUS server.

h. Click *Apply* to save the settings for the RADIUS server.

5. Select the tab for the type of access you want to configure:
   - Enable Password
   - Telnet
   - Console
   - SSH
   - HTTP
   - FTP
6. Select the *Use remote RADIUS server* option.
7. Click *Apply* to save your settings.

Configuring Authentication Using a TACACS+ Server

If you want to use a TACACS+ server to authenticate users who access the router, you must enable the AAA subsystem.

1. Select *Passwords* in the navigation bar and scroll to the bottom of the *Add/Modify/Delete Users* window.
2. In the *Service Authentication* section, select *AAA Mode Enabled*.
3. Click *Apply* to enable the AAA subsystem.
4. Configure the settings for a TACACS+ server.
   a. Select the *TACACS+* tab.

Figure 14-28. Configure the Settings for a TACACS+ Server

b. For *Address*, enter the IP address of the TACACS+ server.

c. For *Shared Key*, enter the shared key. Re-enter the key to confirm it.

d. For *TCP Port*, accept the default port unless the TACACS+ server is operating on a different port.

e. For *Retries*, configure the number of attempts that the ProCurve Secure Router will make to contact the TACACS+ server.

f. Click *Apply* to save the settings for the TACACS+ server.

5. Select the tab for the type of access you want to configure:
   - Enable Password
   - Telnet
   - Console
   - SSH
   - HTTP
   - FTP
6. Select the *Use Remote TACACS+ server* option.
7. Click *Apply* to save your settings.

Configuring Ethernet Interfaces

To configure an Ethernet interface from the Web browser interface, complete the following steps. If you need more information about any of the options, see *Chapter 3: Configuring Ethernet Interfaces*.

1. Click *Physical Interfaces* in the navigation bar.
2. Select the Ethernet port you want to configure (*eth 0/1* or *eth 0/2*). The *Configuration for Ethernet* window is displayed.

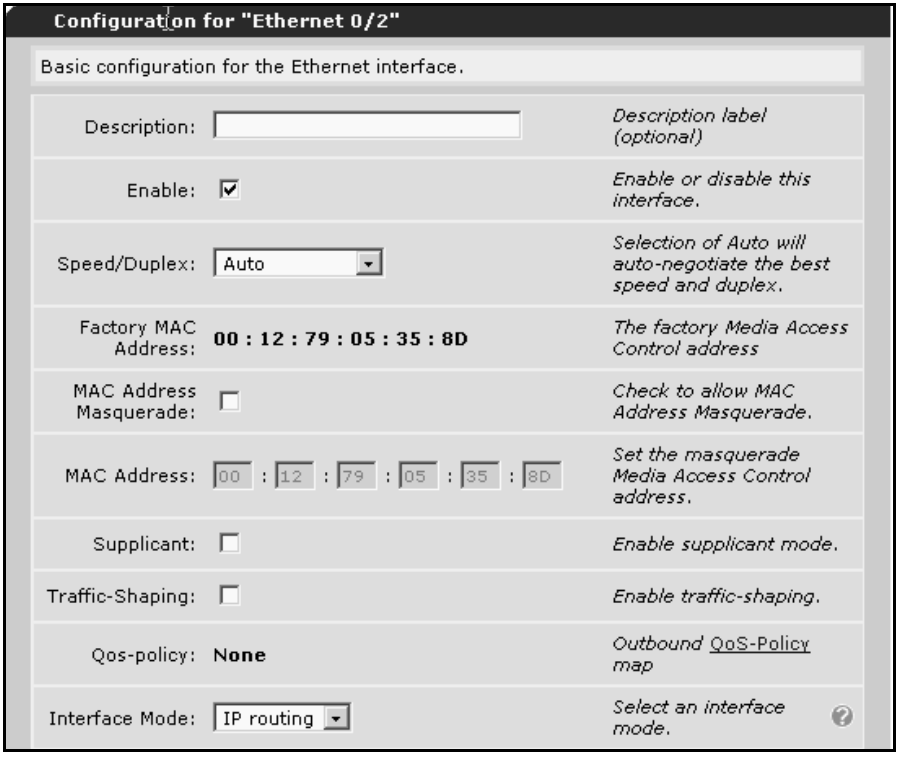

Figure 14-29. Configuration for Ethernet Window

3. If you want to document information about this Ethernet interface, enter an alphanumeric string up to 80 characters in the *Description* box.

4. Click the *Enable* box and then click *Apply* at the bottom of the window to activate the Ethernet interface immediately. You can also complete the Ethernet configuration before clicking *Apply*.
5. Use the pull-down menu to configure the *Speed/Duplex* setting:
   a. To select an automatically negotiated connection, select *Auto*.
   b. To specify a 10 Mbps connection with half-or full-duplex, select *10Mbps/half* or *10Mbps/full*.
   c. To specify a connection at 100 Mbps using a half- or full-duplex setting, select *100Mbps/half* or *100Mbps/full*.
6. The factory-set Media Access Control (MAC) Address for the Ethernet interface is displayed beneath the *Speed/Duplex* box. If you want to keep the MAC address of the router's interfaces uniform, you can enable MAC Address Masquerade by clicking the box. Then, enter the desired MAC address, in hexadecimal, in the boxes provided.
7. Configure supplicant information if the Ethernet interface connects to a network that requires 802.1X authentication.
   a. Click the *Supplicant* box. *Supplicant Username* and *Supplicant Password* boxes are displayed.
   b. In these boxes, enter the username and password required to allow the router to access the 802.1X network. (For more information about the router functioning as an 802.1X client, see "The ProCurve Secure Router as an 802.1X Supplicant" on page 2-65.)
8. If you want to enable Traffic Shaping on this Ethernet interface, check the box. Traffic Shaping limits the bandwidth used for outgoing traffic on an interface, much like the rate limiter for QoS, except that it queues frames instead of deleting them.

9. The *Interface Mode* pull-down allows you to choose IP routing or PPP over Ethernet (PPPoE). The default setting is *IP Routing*. If you select *PPPoE* and then click *Apply*, the *PPPoE Configuration* window is displayed. If you want to configure PPPoE for this interface, see "Configuring PPPoE for the Ethernet Interface" on page 14-50.
   a. If you are using the ProCurve Secure Router with a switch, *802.1q* is also listed as an option under the *Interface Mode* pull-down list. Selecting this option enables VLAN tagging and displays the *Ethernet Subinterface Configuration* settings you must define:
      i. ID: A unique identifier between 1 and 4095 for this subinterface
      ii. VLAN ID: The VLAN ID to use on this subinterface
      iii. Native VLAN: Check the box if this subinterface is the native VLAN; only one subinterface can be set as native
   b. For more information on configuring Ethernet subinterfaces, see "Configure VLAN Support" on page 3-19.
10. Click *Apply* to save the changes you have made to the startup-config.

SNMP Settings

If you are using a Simple Network Management Protocol (SNMP) management console, you can use the Web browser interface to configure SNMP support on the router.

For more information on SNMP settings and configuration, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*.

Enabling the SNMP Server and SNMP Traps

1. Click *SNMP* in the navigation bar, and then select the *Identity* tab.

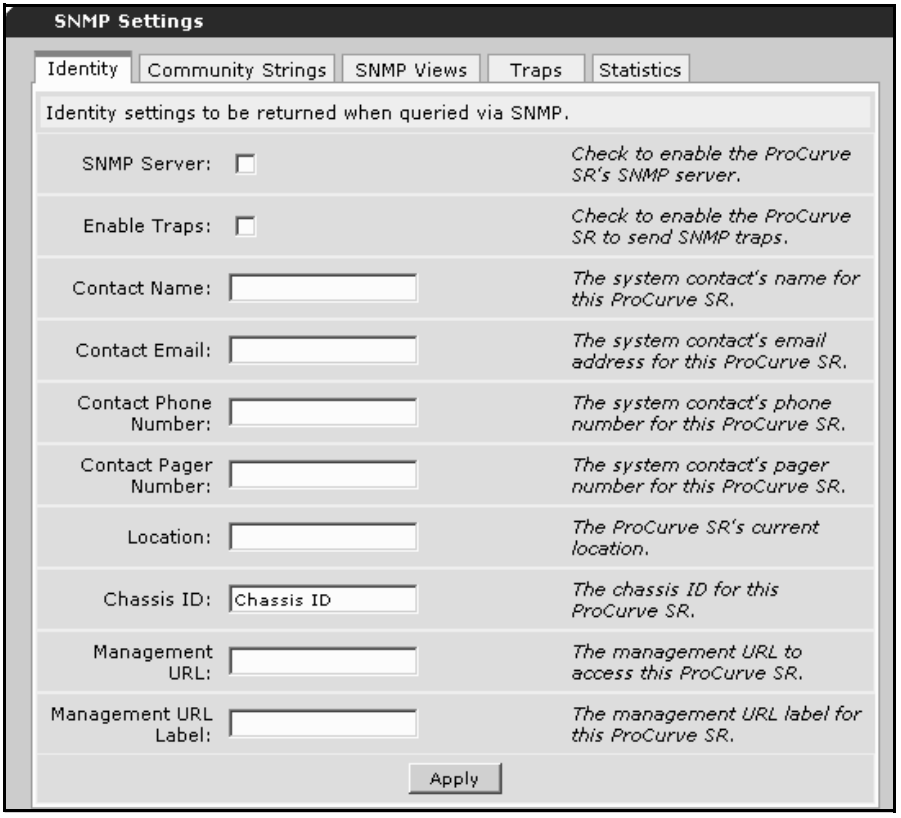

Figure 14-30. SNMP Identity Tab

2. Click *SNMP Server* to enable the SNMP server.
3. Click *Enable Traps* to enable SNMP traps.
4. Configure the remaining settings on the screen, which are optional.
5. Click *Apply* to save your changes.

Configuring SNMP Communities

Use the settings on the *Community Strings* tab to configure at least one SNMP community on the ProCurve Secure Router. You should configure the same community on the SNMP management server, so that you can access SNMP information and manage the ProCurve Secure Router.

1. Click the *Community Strings* tab.

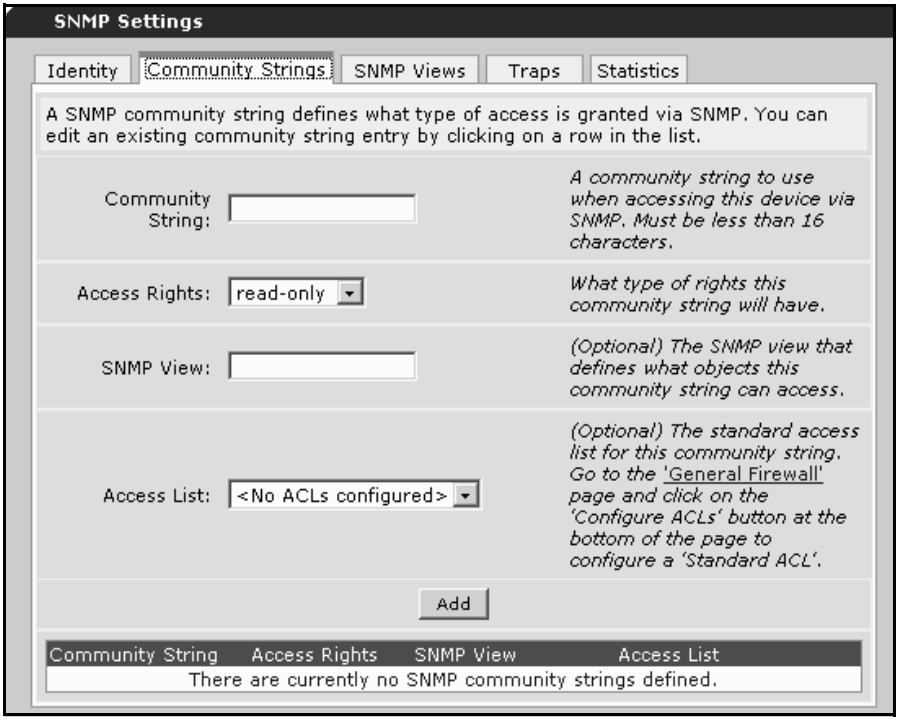

Figure 14-31. SNMP Community Strings Tab

2. In the *Community String* field, specify the community string, which serves as a password to access devices using SNMP.
3. In the *Access Rights* field, use the pull-down menu to specify access control for the community of either read-write or read-only.
4. In the *SNMP View* field, specify the SNMP view for the community string.
5. In the *Access List* field, use the pull-down menu to specify the ACL that you want to use to control the SNMP management server's access to your company's WAN.
6. Click *Add* to save your changes and create the community string.

Configuring SNMP Views

Use the settings on the *SNMP Views* tab to create a subset of SNMP community information and to grant the SNMP management server rights to that view.

1. Click the *SNMP Views* tab.

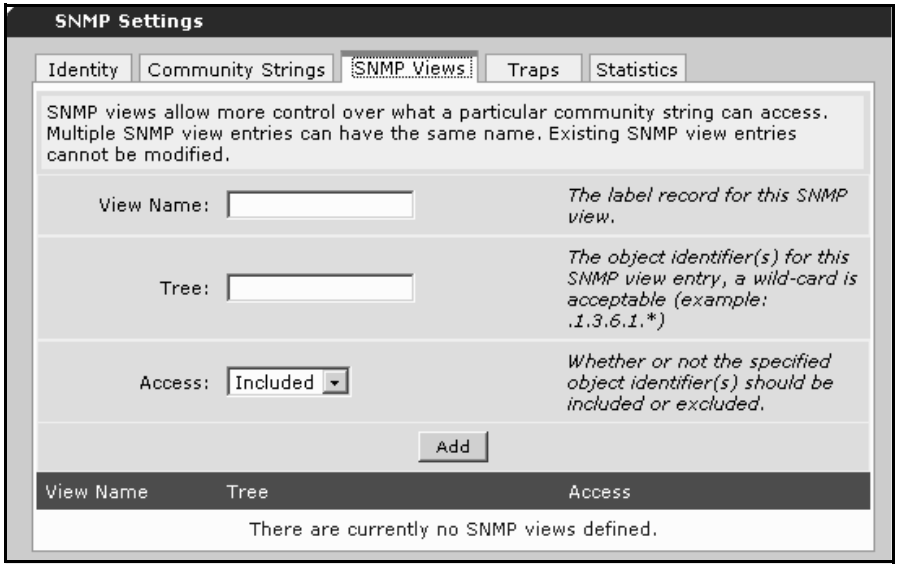

Figure 14-32. SNMP Views Tab

2. In the *View Name* field, specify a name for the SNMP view.
3. In the *Tree* field, specify the object identifiers (OIDs) for the view. You can use an asterisk (*) as a wildcard.
4. In the *Access* field, use the pull-down menu to specify whether the view is an included view or an excluded view.
5. Click *Add* to save your changes and create the SNMP view.

Configuring SNMP Trap Settings

Use the settings on the *Traps* tab to create a subset of SNMP community information and to grant the SNMP management server rights to that view.

1. Click the *Traps* tab.

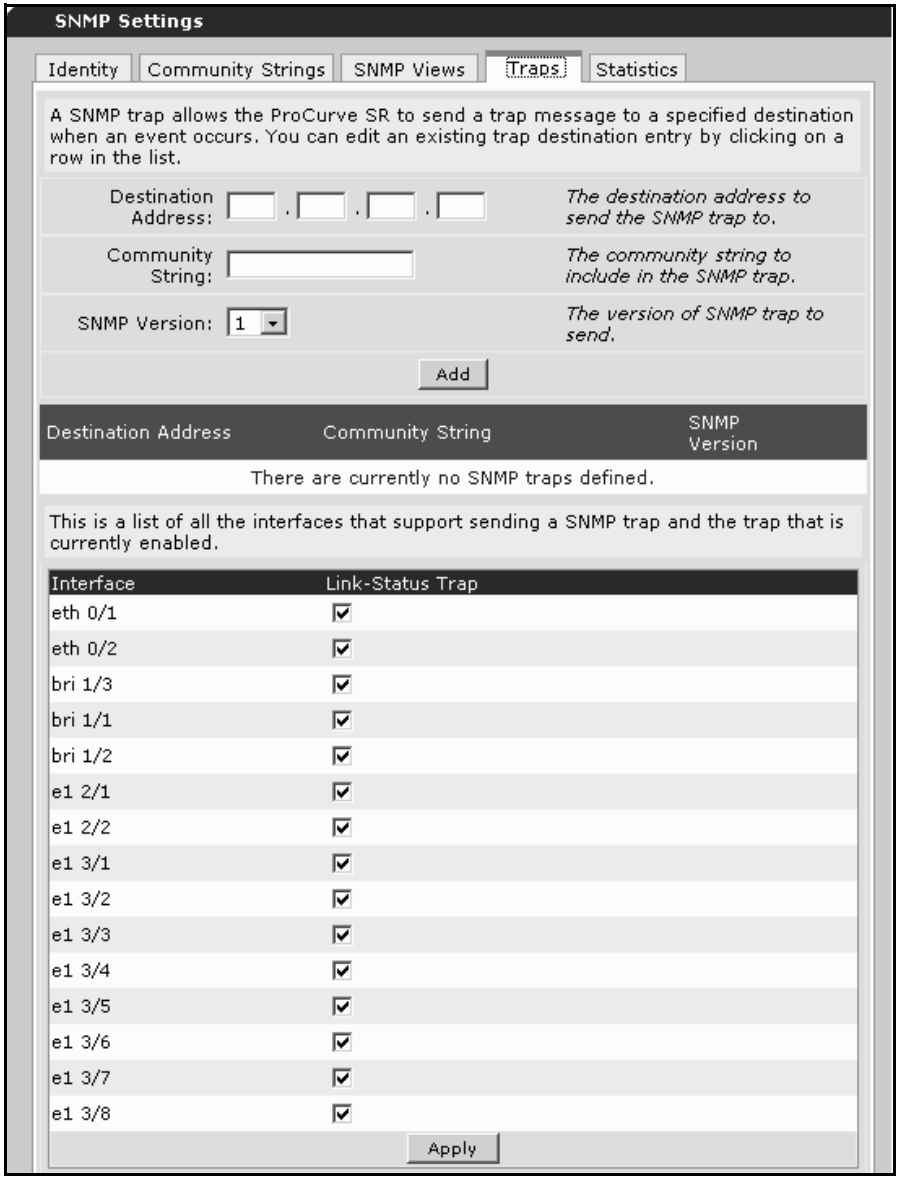

Figure 14-33. SNMP Traps Tab

2. In the *Destination Address* field, enter the IP address of the SNMP management server.
3. In the *Community String* field, specify the community string to include in the SNMP trap.

4. In the *SNMP Version* field, specify the SNMP version for the trap.
5. Click *Add* to save your changes and create the SNMP trap (which will now be listed on the screen).
6. In the interface list, check the boxes for interfaces that are authorized to send SNMP traps, and then click *Apply*.

View SNMP Statistics

Click the *Statistics* tab to view SNMP statistics through the Web browser interface.

IP Settings

The *IP Settings* section allows you to configure the IP address and dynamic Domain Name System (DNS) settings for the Ethernet interface.

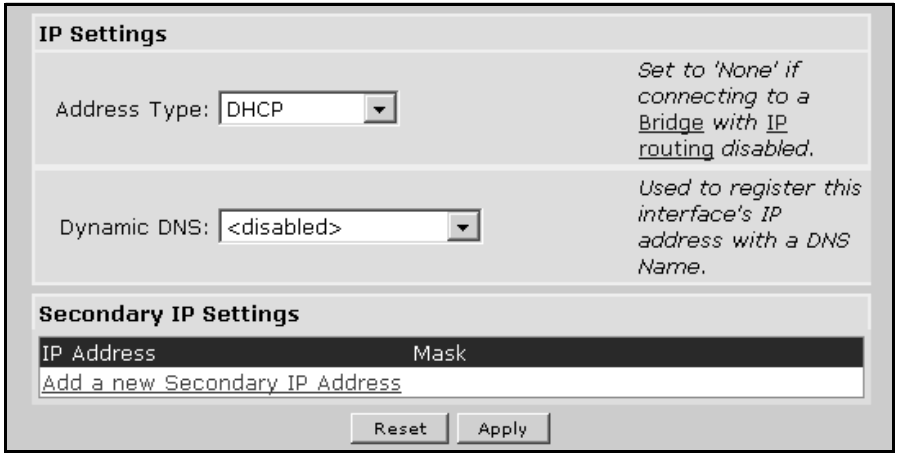

Figure 14-34. IP Settings Section

7. Use the pull-down menu to configure the *Address Type*:
   - *None*—Select this setting if you intend to set up a bridge group with the Ethernet interface.
   - S*tatic*—Select this setting if you want to configure a static IP address. The boxes to enter the IP address and subnet mask are displayed, so that you can enter the appropriate address for the Ethernet interface.
   - *DHCP*—Select this setting to configure the interface as a Dynamic Host Configuration Protocol (DHCP) client.

- *Unnumbered*—To set up the Ethernet interface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

  Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame-Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.

Dynamic DNS

8. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
   a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Choose the service for which you registered with DynDNS.org. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
   b. For *Dynamic DNS Hostname*, enter the hostname you are registering for the interface.
   c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
   d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.

Secondary IP Settings

9. To set secondary IP addresses for your Ethernet interface, click *Add a new Secondary IP Address*. Then enter the IP address and subnet mask in the boxes provided.
10. Click *Apply* to save your configurations.

Ethernet Interface Statistics

You can view status information about the Ethernet interface at the bottom of the *Ethernet Configuration* window. This display provides basic information; for a more comprehensive readout, access the CLI and enter **show interface ethernet 0/<port>** at the enable mode context.

Releasing/Renewing a DCHP IP Address

If the Ethernet interface receives its IP address from a DHCP server, the first line of the *Status for Ethernet* section reports the DHCP address state. If the interface has successfully received an address, this should display "Bound." Next to "Bound" are the words *Release* and *Renew* highlighted in blue.

11. To release the current IP address, click *Release*.
12. To receive an IP address, click *Renew*. When the interface receives an address, the *DHCP field* should display "Bound."
13. To clear the current statistics, click the *Clear Statistics* button.
14. The information in this section refreshes automatically every 5 seconds.

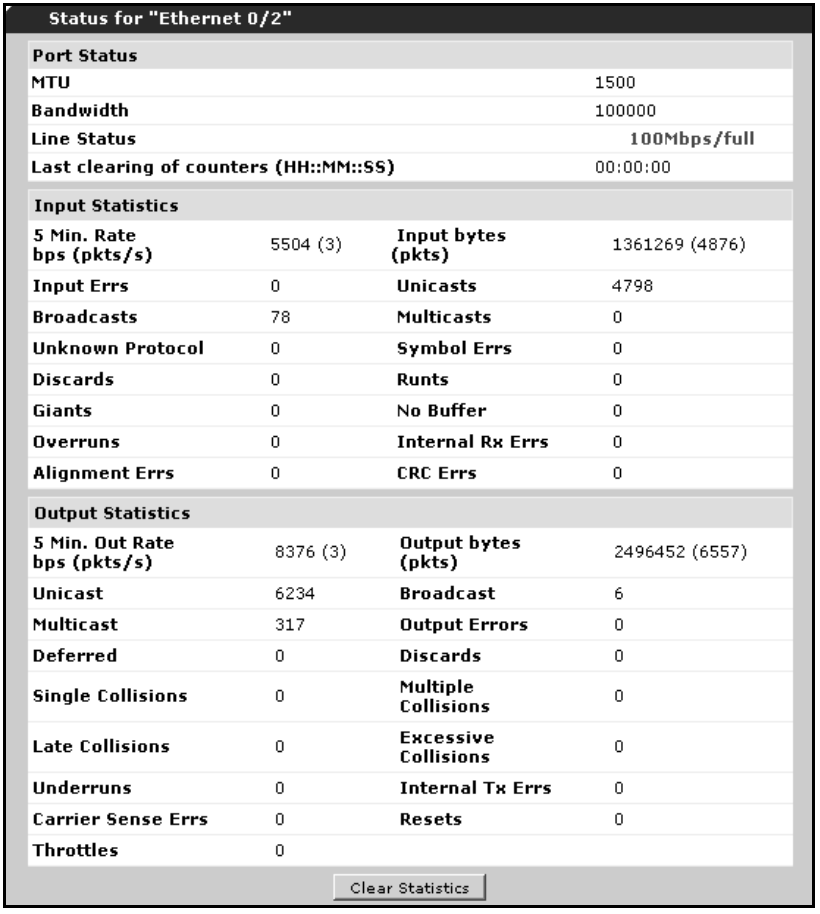

Figure 14-35. Status for Ethernet Interface

Configuring PPPoE for the Ethernet Interface

To configure PPPoE, complete the following steps:

1. Access the *Configuration for Ethernet* window, select *PPPoE* for the *Interface Mode*, and click *Apply.* The *PPPoE Configuration for "ppp <interface number>"* window is displayed.
2. Enter a description if you need to document information about PPPoE settings. This information will be displayed in the running-config under the appropriate PPP interface heading.
3. Click the *Enabled* box to activate the PPP interface.
4. For most environments, accept the default setting of 1500 for the MTU. The ProCurve Secure Router OS will negotiate an MTU of 1492 with the PPP peer. If the two peers fail to negotiate an MTU of 1492, you may need to set the MTU manually.
5. Select *Default Peer Address* if you want to configure the IP address of the PPP peer.

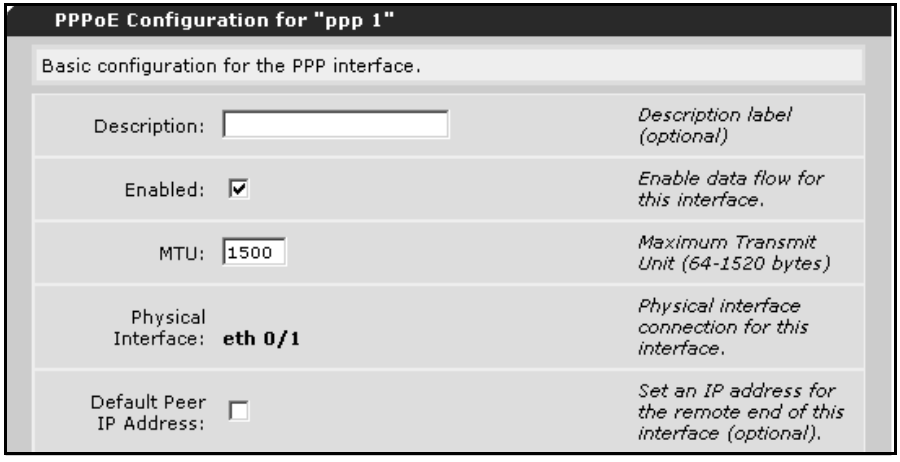

Figure 14-36. PPPoE for the Ethernet Interface

6. If you want to configure PPP authentication, see "PPP Authentication" on page 14-65.
7. Configure IP settings. For *Address Type* select one of the following.
   - *None*—Select this setting if you intend to set up a bridge group with the PPP interface.

- S*tatic*—Select this setting if you want to configure a static IP address. You can then enter the appropriate IP address for the PPP interface in the boxes provided.

  Unnumbered—To set up the PPP interface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

  Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.
- *Negotiated*—Select this setting if you want the PPP interface to negotiate an IP address from your service provider. Select *Default Route* if you want to configure the interface to receive a default gateway from the peer.

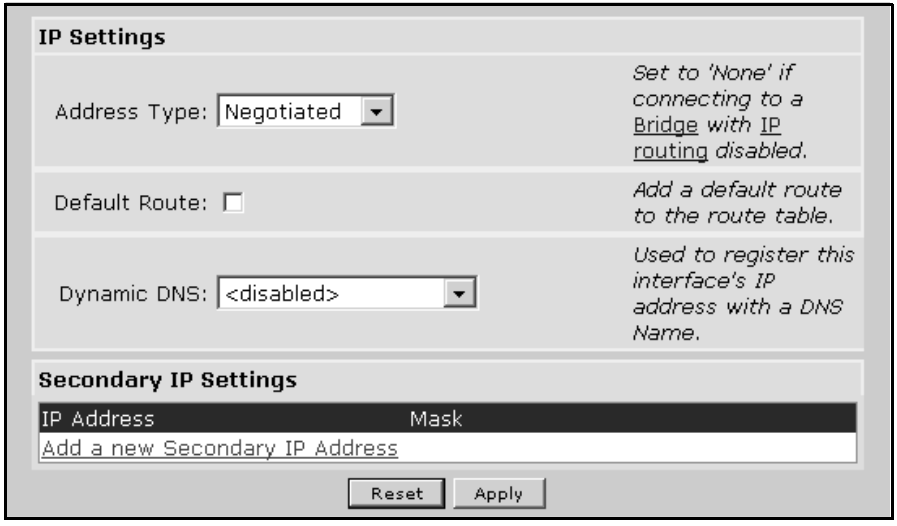

Figure 14-37. Configure IP Settings

Dynamic DNS

8. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
   a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
   b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
   c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
   d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.

Secondary IP Settings

9. To configure secondary IP addresses for the PPP interface, click *Add a new Secondary IP Address*. Then enter the IP address and subnet mask in the boxes provided.
10. Click *Apply* to activate your configurations.

View Statistics for the PPP Interface

Status information is displayed at the bottom of the *Configuration PPPoE* window. After you apply your changes, the *PPP Link State* will be "starting," indicating that the ProCurve Secure Router OS is trying to establish a PPP connection with its peer. Ensure that the *PPP Link State* is eventually "up."

This statistical information automatically refreshes every five seconds.

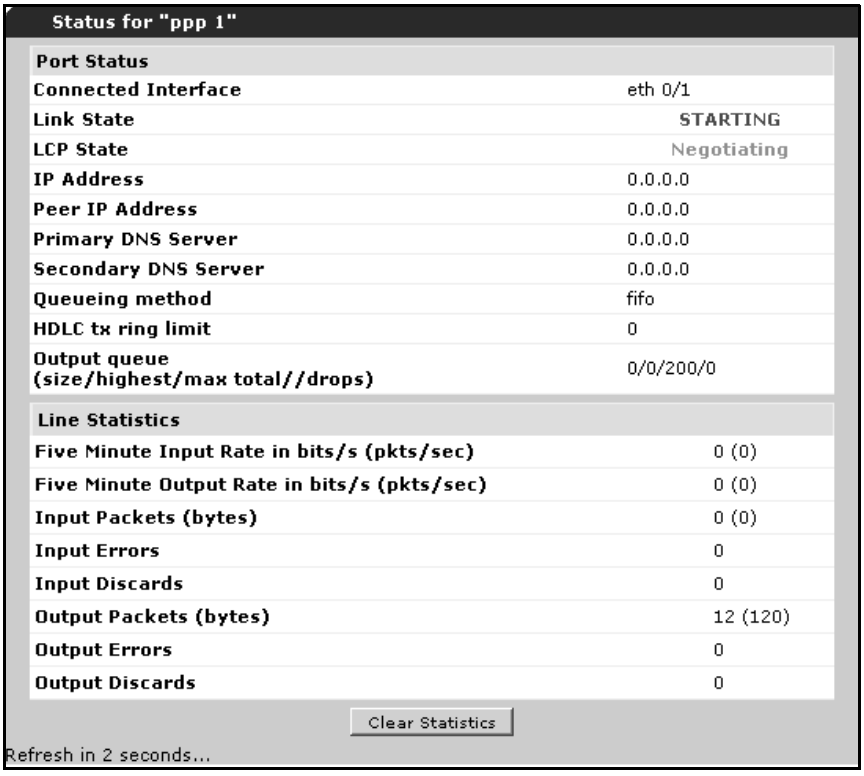

Figure 14-38. View Statistics for PPPoE

Configuring E1 and T1 Interfaces

When you set up an E1- or T1-carrier line, you must configure the Physical Layer and the Data Link Layer. This section explains how to configure the Physical Layer—the E1 or T1 interface—if you have purchased:

- an E1 module that includes a built-in Digital Service Unit (DSU)
- a T1 module that includes a built-in Channel Service Unit (CSU)/DSU

If your public carrier provides an external CSU/DSU, see "Configuring a Serial Interface for an E1- or T1-Carrier Line" on page 14-59.

When you configure the E1 or T1 interface, you must configure the same settings that your public carrier's equipment uses. If you need additional information about any of the options, see *Chapter 4: Configuring E1 and T1 Interfaces*.

1. In the navigation bar of the Web browser interface, select *Physical Interfaces*. The interfaces for all of the modules installed in the router are listed on the *Physical Interfaces* window.

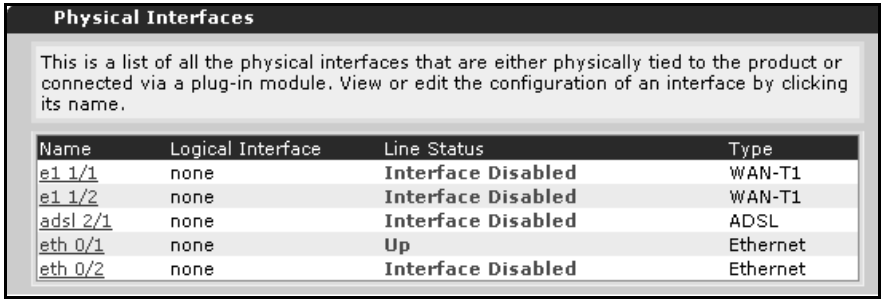

Figure 14-39. Physical Interfaces Window

2. Select the E1 or T1 interface that you want to configure. The *Configuration for the <interface> <slot>/<port>* window is displayed.

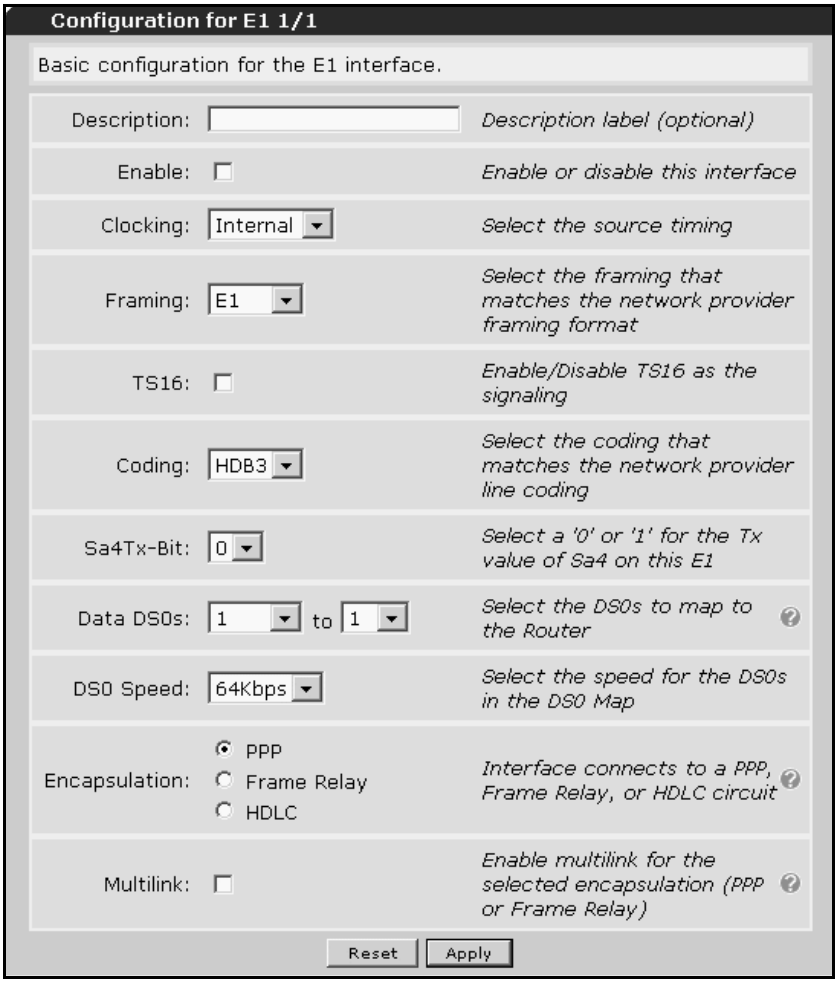

Figure 14-40. Configuration for E1 Interface Window

3. Enter a description in the *Description* box if you want to document information about the E1 or T1 interface. This information will be displayed in the running-config under the appropriate interface heading.
4. To activate the interface, select the *Enable* box and then click *Apply* at the bottom of the window.

5. Configure the clock source for the interface in the *Clocking* pull-down menu.
   - Select *line* if you want the interface to take its timing from the public carrier's equipment.
   - Select *internal* if you want the interface to provide the timing for the connection.
   - Select *through* if you have a module with more than one E1 or T1 port and you want this interface to take its timing from the other interface. (See *Chapter 4: Configuring E1 and T1 Interfaces* for more information about clock sources and when to use the *through* setting.)
6. Set the frame format to match your service provider's settings:
   - If you are configuring an E1 interface, use the pull-down menu to select *E1* or *CRC4*. *E1* is the default setting.
   - If you are configuring a T1 interface, click *ESF* or *D4*. *ESF* is the default setting.

Note

Select the *TS16* box to enable TS16 signaling only if you are configuring the G.703 interface for an E1 + G.703 module. For more information, see "E1 + G.703 and T1 + DSX-1 Modules" on page 14-105.

7. Use the *Coding* pull-down menu to configure the coding to match your service provider's settings:
   - If you are configuring an E1 interface, use the pull-down menu to select *HDB3* or *AMI*. *HDB3* is the default setting.
   - If you are configuring a T1 interface, use the pull-down menu to select *B8ZS* or *AMI*. *B8ZS* is the default setting.
8. If you are configuring a T1 interface, use the pull-down menu to set the facility data link (FDL). The default setting is *ANSI*. You can also select *ATT* or *None*.
9. If you are configuring an E1 interface, you can set the *Sa4Tx-Bit* to 0 or 1. The default setting is 0.
10. In the *Data DS0s* field, configure the channels for the connection. This setting must match the channels configured on your service provider's equipment, or the Data Link Layer protocol cannot establish a connection.
    - If you are leasing the entire E1-carrier line, set the timeslots to 1 to 31.
    - If you are leasing the entire T1-carrier line, set the timeslots to 1 to 24.

11. Accept the default setting of *64 Kbps* for the DS0 speed unless your public carrier tells you to change this setting. Typically, you will change the setting only if you are leasing a T1-carrier line and are using the D4 frame format. In this case, use the pull-down menu to select *56 Kbps*.
12. Select the Data Link Layer protocol for this interface—*PPP*, *Frame Relay*, or High-level Data Link Control (*HDLC*)—and click *Apply*. The *<Protocol> Configuration Settings* window is displayed.
    - If your WAN connection is using PPP, see "Configure PPP as the Data Link Layer Protocol" on page 14-62.
    - If your WAN connection is using Frame Relay, see "Configure Frame Relay as the Data Link Layer Protocol" on page 14-68.
    - If your WAN connection is using HDLC, see "Configure HDLC as the Data Link Layer Protocol" on page 14-74.

Note If you are using PPP or Frame Relay, you can configure a multilink connection. For instructions on configuring this multilink, see *Chapter 2: Increasing Bandwidth* in the *Advanced Management and Configuration Guide*.

Status Information

After you configure the Data Link Layer protocol, a new Data Link Layer section is displayed on the E1 or T1 configuration window. You can now access the configuration window for the Data Link Layer protocol from the E1 or T1 configuration window.

Status information is displayed at the bottom of the E1 or T1 configuration window. This readout refreshes automatically every five seconds. To reset the statistics, click the *Clear Statistics* button.

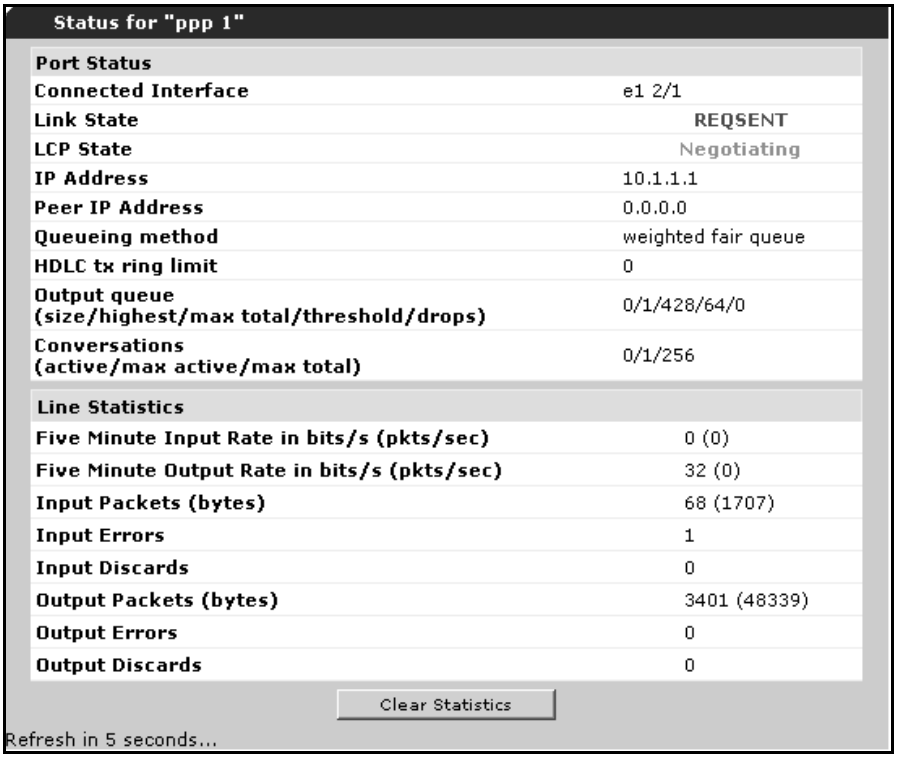

Figure 14-41. Status for E1 Interface

Configuring a Serial Interface for an E1- or T1-Carrier Line

If your public carrier provided you with an external CSU/DSU, you purchased a serial module for the ProCurve Secure Router. When you set up an E1- or T1-carrier line, you must configure the Physical Layer and the Data Link Layer. This section explains how to configure the Physical Layer—the serial interface. If you need additional information about any of the options, see *Chapter 4: Configuring E1 and T1 Interfaces*.

1. In the navigation bar of the Web browser interface, select *Physical Interfaces*. The interfaces for all of the modules installed in the router are listed on the *Physical Interfaces* window.
2. Select the serial interface that you want to configure. The *Configuration for Serial <port number>/<slot number>* window is displayed.

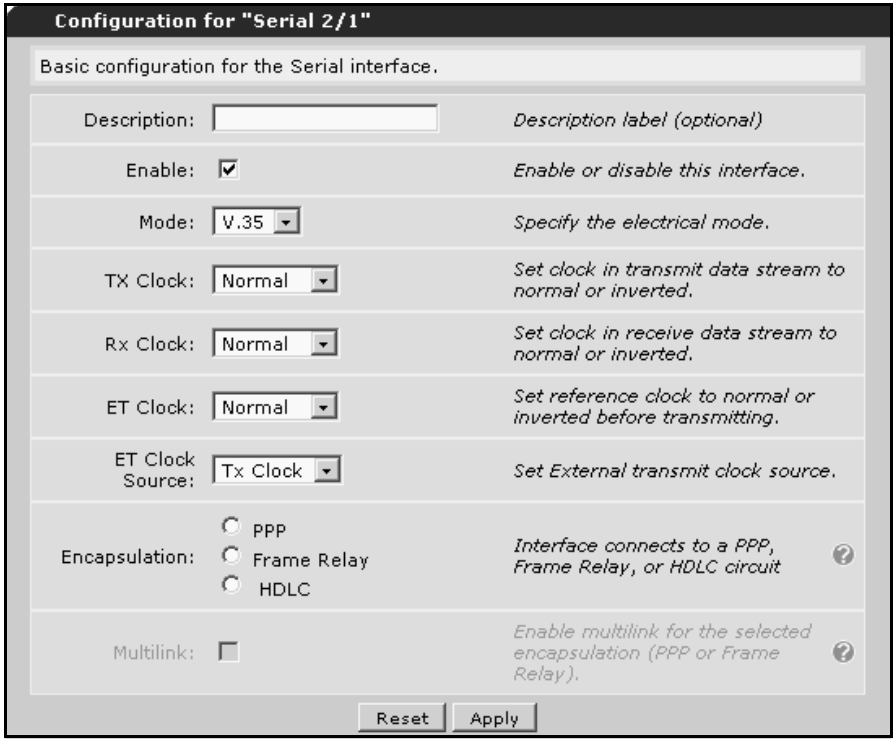

Figure 14-42. Configuration for Serial Window

3. Enter a string of up to 80 characters in the *Description* field if you want to document information about this interface.
4. Select the *Enable* box to activate the interface.
5. For *Mode*, select *V.35* or *X.21*, depending on the type of cable you are using to connect the serial module to the external CSU/DSU. The default setting is *V.35*. If you want to use an *EIA 530* cable from another vendor, the ProCurve Secure Router supports this setting from the CLI. For more information, see *Chapter 5: Configuring Serial Interfaces for E1- and T1-Carrier Lines*.
6. Configure the clock settings.
   a. For *TX Clock*, accept the default setting of *Normal* or select *Inverted* if the router is a long distance from the CSU/DSU.
   b. For *Rx Clock*, accept the default setting of *Normal* or select *Inverted* if the router is a long distance from the CSU/DSU.
   c. For *ET Clock*, accept the default setting of *Normal* or select *Inverted* if the router is a long distance from the CSU/DSU.
   d. For *ET Clock Source*, accept the default setting of *Tx Clock* or select *Rx Clock* if your public carrier tells you to change this setting.
7. For *Encapsulation*, select the Data Link Layer protocol that your public carrier is using. Click *Apply* to save your changes. The *<Protocol> Configuration Settings* window is displayed.
   - If your WAN connection is using PPP, see "Configure PPP as the Data Link Layer Protocol" on page 14-62.
   - If your WAN connection is using Frame Relay, see "Configure Frame Relay as the Data Link Layer Protocol" on page 14-68.
   - If your WAN connection is using HDLC, see "Configure HDLC as the Data Link Layer Protocol" on page 14-74.

Note

If you are using PPP or Frame Relay, you can configure a multilink connection. For instructions on configuring this multilink, see "Configuring MLPPP" on page 16-24 or "Configuring MLFR" on page 16-26. (These sections are in *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* in the *Advanced Management and Configuration Guide.*)

Status Information

Status information is displayed at the bottom of the *Configuration for Serial* window. This readout refreshes every five seconds. To reset the statistics, click the *Clear Statistics* button.

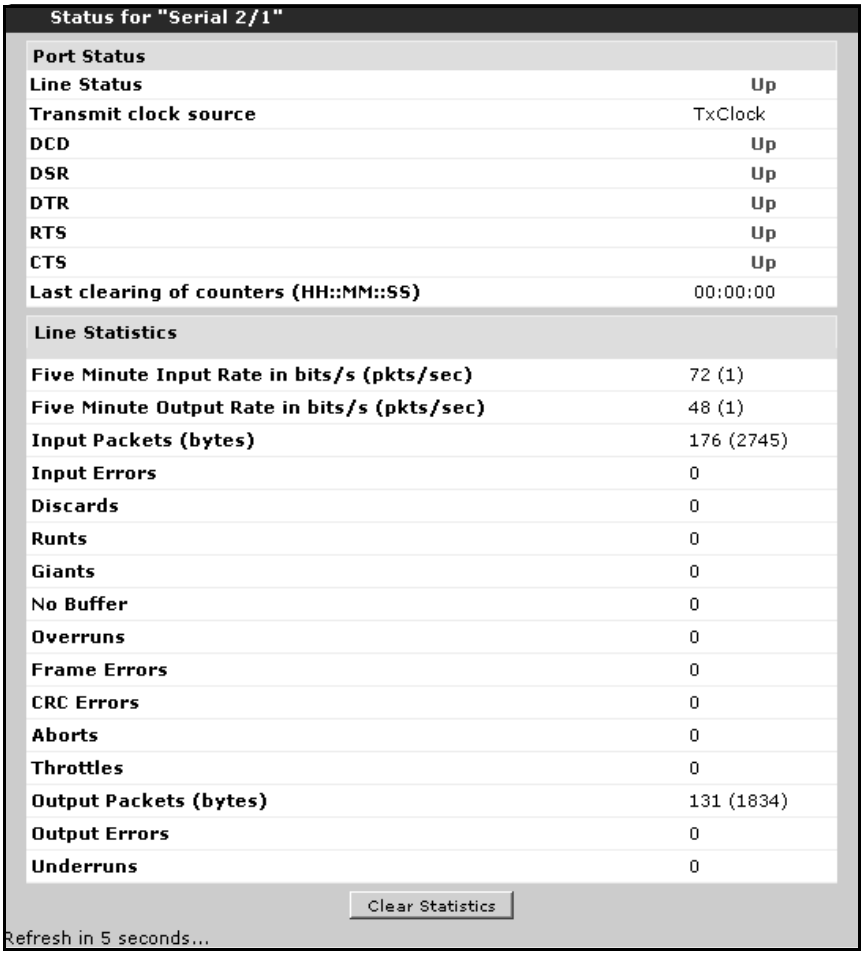

Figure 14-43. Status for Serial Interface

Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces

This section explains how to configure the Data Link Layer protocol for an E1, T1, or Serial interface. You should configure the physical interface to use the same Data Link Layer protocol that your public carrier is using:

- For PPP, see "Configure PPP as the Data Link Layer Protocol" below.
- For Frame Relay, see "Configure Frame Relay as the Data Link Layer Protocol" on page 14-68.
- For HDLC, see "Configure HDLC as the Data Link Layer Protocol" on page 14-74.

If you need additional information about any of the options, see *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces*.

Configure PPP as the Data Link Layer Protocol

The following steps explain the initial configuration of PPP as the Data Link Layer protocol. It is assumed that you have configured the Physical Layer—the E1, T1, or serial interface—and you have selected PPP as the Data Link Layer protocol. As a result, the *PPP Configuration* window is displayed.

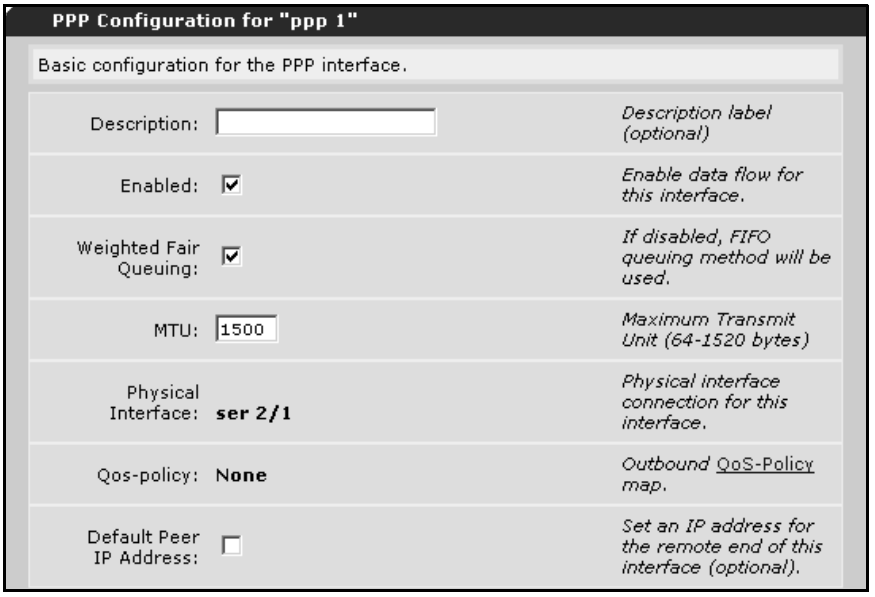

Figure 14-44. PPP Configuration Window

1. From the *PPP Configuration* window, enter a string of text up to 80 characters in the *Description* box if you want to record information about the PPP interface. This description will be displayed in the running-config.
2. Select the *Enabled* box to activate the interface.
3. If you do not want the interface to use Weighted Fair Queuing (WFQ), check the box to deselect it. For more information about WFQ, see "Configuring WFQ" on page 16-59 in *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* of the *Advanced Management and Configuration Guide*.
4. For most environments, you will accept the default MTU of 1500. If you need to adjust the MTU, however, enter the new value in the *MTU* box.
5. Verify that the PPP interface is bound to the correct physical interface.
6. If you have not set a QoS Policy, *None* is displayed for its QoS policy. To create a QoS policy, see "Configuring Quality of Service" on page 16-58 in *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* of the *Advanced Management and Configuration Guide*.
7. To configure the IP address of the PPP peer, select the *Default Peer IP Address* box, and enter the IP address in the boxes provided.
8. To configure authentication, see "PPP Authentication" on page 14-65.

IP Settings

9. For *Address Type* select one of the following.
   - *None*—Select this setting if you intend to set up a bridge group with the PPP interface.
   - S*tatic*—Select this setting if you want to configure a static IP address. The boxes to enter the IP address and subnet mask are displayed, so that you can enter the appropriate address for the PPP interface.
   - *Unnumbered*—To set up the PPP interface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

     Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame-Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.
   - *Negotiated*—Select this setting if you want the PPP interface to negotiate an IP address from your service provider. Select *Default Route* if you want to configure the interface to receive a default gateway from the peer.

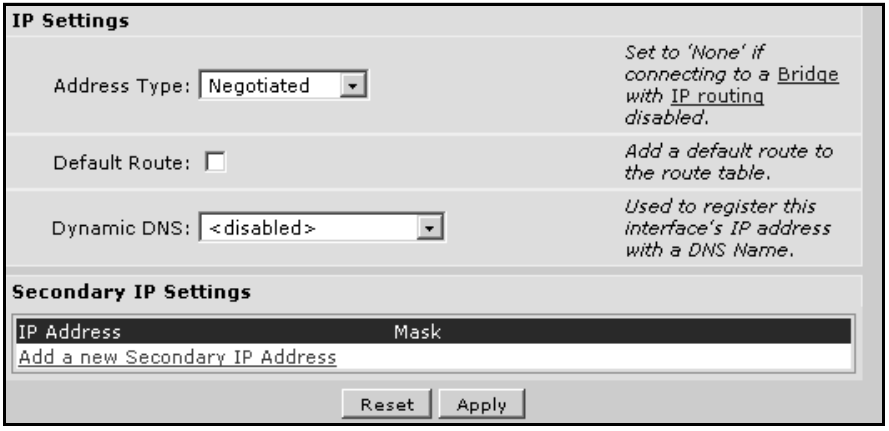

Figure 14-45. IP Settings

Dynamic DNS

10. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
    a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
    b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
    c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
    d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.

Secondary IP Settings

11. To configure secondary IP addresses for your PPP interface, click *Add a new Secondary IP Address*. Then enter the IP address and subnet mask in the boxes provided.
12. Click *Apply* to activate your configurations.

Status Information

Status information is displayed at the bottom of the *Configuration PPP* window. After you apply your changes, the *PPP Link State* will be "starting," indicating that the ProCurve Secure Router OS is trying to establish a PPP connection with its peer. Ensure that the *PPP Link State* is eventually "up." For information about troubleshooting PPP, see "Troubleshooting the PPP Interface" on page 6-59 of *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces*

PPP Authentication

The ProCurve Secure Router supports two authentication protocols for PPP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

When a ProCurve Secure Router asks a peer to authenticate itself using PAP, the peer sends its password in clear text over the wire. The first router matches the password to the password in its PPP database.

CHAP is more secure because the actual password does not cross the wire, where anyone could intercept it. The peer that is authenticating itself hashes its password and sends the hash value to the challenging peer instead. The challenger, who has the password stored in its PPP database, performs the same hash function. It compares the result with the value it received from the peer.

Both peers must use the same protocol.

You can configure the ProCurve Secure Router to require authentication from a peer, or to authenticate itself to a peer, or both.

Requiring a Peer to Authenticate Itself to the Local Router

1. Select *Physical Interfaces* under *System* in the navigation bar.
2. Choose the logical interface for the connection whose remote endpoint you want to authenticate. (It must, of course, be a PPP interface.)
3. You will enter the *PPP Config* window. Move to *Authentication Settings* in the *PPP configuration for "ppp <interface number>"* window.

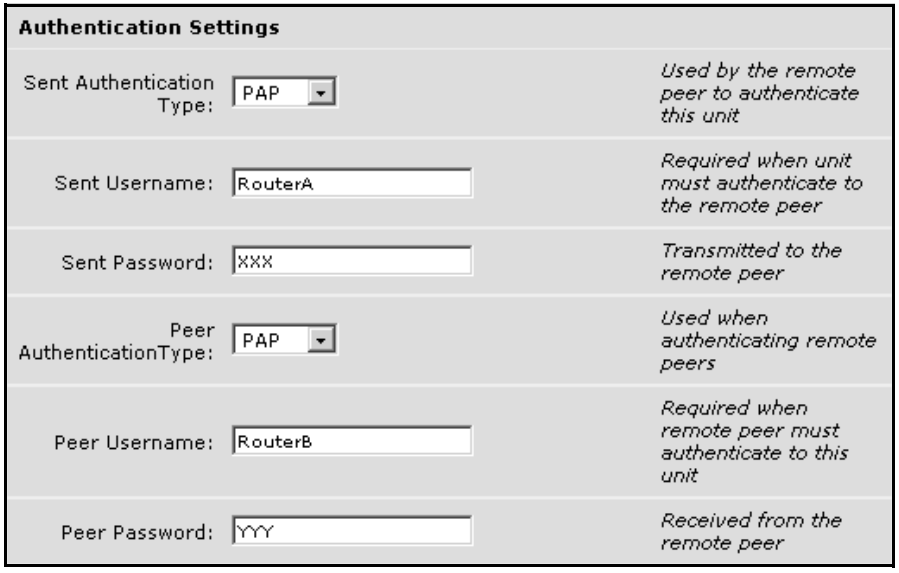

Figure 14-46. Configuring Two-Way PAP Authentication

4. In the pull-down menu for *Peer Authentication Type*, select *PAP* or *CHAP*.

5. Enter the remote endpoint's username and password in the *Peer Username* and *Peer Password* fields. For example, in Figure 14-46, the peer's username is RouterB and its password is YYY. For CHAP the username should be the peer's hostname.
6. Click *Apply*.
7. You also configure the local router to authenticate itself to the peer although this is not necessary. (See "Configuring the Local Router to Authenticate Itself to a Peer" on page 14-67.)

Configuring the Local Router to Authenticate Itself to a Peer

1. Select *System* > *Physical Interfaces*.
2. Choose the logical interface for the connection whose remote endpoint requires the router to authenticate itself (for example, your ISP).
3. You will enter the *PPP Config* window. Move to *Authentication Settings* in the *PPP configuration for "ppp <interface number>"* window.

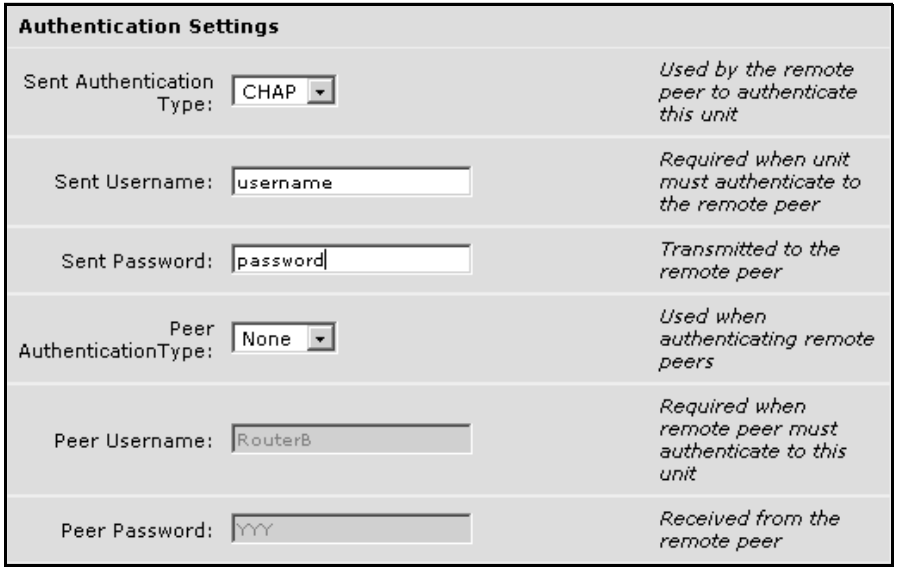

Figure 14-47. Configuring the Local Router to Authenticate Itself

4. In the pull-down menu for *Sent Authentication Type*, select *PAP* or *CHAP*. The protocol must match that requested by the peer. If you do not know the protocol your peer is using, you will either have to contact the peer

or view PPP debug messages in the CLI. (See "PPP Authentication" on page 6-11 of *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces*.)

5. Enter the local router's username and password in the *Sent Username* and *Sent Password* fields. If you are using CHAP, you only have to enter a username if it is different from the router's hostname.
6. Click *Apply*.

Configure Frame Relay as the Data Link Layer Protocol

The following steps explain the initial configuration of Frame Relay as the Data Link Layer protocol. It is assumed that you have configured the Physical Layer—the E1, T1, or serial interface—and you have selected Frame Relay as the Data Link Layer protocol. As a result, the *Frame Relay Configuration* window is displayed.

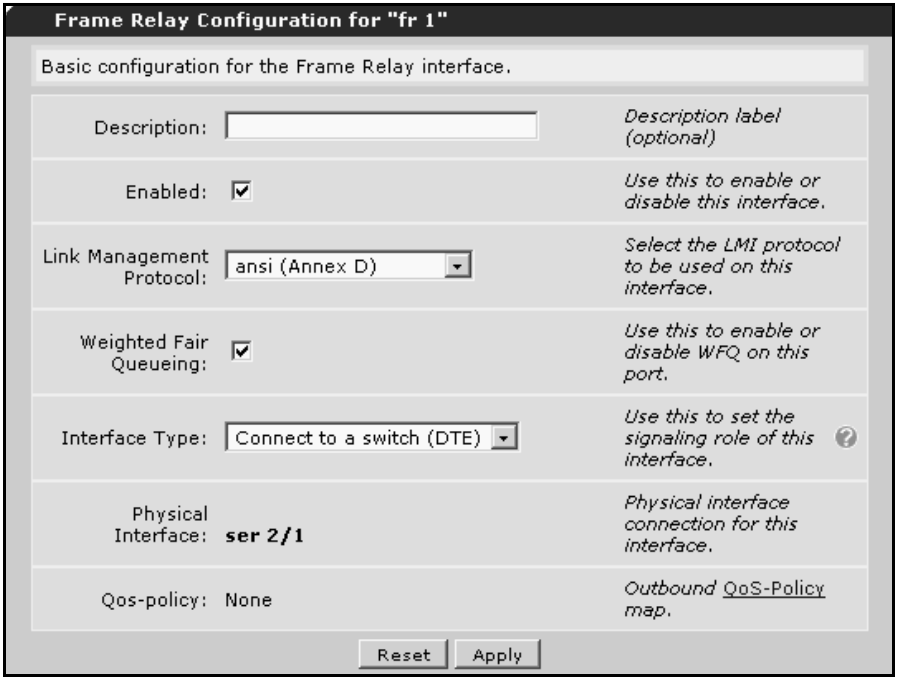

Figure 14-48. Frame Relay Configuration Window

1. From the *Frame Relay Configuration* window, enter a string of text up to 80 characters in the *Description* box if you want to record information about the WAN connection. This information will be displayed in the running-config.
2. Select the *Enabled* box to activate the interface.
3. Use the pull-down menu to select the *Link Management Protocol* that your Frame Relay service provider is using:
   - *ansi (Annex D)*
   - *cisco (Group of Four)*
   - *none*
   - *q933a (Annex A)*
   - *Auto*

   The default setting is *ansi*.
4. *Weighted Fair Queuing* (WFQ) is enabled by default. If you do not want the interface to use WFQ, check the box to deselect it. For more information about WFQ, see "Configuring WFQ" on page 16-59 in *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* of the *Advanced Management and Configuration Guide*.
5. Use the pull-down menu to select the Frame Relay's signaling role:
   - If this interface is acting as Data Terminal Equipment, select *Connect to a switch (DTE)*. For most environments, you will select this setting.
   - If this device is acting as Data Communications Equipment, select *Act like a switch (DCE)*.
   - If this Frame Relay interface will act as both DTE and DCE, select *Both*.
6. Verify that the Frame Relay interface is bound to the correct physical interface. The *Physical Interface* field displays the interface *<slot>/<port>* that is connected to the logical Frame Relay interface that you are configuring.
7. If you have not set a QoS Policy, this Frame Relay interface will display *None* for its QoS policy. For instructions on setting a QoS policy, see "Configuring Quality of Service" on page 16-58 of *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* in the *Advanced Management and Configuration Guide*.
8. Click *Apply* to activate the settings.

Configure a Permanent Virtual Circuit (PVC)

The *Configured Permanent Virtual Circuits* section allows you to create and display PVCs for this WAN connection.

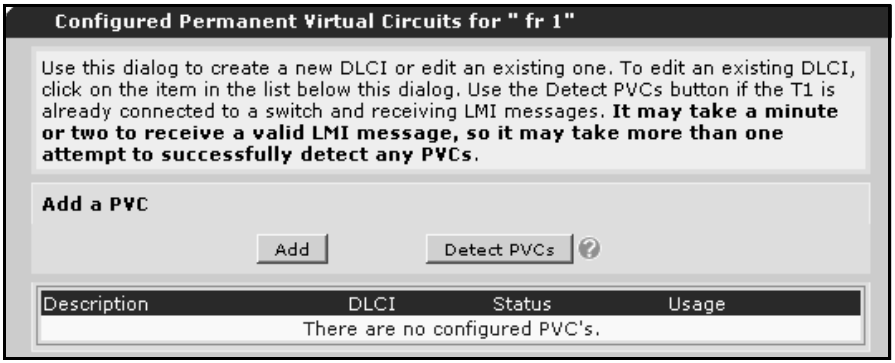

Figure 14-49. Configured Permanent Virtual Circuits Section

9. To create and configure a PVC, click the *Add* button. The *Configuration* window is displayed.

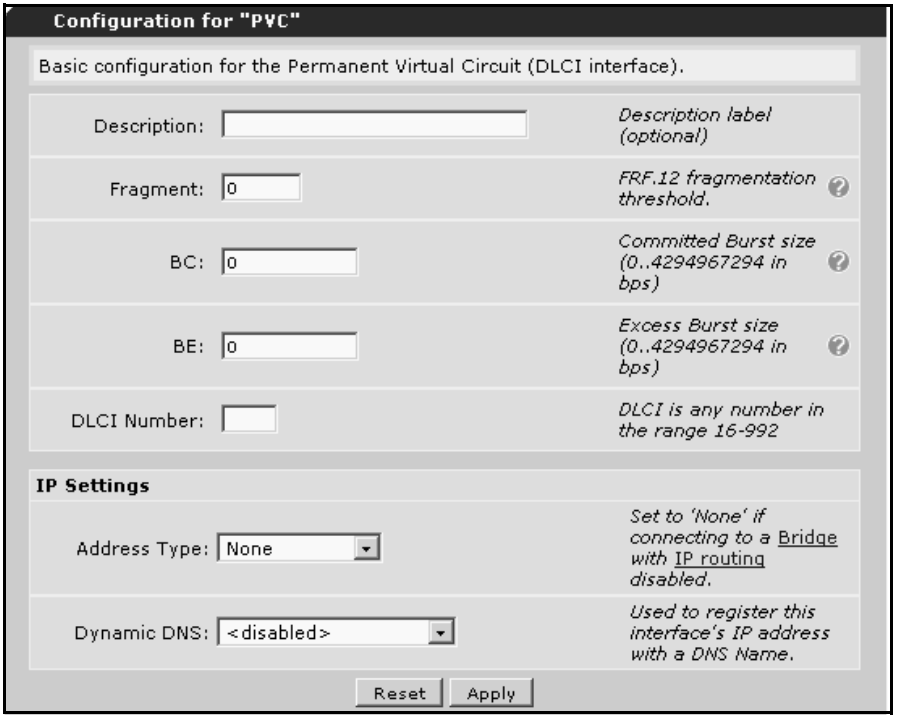

Figure 14-50. Configuration for Frame Relay Subinterface Window

1. Enter a string of text up to 80 characters in the *Description* box if you want to record information about the Frame Relay subinterface. This description will be displayed in the running-config under the appropriate interface heading.
2. Set the FRF.12 fragment threshold by entering the size in the *Fragment* box.
3. Set the committed burst rate in the *BC* box.
4. Set the excess burst rate in the *BE* box.
5. In the *DLCI Number* box, enter the DLCI that your Frame Relay service provider assigned you. This number must be between 16 and 992.

Configure IP Settings

6. Configure the IP settings for the Frame Relay subinterface.
   - *None*—Select this setting if you intend to set up a bridge group with the Frame Relay subinterface.

- S*tatic*—Select this setting if you want to configure a static IP address. Enter the appropriate address for the Frame Relay subinterface in the boxed provided.
- *DHCP*—Select this setting to configure the subinterface as a Dynamic Host Configuration Protocol (DHCP) client.
- *Unnumbered*—To set up the Frame Relay subinterface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

  Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame-Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.

Configure Dynamic DNS

7. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
   a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
   b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
   c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
   d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.
8. Click *Apply* to activate your settings.
9. Repeat steps 9 through 17 for each PVC you need to configure for the Frame Relay interface.

Status Information

10. To view information about the Frame Relay subinterface, scroll to the bottom of the *Configuration for Frame Relay subinterface* window.

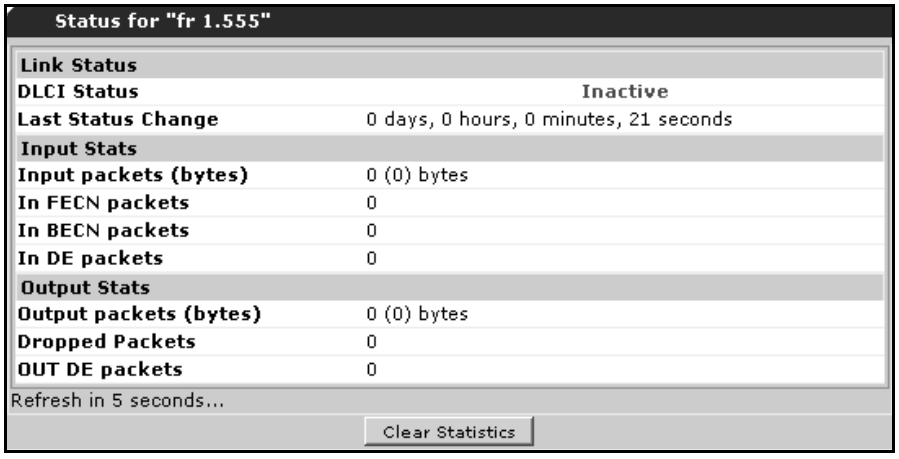

Figure 14-51. Statistics for Frame Relay Subinterface

11. The status information refreshes automatically every five seconds. Reset statistics by clicking the *Clear Statistics* button.
12. To view status information about the Frame Relay interface and LMI status, return to the *Frame Relay Configuration* window and scroll to the bottom of the window.

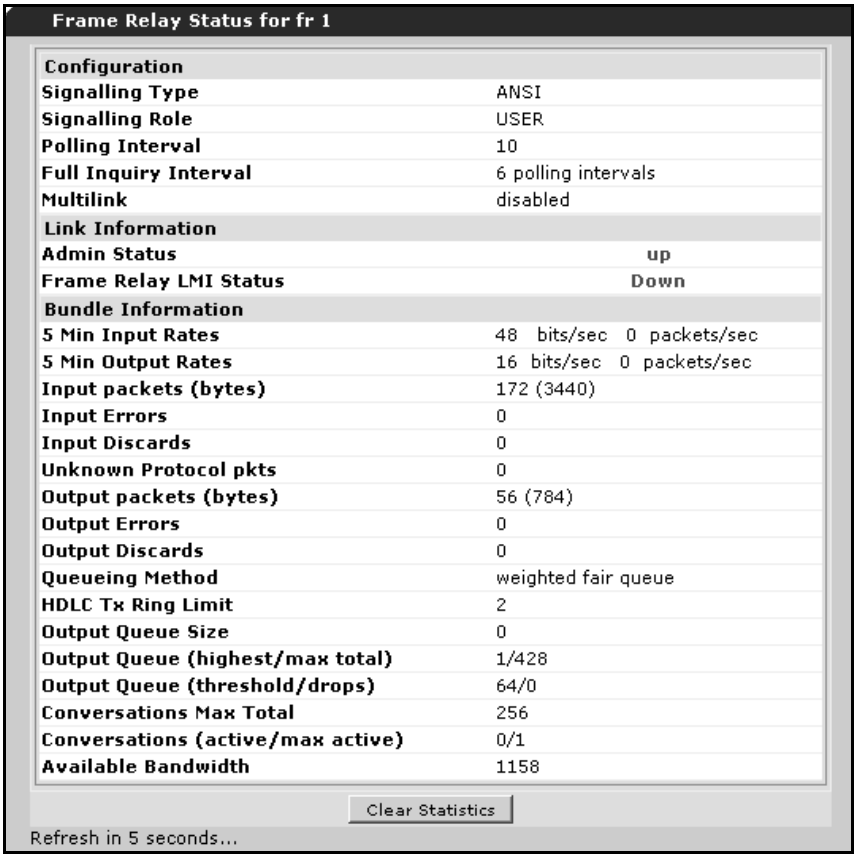

Figure 14-52. Statistics for Frame Relay Interface

Configure HDLC as the Data Link Layer Protocol

The following steps explain the initial configuration of HDLC as the Data Link Layer protocol. It is assumed that you have configured the Physical Layer—the E1, T1, or serial interface—and you have selected HDLC as the Data Link Layer protocol. As a result, the *HDLC Configuration* window is displayed.

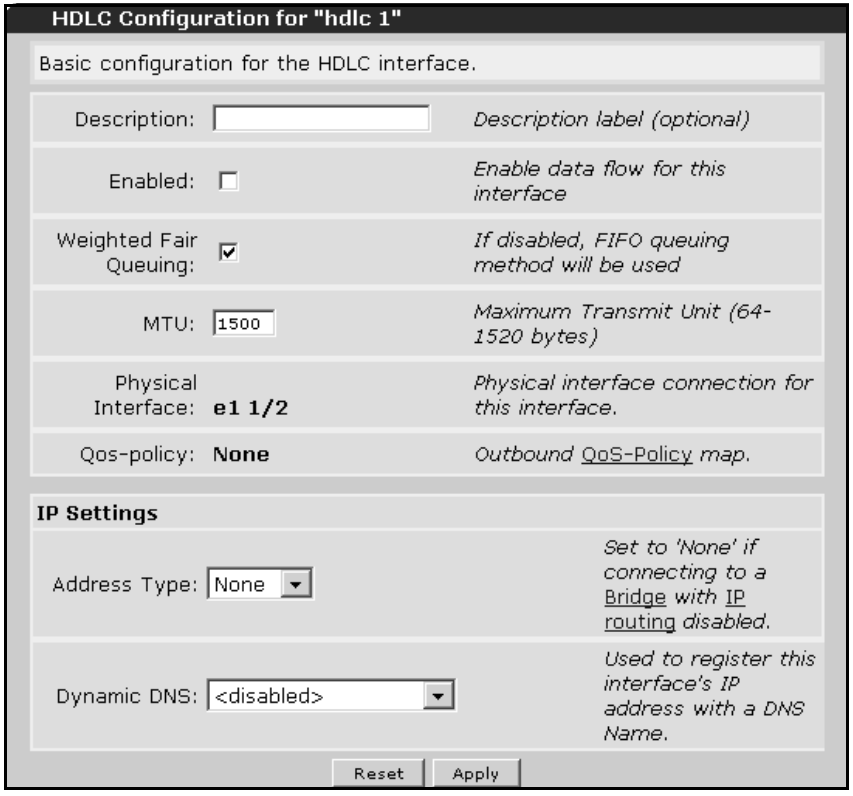

Figure 14-53. HDLC Configuration Window

1. Enter a description in the *Description* box if you want to record some information about the HDLC interface. This information will be displayed in the interface's running-config.
2. Click the *Enabled* box to activate the interface.
3. If you do not want the interface to use *Weighted Fair Queuing*, check the box to deselect it. For more information about WFQ, see "Configuring Quality of Service" on page 16-58 of *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks* in the *Advanced Management and Configuration Guide*.
4. For most environments, you will accept the default MTU of 1500. If you need to adjust the MTU, however, enter the new value in the *MTU* box.
5. Verify that the HDLC is bound to the proper physical interface by checking the *Physical Interface* field.

6. If you have not set a QoS Policy, this HDLC interface will display *None* for its QoS policy.

IP Settings

7. Configure IP Settings.
   - *None*—Select this setting if you intend to set up a bridge group with the HDLC interface.
   - S*tatic*—Select this setting if you want to configure a static IP address. The boxes to enter the IP address and subnet mask are displayed, so that you can enter the appropriate address for the HDLC interface.
   - *DHCP*—Select this setting to configure the HDLC interface as a DHCP client.
   - *Unnumbered*—To set up the HDLC interface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

     Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.

Dynamic DNS

8. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
   a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
   b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
   c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
   d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.
9. Click *Apply* to activate your settings.

Status Information

You can also check the HDLC interface statistics in the *Status for "hdlc <interface>"* section. To reset the statistics, click the *Clear Statistics* button. To get real-time updates, click *Continuous Refresh*. To stop continuous refresh, click the *Stop Refreshing* button.

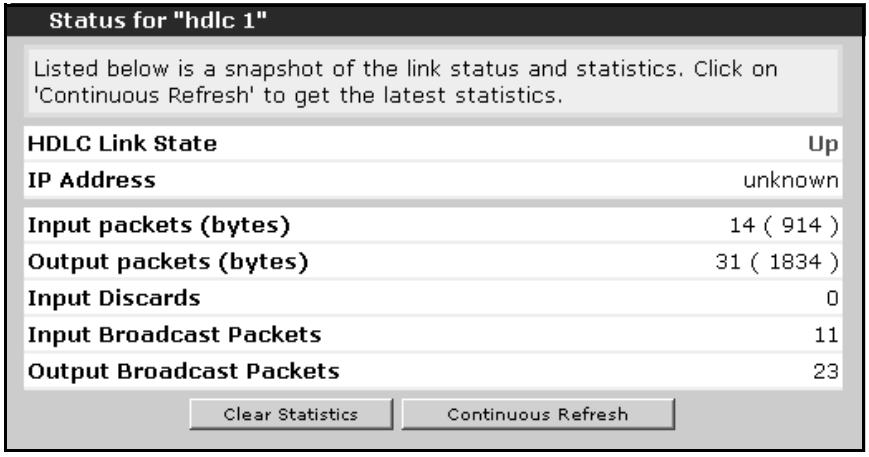

Figure 14-54. Status for HDLC Interface

Configuring ADSL Interfaces

To configure the ProCurve Secure Router to support an Asymmetric Digital Subscriber Line (ADSL), complete the following steps. If you need more information about any of the ADSL or Asynchronous Transfer Mode (ATM) options, see *Chapter 7: ADSL WAN Connections*.

1. From the navigation bar, click *Physical Interfaces*. The *Physical Interfaces* window is displayed.

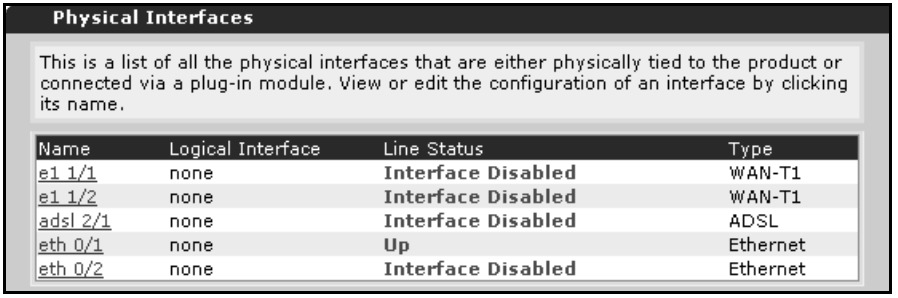

Figure 14-55. Physical Interfaces Window

2. From the list of physical interfaces that are listed, click the ADSL interface that you want to configure. The *Configuration for ADSL* window is displayed.

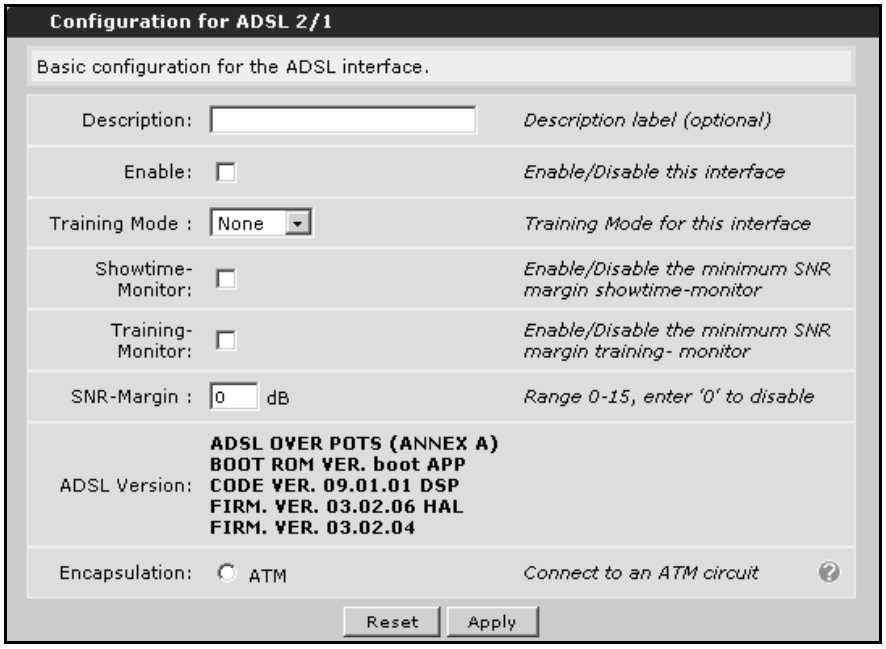

Figure 14-56. Configuration for ADSL Window

3. Enter a description for the interface if you want to document information about the ADSL connection. The description is displayed when you view the running-config file.
4. Click the *Enable* box to activate the ADSL interface.
5. Use the pull-down menu to select the *Training Mode* that your ADSL service provider is using.
6. Select the *Showtime-Monitor* if you want to monitor the signal-to-noise ratio (SNR)-margin after the physical connection has been established.
7. Select the *Training-Monitor* if you want to monitor the SNR-margin during the training phase.
8. In the box provided for the *SNR-Margin*, enter the SNR margin in decibels.
9. The *ADSL Version* displays the type of ADSL module installed in the router and information about the module's boot ROM and firmware.
10. Select *ATM* as the encapsulation.
11. Click *Apply* to save your changes to the startup-config. The *Configuration for "atm <interface>"* window is displayed. (See Figure 14-57.)

Configure an ATM Interface

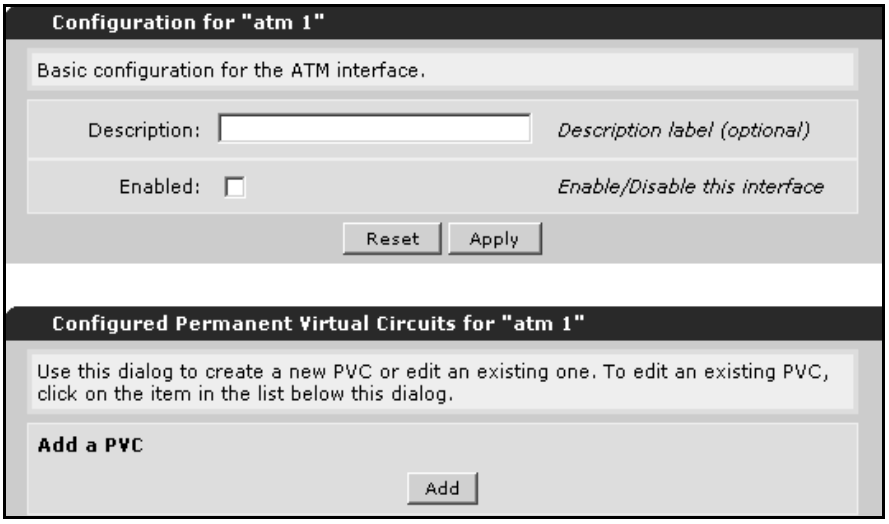

Figure 14-57. Configuration for ATM Interface Window

12. Enter a description if you want to document information about the ATM interface.
13. Click the *Enabled* box to activate the ATM interface.
14. Click *Apply* to save your changes to the startup-config.

Configure the ATM Subinterface

15. In the *Configured Permanent Virtual Circuits* section, click the *Add* button to begin configuring the permanent virtual circuit (PVC). The *Configuration for "atm <subinterface>"* window is displayed.

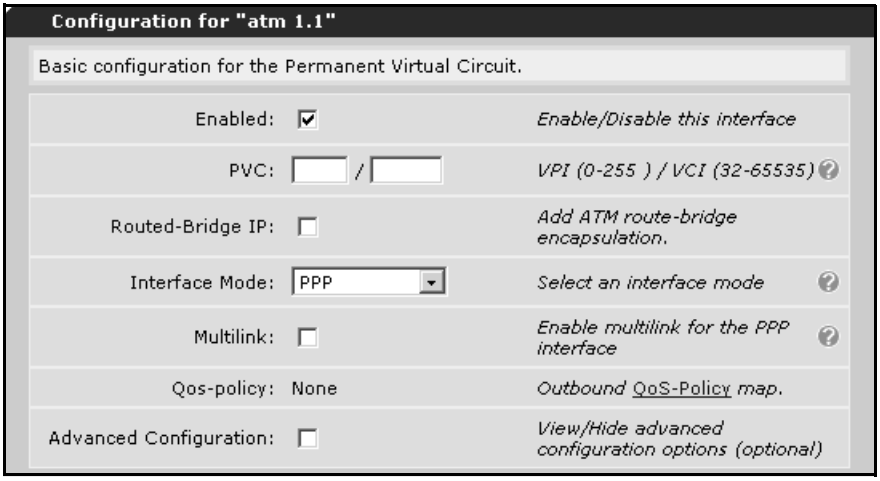

Figure 14-58. Configuration for ATM Subinterface Window

16. Click the *Enabled* box to activate the subinterface.
17. For PVC, enter the virtual path identifier (VPI) in the first box, and enter the virtual channel identifier (VCI) in the second box. For example, if your ADSL service provider assigned you a VPI/VCI of 0/33, you would enter 0 in the first box and 33 in the second box.
18. For *Interface Mode*, use the pull-down menu to select one of the following:
    - *IP routing*, if you are configuring just ATM as the Data Link Layer protocol
    - *PPPoE client*, if you are configuring PPPoE for the ADSL interface
    - *PPP*, if you are configuring PPPoA
19. If your ADSL service provider uses routed bridged encapsulation (RBE), select the *Routed-Bridge IP* box.
20. To configure the ATM encapsulation method, quality of service (QoS) settings, and Operation, Administration, and Maintenance (OAM) settings, click the *Advanced Configuration* box at the top of the *Configuration for ATM Subinterface* window. The *Advanced Configuration* section is displayed.

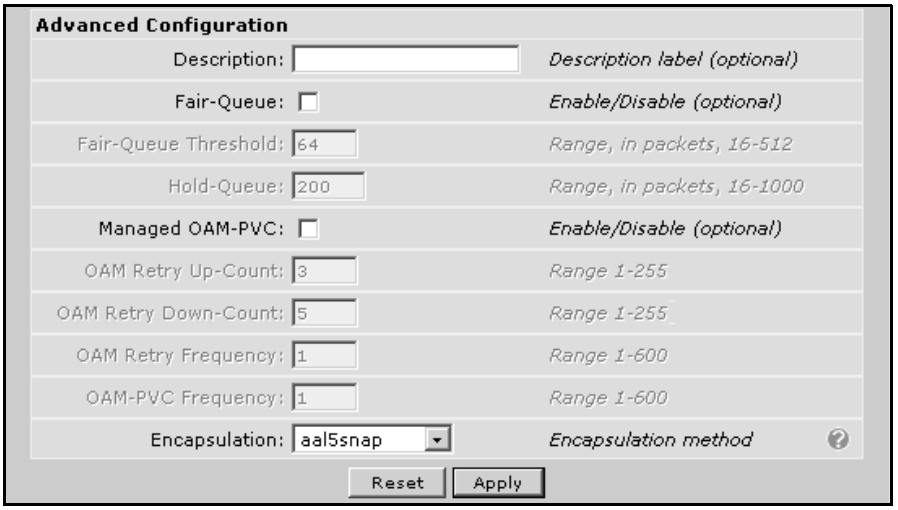

Figure 14-59. Advanced Configuration Section

21. Configure *Fair-Queue*, *Fair-Queue Threshold*, and *Hold-Queue* settings if you want to configure QoS on this interface.
22. Select *Managed OAM-PVC* to manage the Operation, Administration, and Maintenance (OAM) cells. These cells are sent over a reserved VCI to monitor the ATM link, ensuring that it is open from end-to-end. After you select the Managed OAM-PVC option, you can then configure:
    - *OAM Retry Up-Counts*—determines the number of consecutive, end-to-end F5 OAM loopback cell responses that the ADSL interface must receive before the Secure Router OS changes a PVC connection state to up. For this option, configure a number between 1 and 255. The default setting is 3.
    - *OAM Down-Counts*—determines the number of consecutive, end-to-end F5 OAM loopback cell responses that are not received before the Secure Router OS changes the PVC state to down. Specify a number between 1 and 255. The default setting is 5.
    - *OAM Retry Frequency*—determines the frequency (in seconds) at which the ADSL interface transmits F5 OAM loopback cells when verifying a PVC state change. Specify a number of seconds between 1 and 600. The default setting is 1 second.

- *OAM PVC Frequency*—determines the time delay between OAM loopback cells. This setting is used unless the router is verifying a PVC state change (in which case it uses the *OAM retry frequency* setting). Specify a number between 0 to 600 seconds. The default setting is 1 second.

23. Select the encapsulation setting that your ADSL service provider is using:
    - *aalsnap*
    - *aalmux ip*
    - *aalmux ppp*
24. Click *Apply* to save your settings to the startup-config.

If you are configuring just ATM as the Data Link Layer protocol, continue with the next section. If you are configuring PPPoE or PPPoA, you must configure a PPP interface. See "Configuring PPPoE or PPPoA for the ADSL Connection" on page 14-85.

Configuring ATM Only

25. After you select IP routing, a new section called *IP Settings* is displayed.

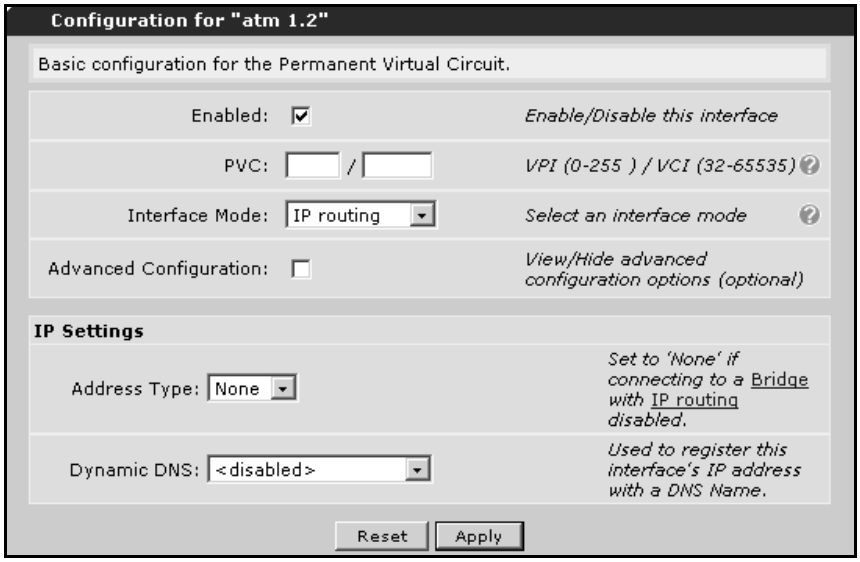

Figure 14-60. IP Settings Section

26. For *Address Type*, use the pull-down menu to select:
    - *None*—Select *None* if you want this interface to be part of a bridge.
    - *Static*—Select *Static* if you want to configure a fixed IP address for the interface. When new fields are displayed, enter an IP address and subnet mask.
    - *DHCP*—Select DHCP if your ADSL service provider wants you to receive an IP address from its DHCP server.
27. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
    a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
    b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
    c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
    d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.
28. Click *Apply* to save your configuration.

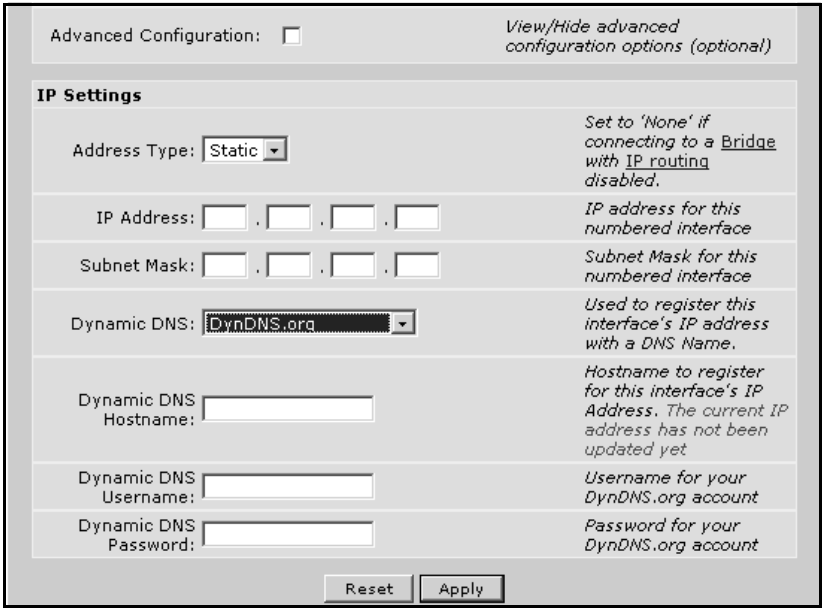

Figure 14-61. Configuring Dynamic DNS in the IP Settings Section

Status Information

You can view information about both the ATM interface and subinterface. To view information about the ATM interface, move to the *Configuration for "atm <interface>"* window and scroll to the bottom of the window. Likewise, you can view the status of the ATM subinterface by scrolling to the bottom of the *Configuration for "atm <subinterface>"* window.

Configuring PPPoE or PPPoA for the ADSL Connection

After you select *PPPoE Client* or *PPP* as the *Interface Mode* for the ATM subinterface, a PPP configuration screen is displayed. (See Figure 14-62.) You must then configure the PPP interface:

1. Enter a description if you need to document information about the PPP interface. This information will be displayed in the running-config under the appropriate PPP interface heading.
2. Click the *Enabled* box to activate the PPP interface.
3. For most environments, you can accept the default setting of 1500 for the MTU. If you selected the *PPPoE Client* setting for the ATM *Interface Mode*, the ProCurve Secure Router OS will automatically negotiate an MTU of 1492 with the PPP peer. If the two peers fail to negotiate an MTU of 1492, you may need to set the MTU manually.
4. Select *Default Peer Address* if you want to configure the IP address of the PPP peer.
5. If you want to configure PPP authentication, see "PPP Authentication" on page 14-65.

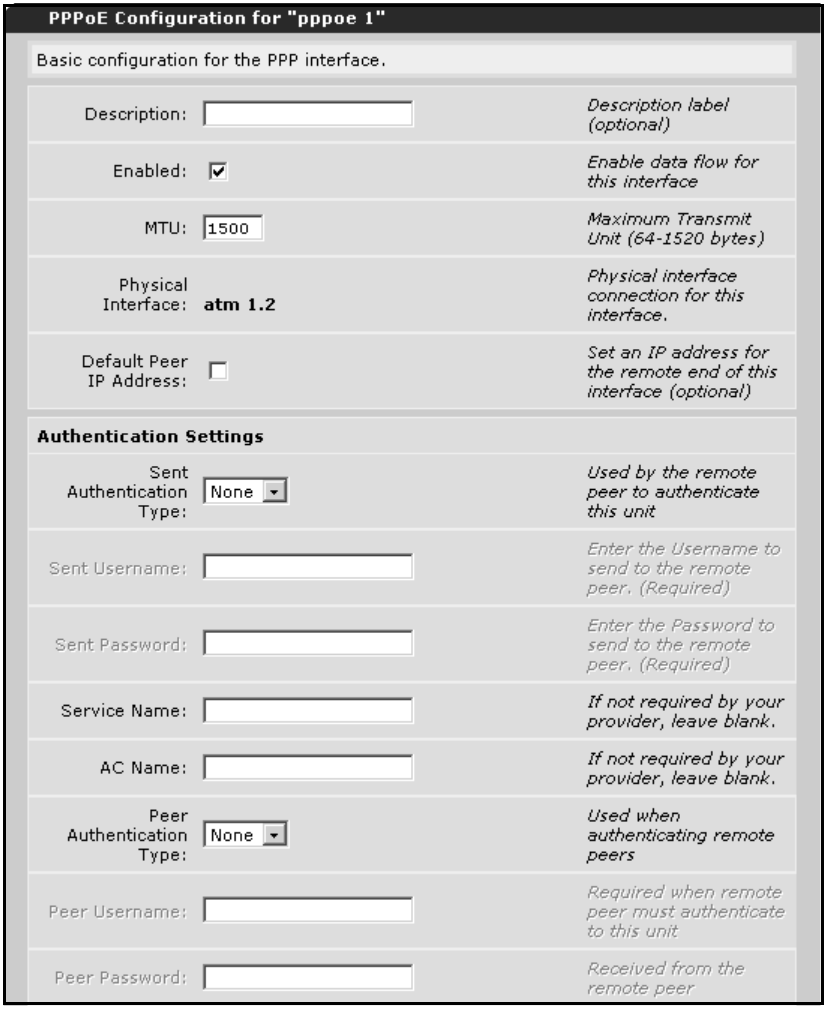

Figure 14-62. PPPoE Configuration Window

6. Configure IP settings. For *Address Type* select one of the following.
   - *None*—Select this setting if you intend to set up a bridge group with the PPP interface.
   - S*tatic*—Select this setting if you want to configure a static IP address. The boxes to enter the IP address and subnet mask are displayed, so that you can enter the appropriate address for the PPP interface.
   - *Negotiated*—Select this setting if you want the PPP interface to negotiate an IP address from your service provider.

- *Unnumbered*—To set up the PPP interface with the same IP address as another interface, click the *Unnumbered* option. The *Interface* box is displayed.

  Use the pull-down menu for the *Interface* box to select the appropriate interface. The menu will display any ATM subinterfaces, Frame Relay subinterfaces, HDLC interfaces, loopback interfaces, and PPP interfaces that are already configured.

7. Select *Default Route* if you want this interface to provide the default route for the router.

Dynamic DNS

8. Configure dynamic DNS, if needed. For more information about dynamic DNS, see "Configuring Dynamic DNS" on page 14-124.
   a. For *Dynamic DNS*, use the pull-down menu to select *DynDNS.org*, *DynDNS.org Static*, or *DynDNS.org Custom*. Additional boxes are displayed, allowing you to configure information about your account with DynDNS.org.
   b. For *Dynamic DNS Hostname*, enter the hostname required to register the interface's IP address.
   c. For *Dynamic DNS Username*, enter the username for your company's account with DynDNS.org.
   d. For *Dynamic DNS Password*, enter the password for your company's account with DynDNS.org.

Secondary IP Settings

9. To configure secondary IP addresses for the PPP interface, click *Add a new Secondary IP Address*. Then enter the IP address and subnet mask in the boxes provided.
10. Click *Apply* to activate your configurations.

View Statistics for the PPP Interface

Status information is displayed at the bottom of the PPP configuration window. After you apply your changes, the *PPP Link State* will be "starting," indicating that the ProCurve Secure Router OS is trying to establish a PPP connection with its peer. Ensure that the *PPP Link State* is eventually "up."

Configuring Demand Routing for a Primary or Backup Connection

The process for configuring demand routing through the Web browser interface differs slightly from the process outlined for the CLI. Although you configure the same settings, you configure them in a different order.

When you set up an ISDN connection using demand routing, ProCurve Networking recommends that you configure Point-to-Point Protocol (PPP) authentication to ensure that only authorized peers can establish a connection with your router.

To minimize the cost of your dial-up connection, ProCurve Networking also recommends that you configure the idle timer to match how your company is charged for the line. (If the dial-up connection is idle for the amount of time specified by the idle timers, the ProCurve Secure Router terminates the call)

For example, if your public carrier charges your company for every two minutes that the ISDN line is established, you can set the idle timer to 110 seconds. The ProCurve Secure Router will then disconnect the ISDN line when it has been idle for 110 seconds, and your company will not be charged for an additional two minutes

Configuring an ACL to Define Interesting Traffic

The first step in configuring demand routing is to define the interesting traffic-the traffic that triggers, or activates, the WAN connection. For example, if you are configuring demand routing for an ISDN connection between the main office and a branch office, you could define the interesting traffic on the main office router as the packets with the following source and destination:

- source—from a particular subnetwork at the main office
- destination—to the subnetwork at the branch office

To define interesting traffic for your dial-up connection, you configure an extended ACL:

1. In the left navigation bar of the Web browser interface, click *General Firewall*.
2. Scroll to the bottom of the *General Firewall* screen and click the *Configure ACLs* button. The *Access Control Lists* screen is displayed.

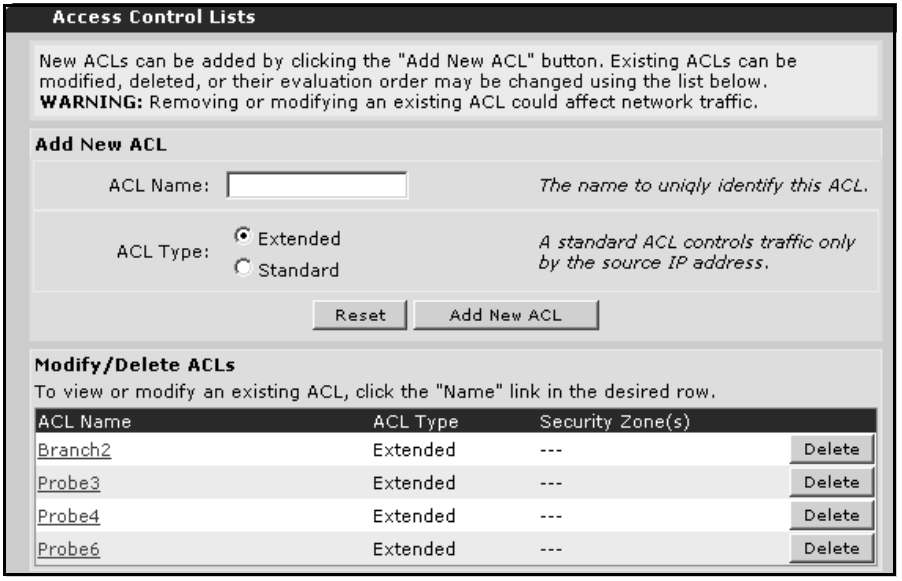

Figure 14-63.Configuring an ACL List

3. In the *ACL Name* field on the *Access Control Lists* screen, enter a name for the extended ACL.
4. In the *ACL Type* field, select *Extended*.
5. Click the *Add New ACL* button. The *Add/Modify/Delete Policy Traffic Selectors* screen is displayed.

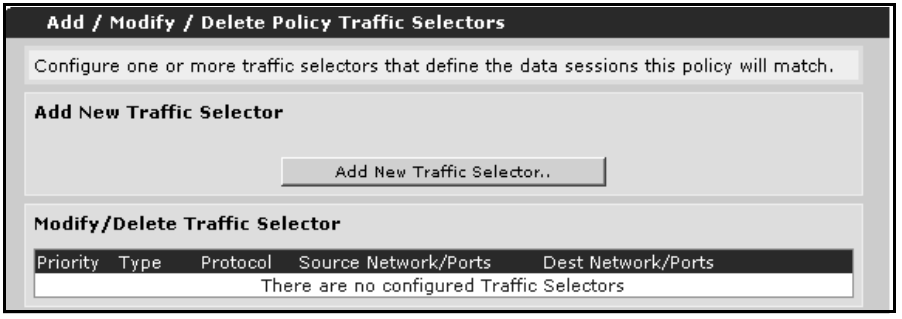

Figure 14-64.Adding a Traffic Selector

6. Click the *Add New Traffic Selector* button. The *Add New Custom Policy Entry* screen is displayed.

7. In the Filter Type field on the A*dd New Custom Policy Entry* screen, select:
   - permit to define traffic that will initiate the dial-up connection
   - deny to define traffic that will be ignored
8. In the *Protocol* field, use the pull-down menu to select traffic based on a particular protocol.
9. In the *Source Data* section, define the source IP address and port.
10. In the *Destination Data* section, define the destination IP address and port.
11. Click the *Apply* button to save your changes. The permit or deny statement that you configured is listed on the *Add/Modify/Delete Policy Traffic Selectors* screen. Add another traffic selector, if necessary.

Configuring the BRI Interface

The next step is to configure the physical interface for demand routing—the BRI interface. Complete the following steps:

1. In the navigation bar of the Web browser interface, select *Physical Interfaces*. The interfaces for all of the modules installed in the router are listed on the *Physical Interfaces* window.
2. The ports on the ISDN module are listed as BRI interfaces. Select the BRI interface that you want to configure. The *Configuration for the BRI <slot>/<port>* window is displayed.

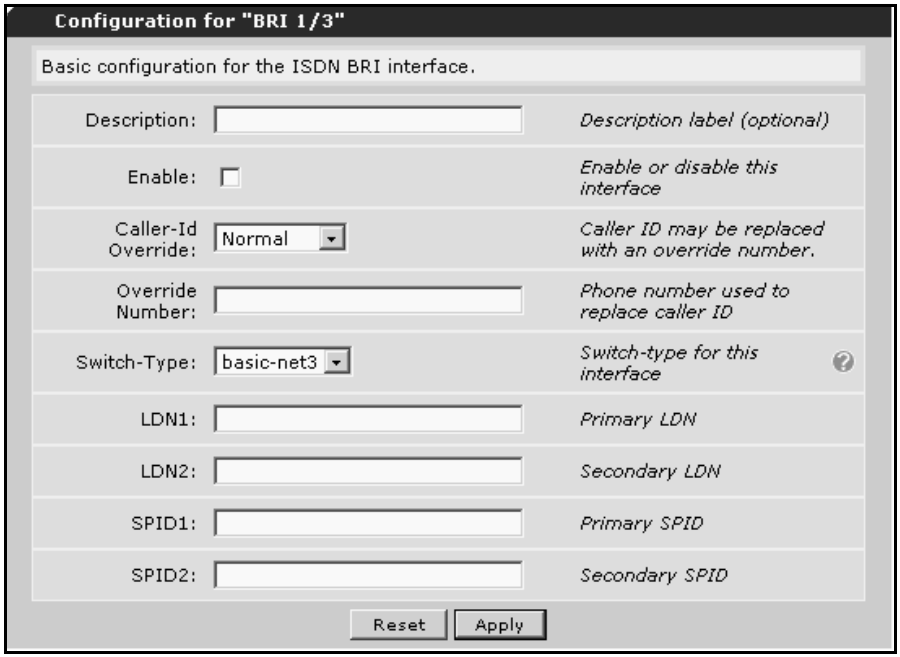

Figure 14-65. Configuration for a BRI Interface

3. Enter a description in the *Description* box if you want to document information about the BRI interface. This information will be displayed in the running-config under the appropriate interface heading.
4. To activate the interface, select the *Enable* box.
5. If you want the BRI interface to replace the caller ID of incoming calls with a different number, select the *Caller Id Override* box. Enter the number that replaces incoming numbers in the *Override Number* field.
6. Select the ISDN signaling used by your service provider from the *Switch-Type* pull-down menu.
7. Enter the local directory number (LDN) for the ISDN line in the *LDN1* field.
8. If your service provider has assigned this line a secondary LDN, enter it in the *LDN2* field.
9. In North America, service providers assign ISDN lines Service Profile Identifiers (SPIDs). Enter your line's primary SPID in the *SPID1* field. If the line has been assigned a secondary SPID, enter it in the *SPID2* field.
10. Click *Apply*.

Troubleshooting the BRI Interface

After you activate the BRI interface, you can view its status. Scroll to the *Status for BRI* window. The *Line Status* indicates whether the interface is up or down and whether it is currently active. You can view the *B1 State*, *B2 State*, and *D-Channel State* to determine which channels are currently active. You can also view statistics for inbound and outbound packets and for errors.

Click the *Continuous Refresh* button to view the statistics in real-time. Click the *Stop Refreshing* button to freeze the display.

Caution

Clicking the *Continuous Refresh* button requires the router to send continuous updates. This consumes bandwidth and may create a security issue.

The line status for the BRI interface shown in Figure 14-66 is "Disabled"; the interface has not succeeded in negotiating with the ISDN switch to bring up the line.

Figure 14-66. Viewing the BRI Interface's Status

You can use the options in the *Maintenance* window to troubleshoot a BRI interface:

- Occasionally, a BRI interface may enter a loop if it does not complete the call disconnect process. Select the *Reset* option and click *Apply* to reset the port hardware.
- You can restart the D-channel by selecting the *Restart-d* option and clicking *Apply*. For example, you might need to restart the D-channel if a problem occurs during the call process.

Configuring an ISDN Group

If you are configuring demand routing for a primary ISDN module, you must configure an ISDN group. If you are configuring demand routing for a backup ISDN module, skip this step.

To configure an ISDN group, complete the following steps:

1. Click *ISDN Group* in the *System* section of the navigation bar.

Figure 14-67. ISDN-Group

2. To add a new ISDN group, click the *Add New Group* button.

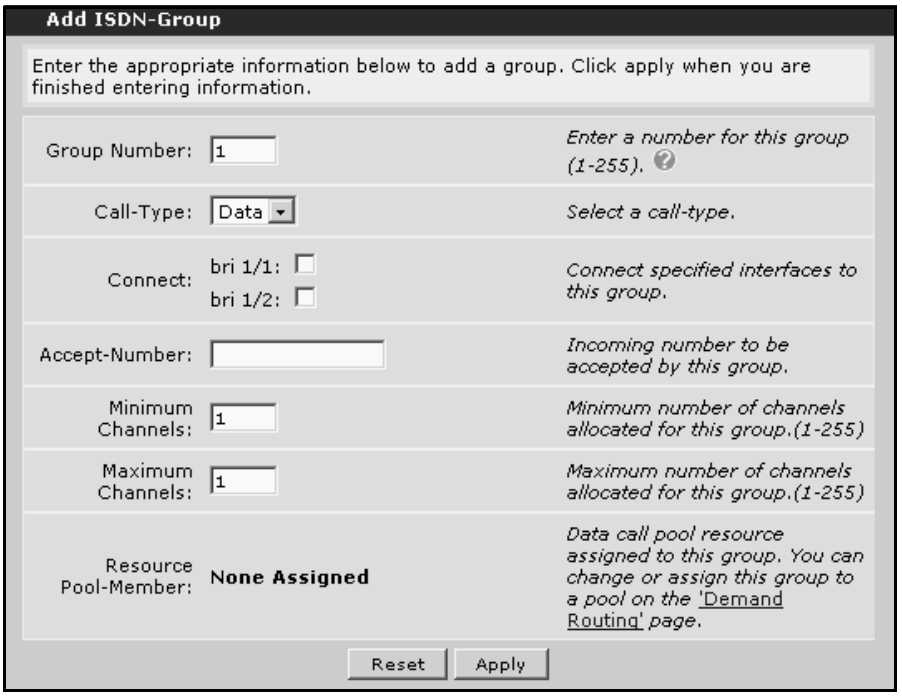

Figure 14-68. Add ISDN-Group

3. In the *Group Number* field on the *Add ISDN-Group* screen, enter a number to identify this group. Each ISDN group must have a unique number, in the range from 1 to 255.
4. In the *Connect* field, select the interfaces that you want to assign to this ISDN group.
5. In the *Accept-Number* field, enter an incoming accept number. The ProCurve Secure Router will accept calls for this ISDN group only from this number.
6. If you want to configure support for multilink PPP, configure the *Minimum Channels* and *Maximum Channels* fields.
7. Click *Apply* to save your changes.

Configuring the Demand Interface

After you configure the ISDN group, you should configure the demand interface. The demand interface handles the Data Link Layer protocol for the demand-routing connection in addition to other functions for the ISDN call. The actual Data Link Layer protocol used for demand-routing connections is PPP.

To add a new demand interface, complete the following steps:

1. Click *Demand Routing* in the *Router/Bridge* section of the navigation bar.

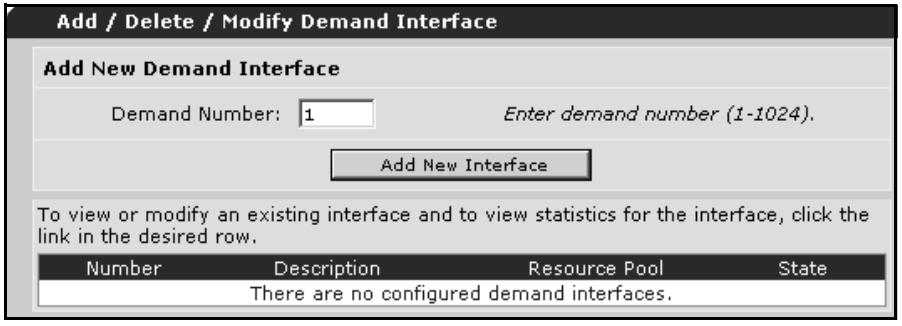

Figure 14-69. Add/Delete/Modify Demand Interface

2. On the *Add/Delete/Modify Demand Interface* screen, in the *Demand Number* field, enter a number for the interface in the range from 1 to 1,024.
3. Click the *Add New Interface* button. The "Demand Configuration" screen is displayed.

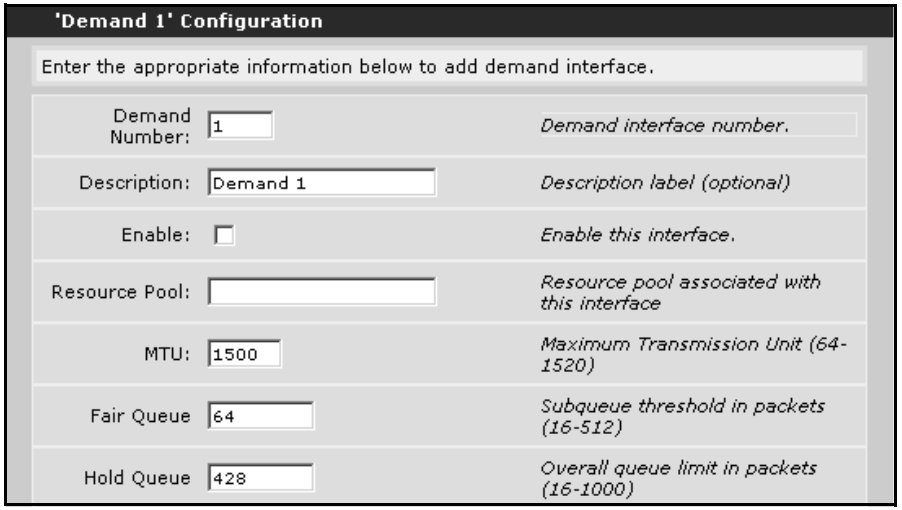

Figure 14-70. Demand Interface Configuration

4. On the *Demand Configuration* screen, in the *Description* field, enter a description, if you want to record information in the startup-config that will identify this demand interface.
5. Check the *Enable* box.
6. In the *Resource Pool* field, enter a name for the resource pool that will be associated with this demand interface.
7. Accept the default settings for **MTU**, **Fair Queue**, and **Hold Queue** unless you need to customize these settings for your environment.

Note

Unlike other WAN connections on the ProCurve Secure Router, demand routing does not create a persistent, one-to-one relationship between the physical interface and the logical interface. Instead, the resource pool links the logical interface to one or more physical interfaces. (You will associate an ISDN group or physical interface with the resource pool later.)

8. In the *Demand Configuration* section, enter values for the *Called Number* and the *Caller Number* if you want to restrict the incoming and outgoing calls by specific numbers.
9. In the *Connect Mode* field, use the pull-down menu to specify whether the demand interface can originate or answer a call, or both.

10. In the *Connect Order* field, use the pull-down menu to specify the order in which connect-sequence commands are processed. You can select *Beginning*, *LastSuccess*, or *NextAfterLastSuccess*. (*Connect-sequence* commands provide the dial-up instructions for the connection.)

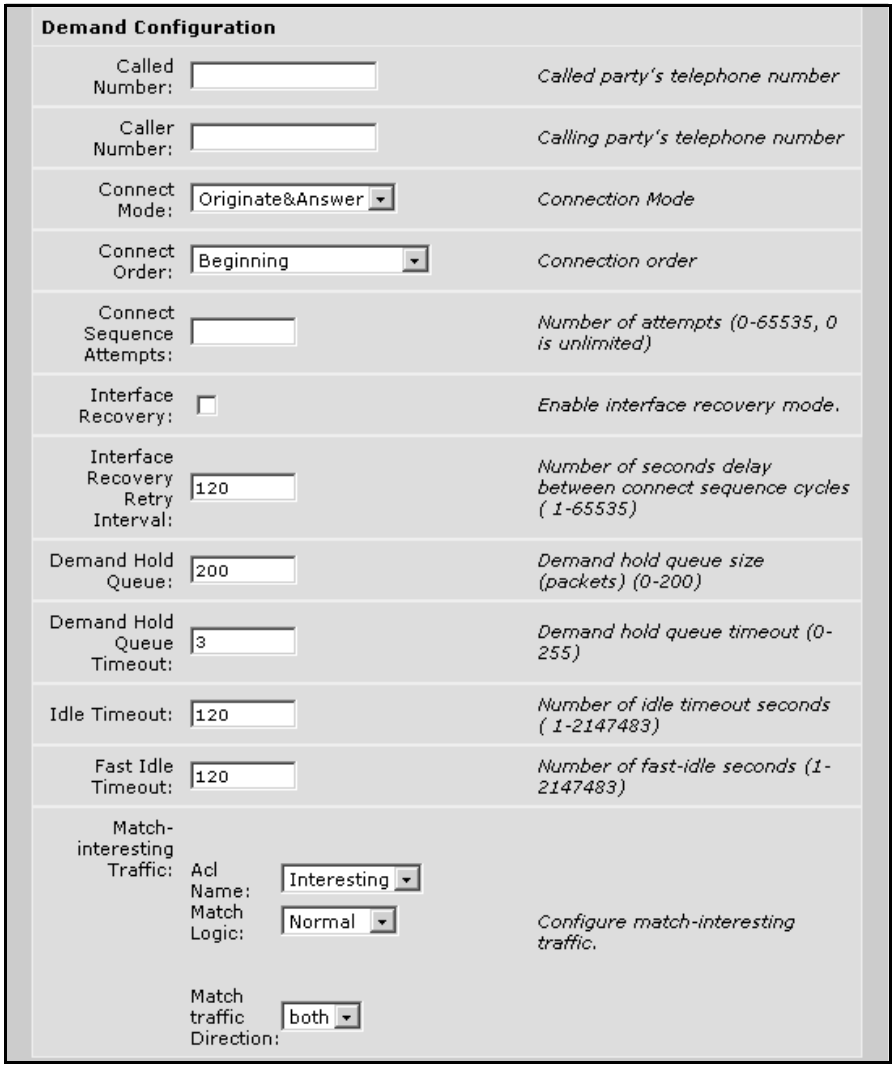

Figure 14-71. Demand Configuration

11. In the *Connect Sequence Attempts* field, enter the number of times that you want the router to try each connect-sequence.

12. Select *Interface Recovery* to enable recovery mode if the ProCurve Secure Router is unable to establish a demand routing connection.
13. In the *Interface Recovery Retry Interval*, enter the number of seconds that the router should wait between connection attempts (during recovery mode).
14. If you want, customize the *Demand Hold Queue* and *Demand Hold Queue Timeout* settings for your environment. The router uses the hold queue when it receives interesting traffic but that demand-routing connection is not currently established.
15. If you want, customize the *Idle Timeout* and *Fast Idle Timeout* settings for your environment.

    The *Idle Timeout* setting determines how long the line must remain idle before the router disconnects the ISDN or analog call.

    The *Fast Idle Timeout* setting is used if a BRI interface or an analog interface is in contention. That is, if the BRI or analog interface is currently in use and the router needs to establish another connection using that interface, the router places the interface in "fast idle timeout." This decreases the time that the line must be idle before the router can disconnect the call, thus freeing up the resource for the other connection.
16. In the *Match-Interesting Traffic* section, select the ACL that defines the interesting traffic, select the matching logic, and apply it to incoming or outgoing traffic, or both.

Configuring PPP for the Demand Interface

17. In the *PPP Configuration* section, configure sent and peer authentication as needed to prevent an unauthorized peer from trying to connect to your ProCurve Secure Router.

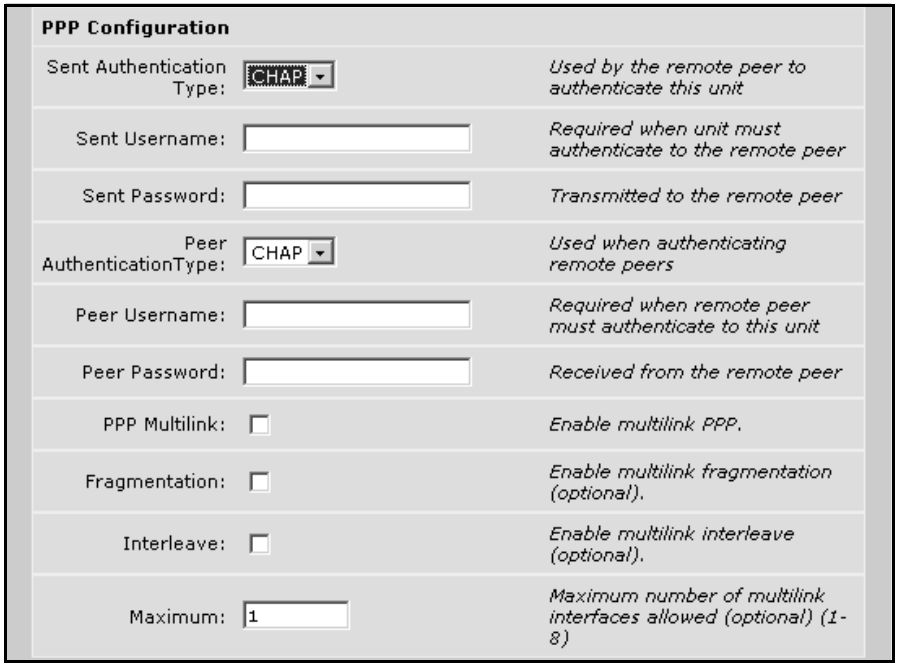

Figure 14-72. PPP Configuration for the Demand Interface

18. If you want to increase bandwidth, configure the PPP multilink options. MLPPP is supported only on the primary ISDN modules. (Remember, you must also configure the ISDN group to support MLPPP.)

Configuring IP Settings for the Demand Interface

19. In the *IP Settings* section, in the *Address Type* field, use the pull-down menu to select a static IP address, an unnumbered interface, or a negotiated IP address.

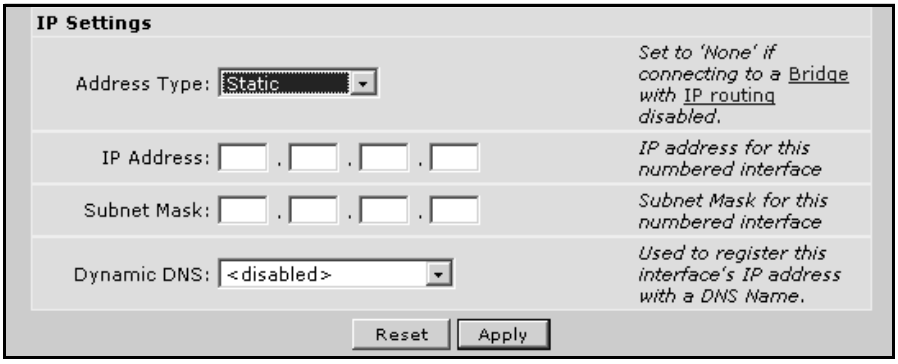

Figure 14-73. IP Settings for the Demand Interface

20. If you selected *Static* for *Address Type*, enter the address and subnet mask in the *IP Address* and *Subnet Mask*, respectively.
21. Click *Apply* to save the settings for the demand interface. You are returned to the first demand routing screen.

Assigning an ISDN Group or BRI Interface to the Resource Pool

You must now assign an ISDN group or BRI interface to the resource pool that you created earlier. (See "Configuring the Demand Interface" on page 14-95.) If you are configuring demand routing for a primary ISDN module, you will assign the ISDN group to the resource pool. If you are configuring demand routing for a backup ISDN module, you will assign the BRI interface to the resource group.

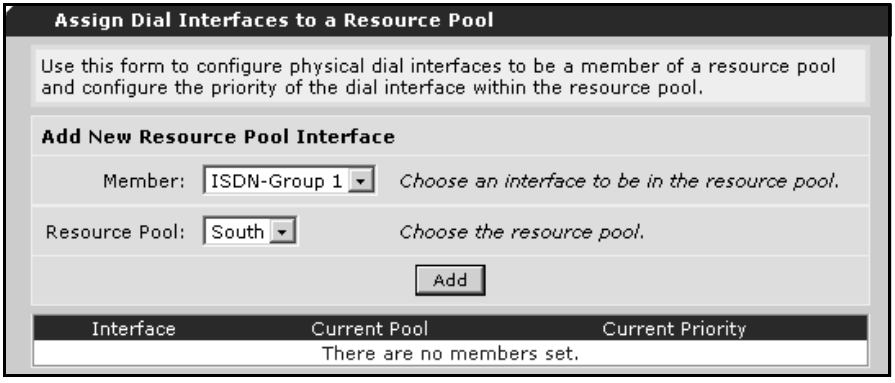

Figure 14-74. Assign Dial Interfaces to a Resource Pool

1. On the *Assign Dial Interfaces to a Resource Pool* screen, in the *Member* field, use the pull-down menu to select either:
   - an ISDN group, if you are configuring demand routing for a primary ISDN interface
   - an interface, if you are configuring demand routing for a backup interface
2. In the *Resource Pool* field, use the pull-down menu to select the resource pool. Make sure that you select the same resource pool that you assigned to the demand interface.
3. If you assign a BRI interface to the resource pool, assign it a priority number.
4. Click the *Add* button. You are returned to the first demand routing screen.

Configuring Connect Sequences

You must configure a connect sequence to specify the dial-up instructions for the connection. When you configure a connect sequence through the Web browser interface, you specify:

- the number of the demand interface
- the telephone number that the router dials to connect to the other site
- the type of dial-up connection that the router should establish
- the number of times that the router should try to process this connect sequence (per connect-sequence attempt).

When the ProCurve Secure Router detects interesting traffic and no connections are currently established to carry this traffic, the router uses a connect sequence to try to establish a connection. This process is called an *activation attempt*.

You can configure more than one connect sequence for a demand interface.

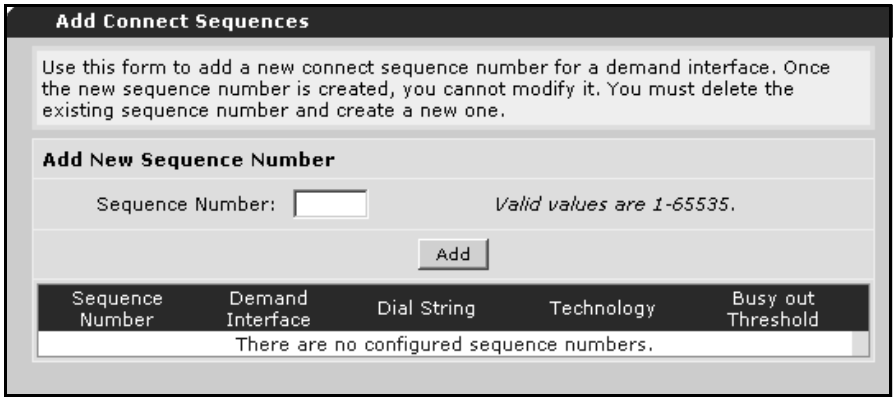

Figure 14-75. Add Connect Sequences

To configure a connect sequence, complete the following steps:

1. On the *Add Connect Sequences* screen, in the *Sequence Number* field, enter a unique number to identify this connect sequence.
2. Click the *Add* button.

   The *Sequence Configuration* screen is displayed. The *Sequence Number* field should display the number that you entered for this connection sequence.

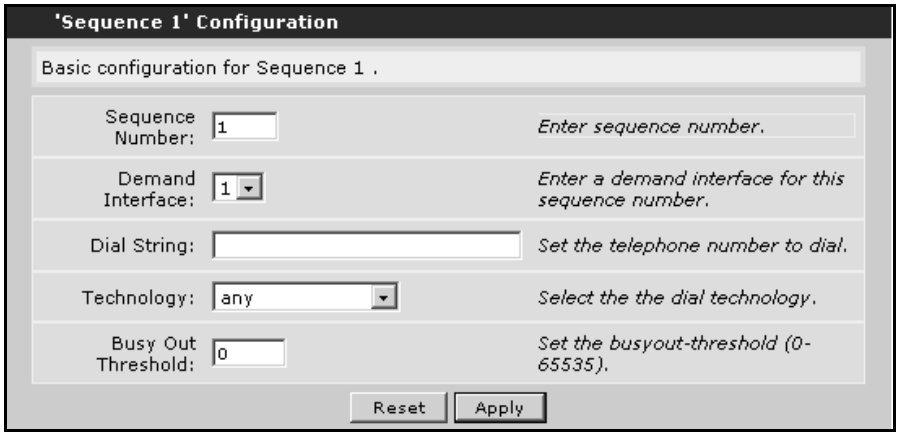

Figure 14-76. Demand Interface Sequence Configuration

3. In the *Demand Interface* field, use the pull-down menu to select the appropriate demand interface for this connect sequence.

4. In the *Dial String* field, enter the telephone number for the peer.
5. In the *Technology* field, use the pull-down menu to select one of the following:
   - any
   - forced-analog
   - forced-isdn-56k
   - forced-isdn-64k
   - isdn-56k
   - isdn-64k
6. In the *Busy Out Threshold* field, enter the number of times that the router should try to make this connection. If you leave the default setting of 0, the router makes an unlimited number of attempts.
7. Click the *Apply* button to save your changes.

Configuring a Static Route or a Floating Static Route

The ProCurve Secure Router must know the route to the far-end network that is connected through the demand interface. If you are configuring a primary connection, you will configure a static route. If you are configuring a backup connection, you will configure a floating static route.

To configure a static route or a floating static route, complete the following steps:

1. Click *Route Table* in the *Router/Bridge* section of the navigation bar.

   The *Add a Static Route to the Route Table* screen is displayed.

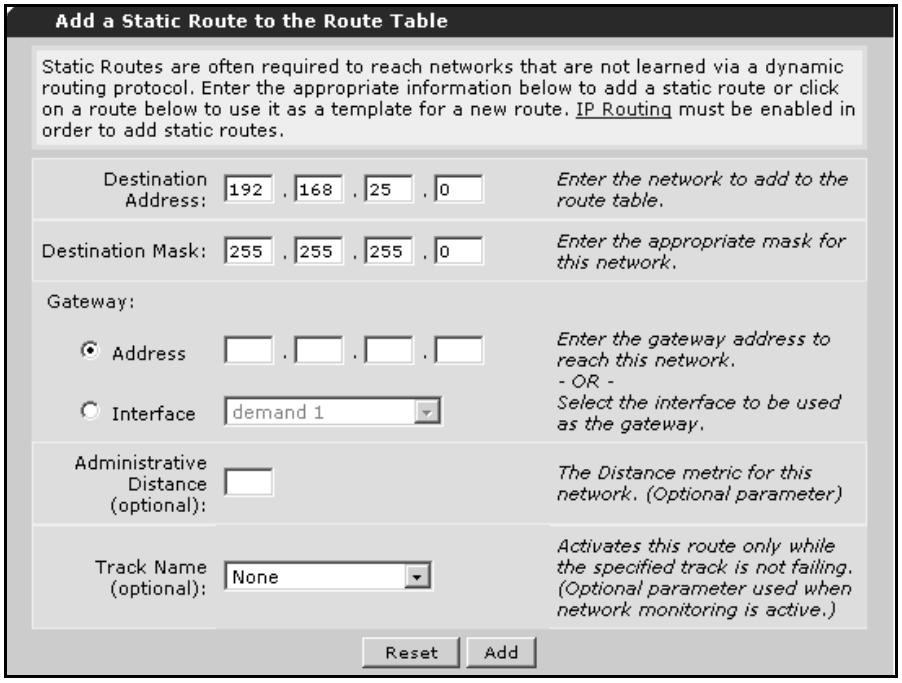

Figure 14-77. Add a Static Route to the Route Table

2. In the *Destination Address* and *Destination Mask* fields, enter the IP address and subnet mask, respectively, for the far-end network.
3. Under *Gateway*, click the *Interface* option and use the pull-down menu to select the appropriate demand interface.
4. If you are configuring a route for a backup connection, in the *Administrative Distance* field, enter a number for the administrative distance.
5. If you are using network monitoring, in the *Track Name* field, use the pull-down menu to select the track for the interface.
6. Click the *Apply* button to save your changes.

E1 + G.703 and T1 + DSX-1 Modules

The E1 + G.703 and the T1 + DSX-1 modules allow you to use some channels of a carrier line for data and some channels for analog voice. When you configure one of these modules, you should first configure the E1 or T1 interface that will be used for data. As part of this configuration, you must assign the channels that will be used for data to the E1 or T1 interface. The remaining channels are then automatically assigned to the G.703 or DSX-1 interface.

When you configure the E1 or T1 interface, you set the clock source for the entire module. If you set the clock source to *line*, the module will take its timing from the public carrier's equipment that is attached to the E1 or T1 interface. If you set the clock source to *through*, the module will take its timing from the PBX that is attached to the G.703 or DSX-1 interface.

For more information about E1 or T1 settings, see "Configuring E1 and T1 Interfaces" on page 14-54.

In the Secure Router OS, the G.703 interface is referred to as an E1 interface. Specifically, it is the interface for port 2 in the slot where the E1 + G.703 module is installed. For example, if the E1 + G.703 module is installed in slot 2, the G.703 interface is E1 2/2.

The DSX-1 interface is referred to as a T1 interface. It is the interface for port 2 in the slot where the T1 + DSX-1 module is installed. For example, if the T1 + DSX-1 module is installed in port 1, the DSX-1 interface is T1 1/2.

However, to avoid confusion between the interfaces used for data and the interfaces used for analog voice, these instructions will use the terms *G.703 interface* and *DSX-1 interface*.

When you configure the G.703 or DSX-1 interface, the settings that you enter should match those used by your private branch exchange (PBX). To configure the G.703 or DSX-1 interface from the Web browser interface, complete the following steps:

1. From the navigation bar, click *Physical Interfaces*. The *Physical Interfaces* window is displayed.
2. Select the G.703 or DSX-1 interface. The configuration window for that interface is displayed.

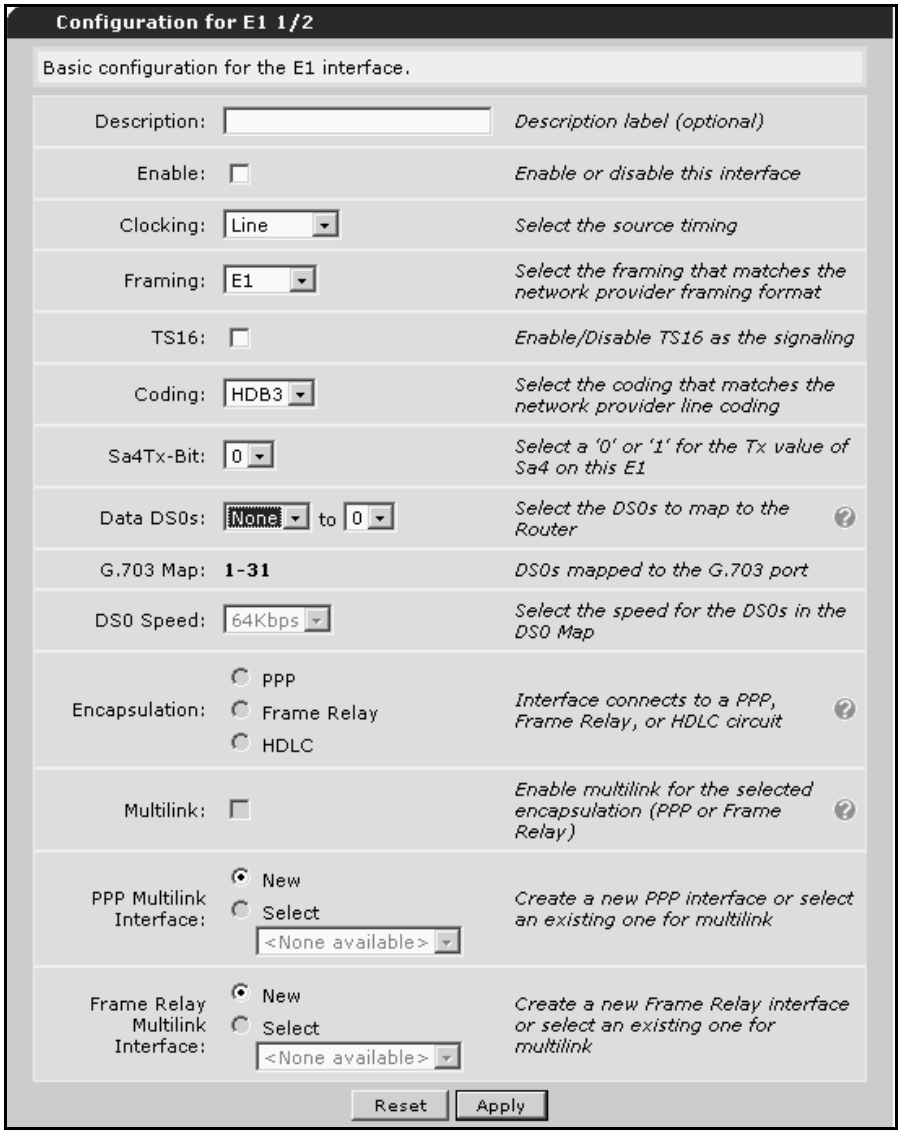

Figure 14-78. Configuration Window for G.703 Interface

3. Enter a description in the *Description* box if you want to document information about the G.703 or DSX-1 interface. This information will be displayed in the running-config under the appropriate interface heading.
4. To activate the interface, select the *Enable* box.

5. Ignore the clock source, because you set the clock source for this module on the E1 or T1 interface.
6. Set the frame format:
   - If you are configuring a G.703 interface, use the pull-down menu to select *E1* or *CRC4*. *E1* is the default setting.
   - If you are configuring a DSX-1 interface, click *ESF* or *D4*. *ESF* is the default setting.
7. Select the *TS16* box to enable TS16 signaling if you are configuring a G.703 interface. For more information about this setting, see *Chapter 9: Configuring the E1 + G.703 and T1 + DSX-1 Modules*.

Note

By default, the **signaling-mode** setting for the DSX-1 interface is set to **robbed-bit**. If you need to change this setting, you must enter the command from the CLI. You must also adjust the **line-length** setting from the CLI. For information about these settings, see *Chapter 9: Configuring the E1 + G.703 and T1 + DSX-1 Modules*.

8. Use the pull-down menu to configure the coding:
   - If you are configuring a G.703 interface, use the pull-down menu to select *HDB3* or *AMI*. *HDB3* is the default setting.
   - If you are configuring a DSX-1 interface, use the pull-down menu to select *B8ZS* or *AMI*. *B8ZS* is the default setting.
9. Ignore the *Data DS0s* field, because you configure channels for the E1 or T1 interface, and the remaining channels are assigned to the G.703 or DSX-1 interface.
10. Click *Apply* to save your configurations.

Status Information

Status information is displayed at the bottom of the configuration for the G.703 or DSX-1 window. This readout is not in real-time. To update the readout to the current statistics, click the *Continuous Refresh* button. To end continuous refresh, click the *Stop Updates* button. To reset the statistics, click the *Clear Statistics* button.

Bridging

You can configure the router to act as a remote bridge so that it can:

- bridge non-IP protocols
- bridge two sites using addresses on the same subnet

The ProCurve Secure Router automatically implements Rapid Spanning Tree Protocol (RSTP), or IEEE 802.1w, on all bridged interfaces. Bridges and switches run RSTP to eliminate loops from the network topology.

Configuring Bridging

You configure a bridge by assigning interfaces to it. These interfaces then act like bridge ports. They learn the MAC addresses for frames so that they can properly forward frames received on other bridged interfaces.

To configure bridging, complete the following steps:

1. If you are configuring the router to bridge two remote segments of the same subnet, you must set the default gateway and disable IP routing before configuring the bridge:
   a. Select *Default Gateway* under *Router/Bridge* in the navigation bar. Enter the IP address for the router's default gateway. This address should either be a router interface or a unit that knows how to reach the router; otherwise, you will lock yourself out of the Web browser interface. Click *Apply*.
   b. Select *Routing* under *Router/Bridge* in the navigation bar. Uncheck the *IP Routing* box. Click *Apply*.

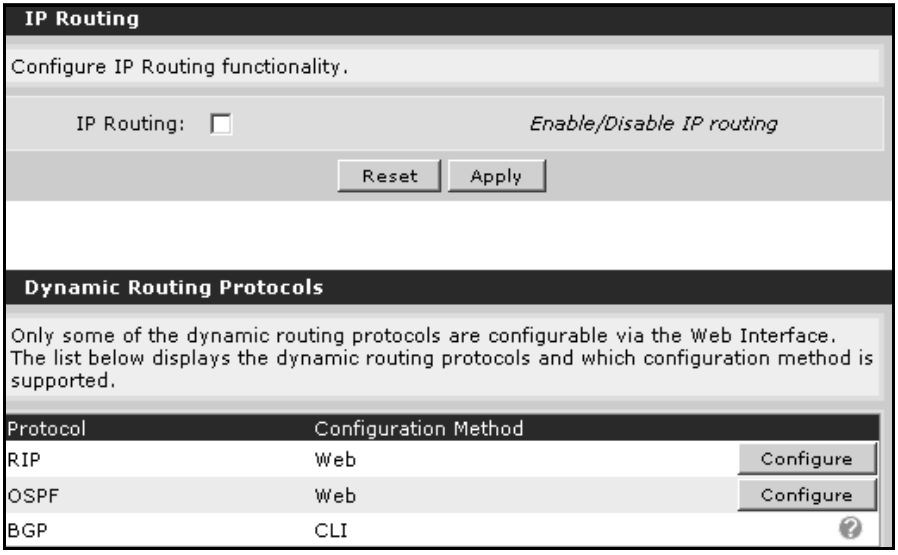

Figure 14-79. Disabling Routing

2. Select *Bridging* under *Router/Bridge* in the navigation bar.
3. Enter a number between 1 and 255 in the *Bridge Number* box in the *Add/Modify/Delete Bridge* window.
4. Click *Add*.

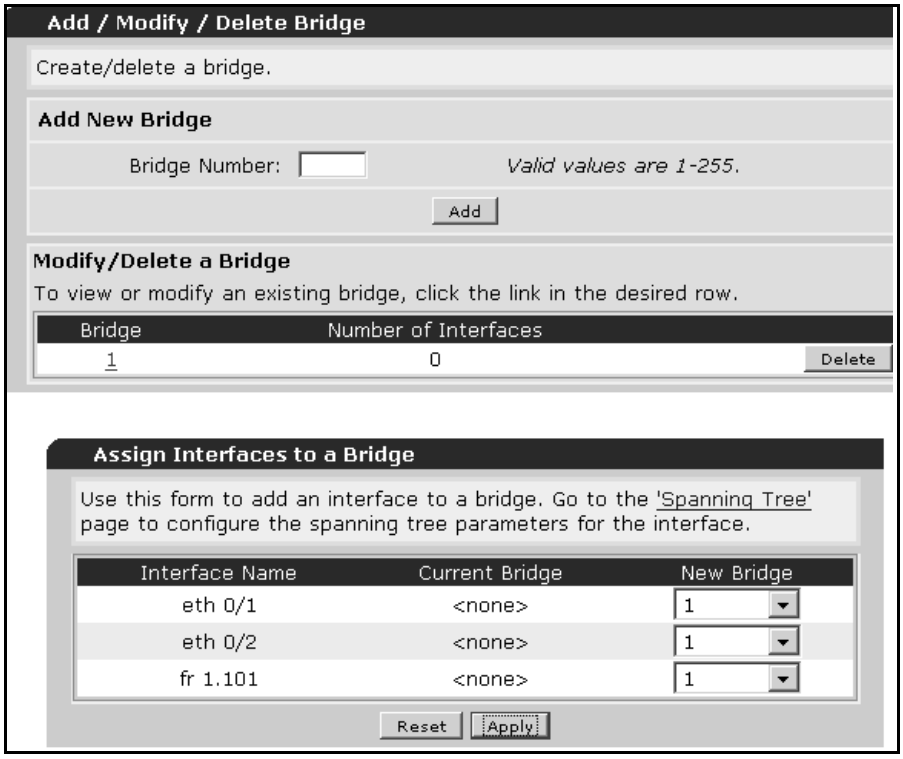

Figure 14-80. Configuring a Bridge

5. The *Assign Interfaces to a Bridge* window displays all Ethernet and logical interfaces on the router. (For Frame Relay and ATM, it displays subinterfaces.) For each interface that should participate in the bridge, select the bridge group from the pull-down menu. (You should assign at least two interfaces to every bridge.)
6. Click *Apply*.

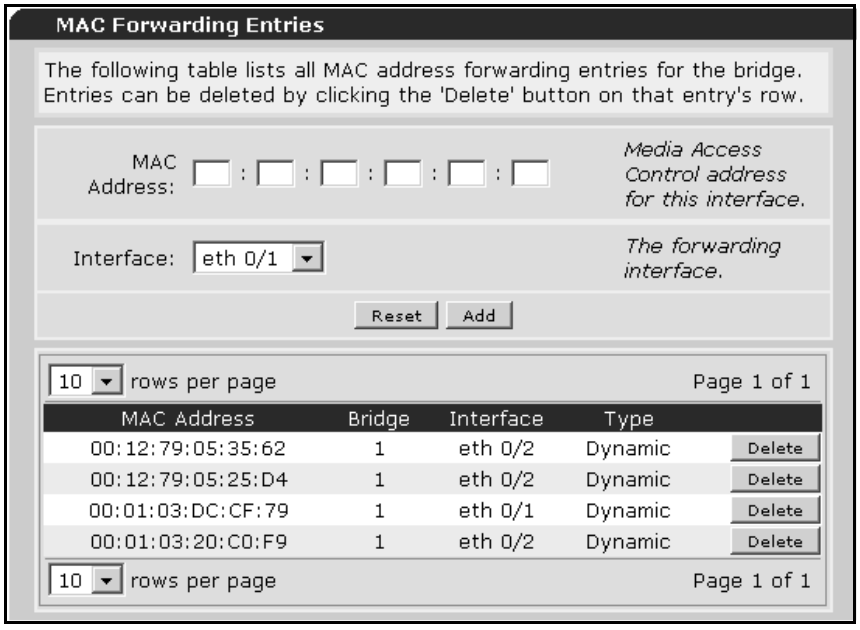

Figure 14-81. Viewing the Bridge Table

A bridge group on the ProCurve Secure Router listens for frames from connected hosts. It stores the frame's source MAC address with the interface on which the frame arrived in a bridge table. The bridge will then send frames only through the interface that connects to the host to which the frames are destined, rather than flood the frames through all interfaces.

You can view the bridge table at the bottom of the window. This table includes the MAC addresses of connected hosts with their forwarding interface. For example, in Figure 14-81, the router knows to forward frames destined to 00:01:03:20:C0:F9 through the Ethernet 0/2 interface.

You can manually add a host by entering its MAC address in the corresponding fields of the *MAC Forwarding Entries* window. Select the forwarding interface from the *Interface* pull-down menu.

Configuring the Spanning Tree Protocol

Typically, RSTP will run on your WAN without any further configurations. However, you can:

- view information about the spanning tree
- configure the router to run the legacy version, STP, rather than RSTP
- change the router's bridge priority
- alter spanning tree timers
- configure properties for individual interfaces

Viewing a Spanning Tree

RSTP and STP prune connections in a looped topology. All nodes participating in the same bridge group generate a shared, loopless topology. You can view information about this topology, called a spanning tree instance. Follow these steps:

1. Select *Spanning Tree* under *Router/Bridge* in the navigation bar.
2. Scroll down to the *Spanning Tree Properties* window and select the *Spanning Tree Instance* that you want to view.
3. A window, such as the one displayed in Figure 14-82, will display information that you can view to determine:
   - Which network device is the root.
   - Which interfaces are forwarding packets.
   - Which interfaces have been disabled—for example, in Figure 14-82 the Frame Relay 1.102 subinterface provides a redundant connection to the root, so its role is "Blocking" and it does not forward packets.
   - Which interface role each interface is playing—Root ports are on the best path to the root device. Designated ports connect to root ports on neighbors further from the root. Edge ports connect to end devices. For example, in Figure 14-82, the Ethernet 0/2 interface connects the local device to the root, and the Ethernet 0/1 interface provides a connection to the root for a connected network.

   The *Spanning Tree Properties "STP <instance number>"* window displays information about the root bridge in the *Root ID* column and the local device in the *Bridge ID* column. For example, in Figure 14-82, the root is identified by its MAC address 00:12:79:05:25:D4, and it is connected to the local router through the Ethernet 0/2 interface.

The *Spanning Tree Port Information "STP <instance number>"* window displays information about the interfaces on the local router, including their role in the spanning tree, whether they are forwarding packets, and the cost for their connection.

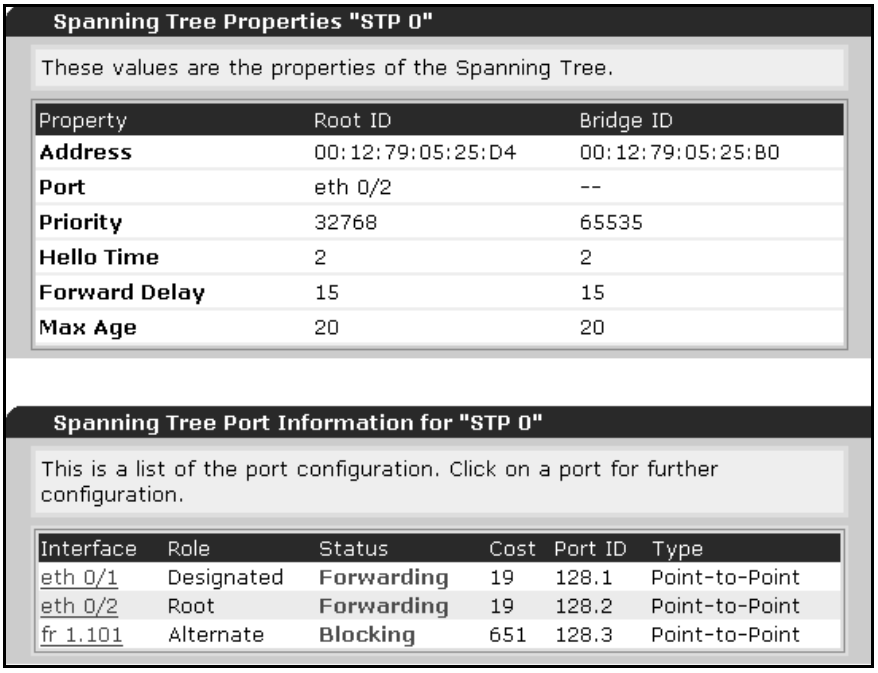

Figure 14-82. Viewing a Spanning Tree

Setting Global Spanning Tree Parameters

You set the spanning tree protocol version, router's bridge priority, and spanning tree timers in the *Spanning Tree* window.

1. Select *Spanning Tree* under *Router/Bridge* in the navigation bar.
2. RSTP is fully backwards compatible with STP. When an RSTP interface detects an STP message, it automatically implements STP. You should generally run RSTP, which reduces convergence time from about a minute to less than a second.

   However, if, for whatever reason you decide to use STP, select *Legacy STP (802.1d)* from the *Spanning Tree Mode* pull-down menu.

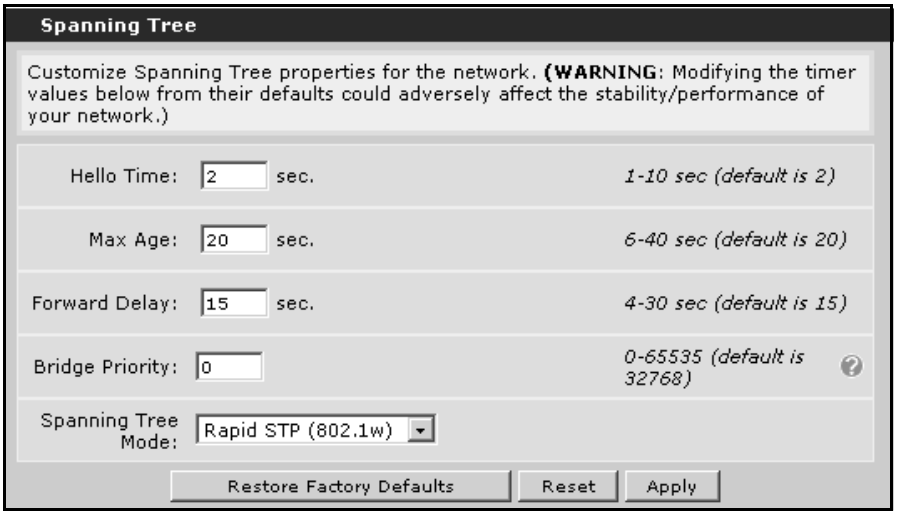

Figure 14-83. Configuring Spanning Tree Properties

3. Bridges elect the device with the *lowest* bridge ID (priority plus MAC address) root. You can manipulate which device becomes root by changing devices' priorities. Enter a number between 0 and 65535 in the *Bridge Priority* field. For example, enter 0 to ensure that the local router becomes root. In Figure 14-83, the priority has been set to 0 to ensure that it becomes the root. (The default priority is 32768.)

Caution

You should alter timers only if you have a great deal of experience working with spanning tree protocols. Otherwise, you could slow convergence or cause interfaces to toggle between forwarding and blocked states.

4. Enter times for the forward delay, hello, and maximum age timers in the corresponding fields. Click *Apply*.

   The *Restore Factory Defaults* button returns the timers and STP version to their defaults. The *Reset* button returns to the settings that were established the last time you clicked *Apply*.

Table 14-1. Spanning Tree Timers

Timer	Function	Default	Range
hello time	Each forwarding interface periodically transmits BPDU hellos. If neighbors miss three hellos from an interface, they assume the connection is down and send out TC BPDU to this effect. Take care when altering this timer, because incompatible settings can cause devices to believe a connection is down when it is not.	2 seconds	0 to 1,000,000
max age	The device discards information from a BPDU when its maximum age timer expires. With STP, the timer determines how long a device will wait to receive information on a connection from the root before assuming the connection is down.	20 seconds	6 to 40
forward delay	The device waits this interval before forwarding BPDU. With STP, this setting determines how long the device stays first in the listening and then in the learning stage.	15 seconds	4 to 30

Configuring Spanning Tree Settings for Individual Interfaces

You can manually configure settings such as cost for the connection for each bridged interface.

1. Select *Spanning Tree* from the navigation bar.
2. Scroll to the *Spanning Tree Properties* window and select *Spanning Tree Instance*.
3. Select the interface that you want to configure from the *Spanning Tree Port Information* window that is displayed.
4. The *Spanning Tree Port Information* window will display. (See Figure 14-84.) You can then alter certain settings:
   a. You can alter the port priority for the connection. A lower priority increases the connection's chance of being selected. (Priority only comes into account when two connections have the same cost.) Select the priority from the *ID* pull-down menu.
   b. RSTP allows point-to-point interfaces to assert sync to rapidly transition to the forwarding state. Interfaces automatically determine whether they are on point-to-point or shared connections by their duplex setting.

If necessary, you can override this setting and manually set the connection type. Select *Forced Point-to-Point* or *Forced Shared* from the *Link Type Configuration* pull-down menu.

If you leave this setting at the default *Automatically determined*, then the *Link Type* displays the setting used on the interface.

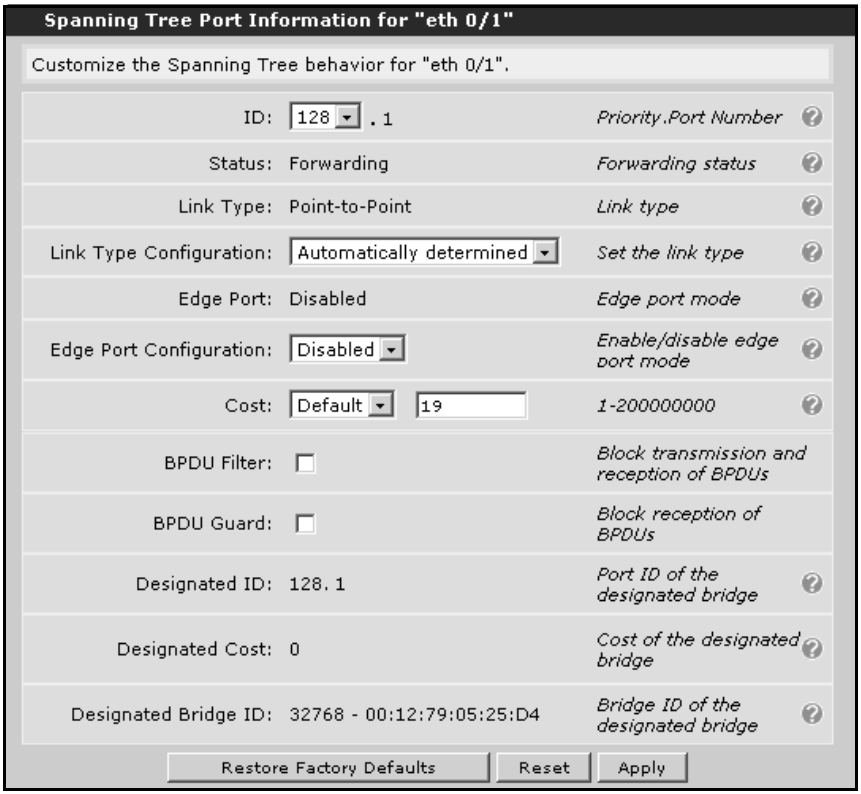

Figure 14-84. Spanning Tree Options on an Interface

c. Edge ports connect directly to end devices. RSTP allows such interfaces to immediately begin forwarding packets so that applications on the user device do not timeout.

   To configure an interface to be an edge port, select *Enabled* from the *Edge Port Configuration*. You can then check the *BPDU Guard* box to prevent the end device from joining the spanning tree.

d. The Secure Router OS automatically calculates a cost for each connection based on its bandwidth. You can alter this cost by selecting *Specify* from the *Cost* pull-down menu. Then enter a cost between 1 and 200,000,000 in the field that is displayed.

Routing

The ProCurve Secure Router stores routes in a route table, which it uses to route traffic from one network to another. Each route includes:

- destination IP address and subnet mask
- administrative distance—the reliability of the route
- metric—the cost of reaching the destination
- next hop address or forwarding interface
- type—how the router learned the route

The router automatically adds directly connected networks to its route table. It must learn routes to all other networks to which it will forward traffic. A router can learn:

- static routes, which you add manually
- dynamic routes, which it discovers using a routing protocol

This section explains how to configure static routing.

Configuring a Static Route

Static routing can be a good solution for your network when your network has:

- a simple topology and a single router at each site
- a single destination for traffic—for example, to an ISP
- only one path for IP traffic

Follow these steps to add a static route:

1. Select *Route Table* under *Router/Bridge* in the navigation bar.
2. The *Add a Static Route to the Route Table* window will display. Enter the destination network's IP address and subnet mask in the *Destination Address* and *Destination Mask* fields.
3. Specify how the router will forward packets that arrive for this destination in the *Gateway* field:
    a. You can configure a next hop address, which is the address of a router that is one hop closer to the destination than the local router. Select *Address* and enter this address.

b. You can alternatively specify the local interface through which the router will forward traffic destined to the destination network. Select *Interface* and choose the forwarding interface from the pull-down menu.

   This option has several advantages, particularly when you are connecting to an ISP router:
   – You do not need to know the IP address of the connecting router.
   – The route will remain valid even if the connecting router changes its IP address.

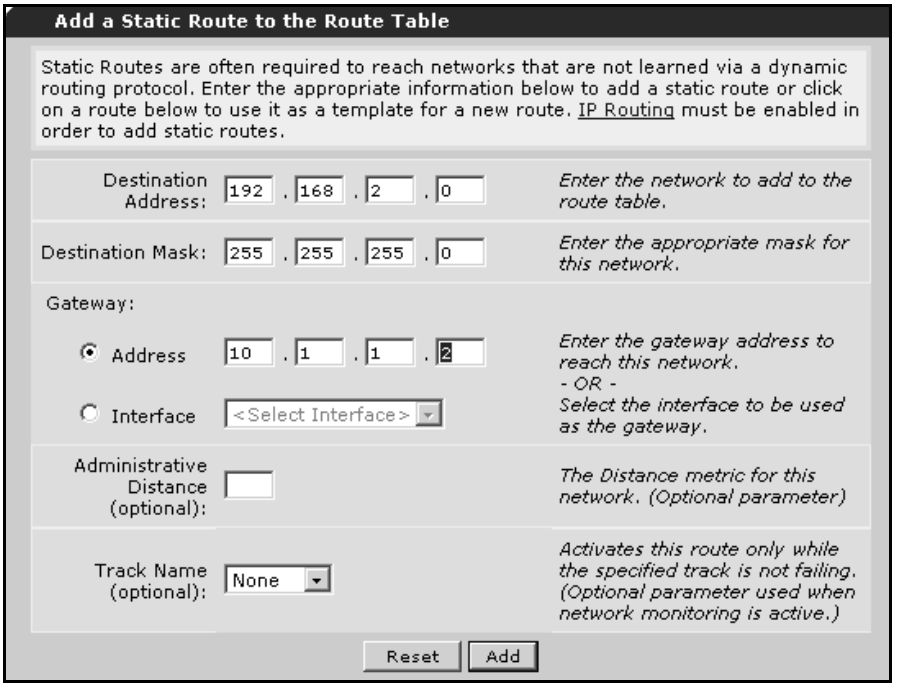

Figure 14-85. Adding a Static Route

4. If you want, you can configure an administrative distance for the route. Enter the distance in the *Administrative Distance* field.

   A router can learn routes in many different ways. A route's administrative distance informs the router how reliable the route is. When the router knows more than one route to a destination, it chooses the route with the lowest administrative distance.

By default, static routes have an administrative distance of 1. When you configure more than one static route to the same destination (for example, a route through a primary connection and a route through a backup connection), you should assign the route with lower priority a higher administrative distance. The router will only add the second route if the first route becomes unavailable.

5. If you are using network monitoring, in the *Track Name* field, use the pull-down menu to select the track for the interface.
6. Click *Add*.

   The *Route Table* screen displays all routes that the router is currently using to forward traffic, including any static routes. You can delete a static route by clicking the *Delete* button to its right.

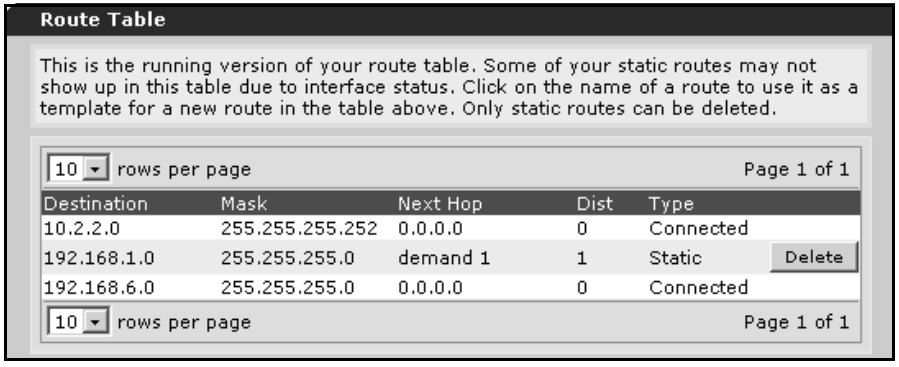

Figure 14-86.Route Table

Configuring a Default Route

A default route is a special static route. It is a route to network 0.0.0.0 0.0.0.0. The all-zero subnet mask ensures that all traffic matches this route. When a packet arrives en route to a destination to which the router does not know a more specific route, it uses the default route rather than dropping the packet.

For example, your network connects to the Internet through PPP interface 1 only. Rather than learning routes to all external networks from the ISP router, the router can simply forward all external traffic (that is, traffic for which it does not know another route) through the PPP interface.

Configure a default route as you would any other static route:

1. In the navigation bar, select *Route Table* under *Router/Bridge*.

2. Enter 0.0.0.0 in the *Destination Address* field and 0.0.0.0 in the *Destination Mask* field.
3. It is often a good idea to use a forwarding interface as the gateway rather than a next hop address. In this way, the route remains valid even if the peer router's IP address changes. Select *Interface* and choose the forwarding interface from the pull-down menu.

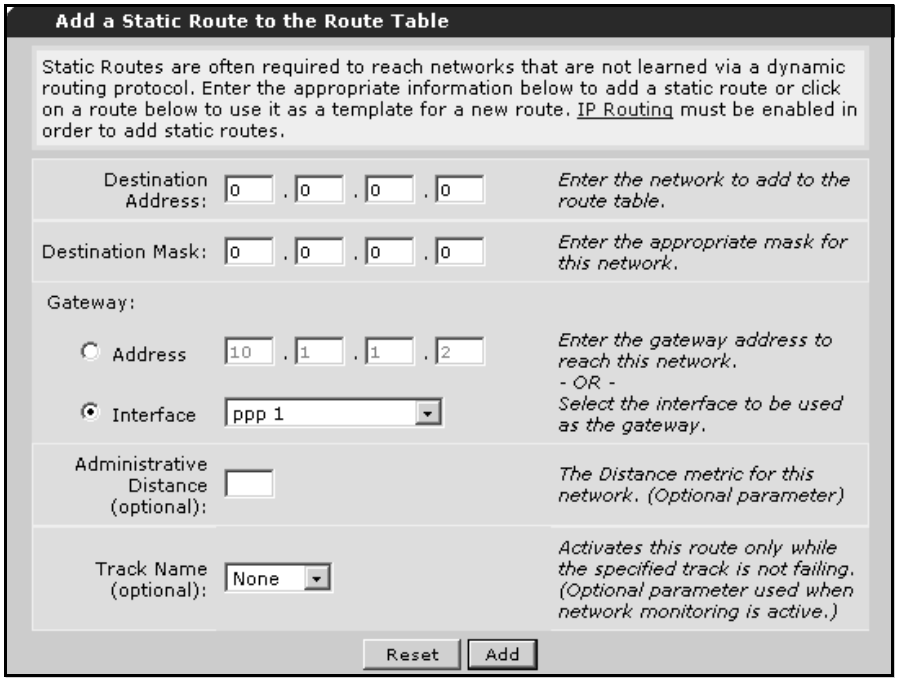

Figure 14-87. Configuring a Default Route

DNS Services

The ProCurve Secure Router automatically acts as a DNS client. You must, however, specify the address for its DNS server or servers. You can also:

- add entries to the router's host table for any local hosts whose addresses the router should be able to resolve on its own
- enable DNS proxy so that the router can act as a name server for clients
- configure dynamic DNS so that an interface with a dynamic address will automatically update its dynamic DNS service provider when its address changes

Configuring DNS Support

To configure DNS support in the Web browser interface, you should follow this process:

1. In the navigation bar, select *Hostname/DNS* under *System*.
2. If you have not already done so, you can change the router's hostname. Enter a name that is significant for your network in the *Host Name* field.
3. Enter your network's domain name in the *Domain* field.
4. The *Enable DNS Lookup* box should be checked. If it is not, select it. This allows the router to act as a DNS client, look up its own requests in the local host table, and send its own DNS requests to an external server.

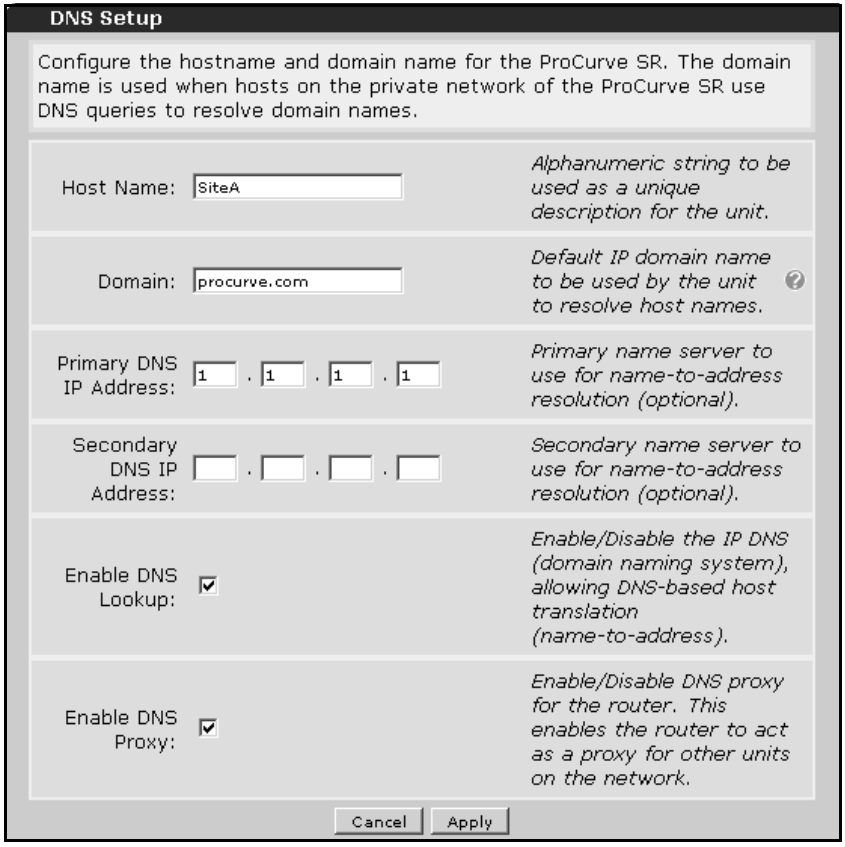

Figure 14-88. Configuring DNS Settings

5. Enter the IP address for the DNS server to which the router should send queries in the *Primary DNS IP Address* field. You can enter the address for an optional additional server in the *Secondary DNS IP Address* field.
6. If you want to enable the router to act as a name server for clients and to forward their queries to an external DNS server, click the *Enable DNS Proxy* box.

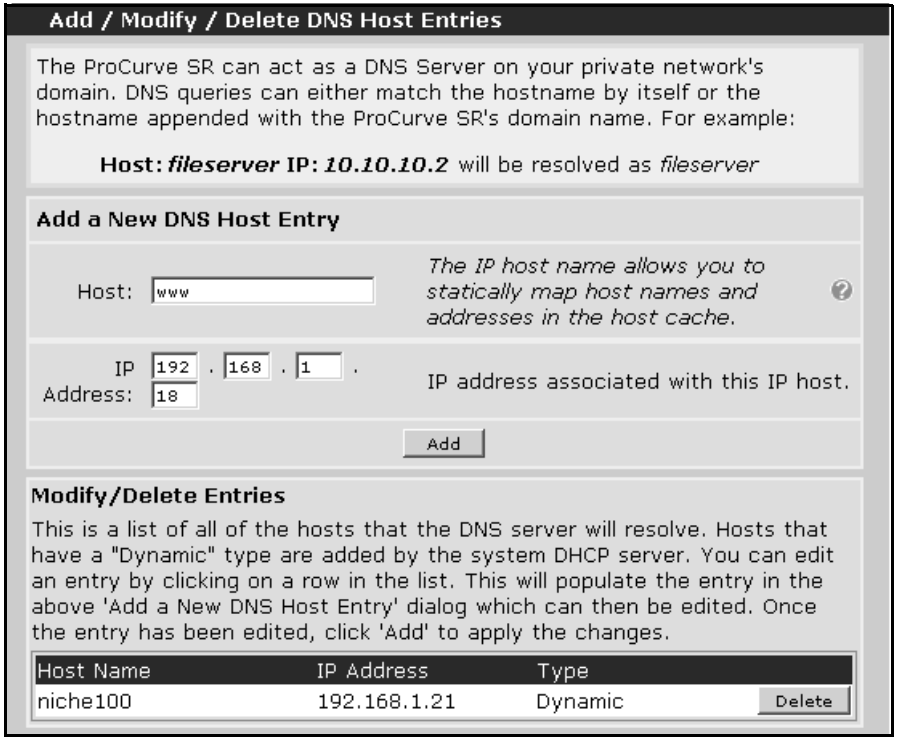

Figure 14-89. Configuring the Local Host Table

7. Configure the router's local host table:
   a. In the *Add/Modify/Delete DNS Host Entries* window, enter a hostname and the corresponding IP address. The host should be in the router's default domain, so you do not need to include the domain name. Click *Add*.
   b. The host table automatically includes all of the router's DHCP clients. (For example, in Figure 14-89, the entry labeled "Dynamic" is a DHCP client.) You can edit or remove the entries for these clients, as well as any entries that you have entered manually. Click the hostname. The interface automatically populates the correct fields with the host's information. Edit the entry and click *Modify*.
   c. To remove an entry entirely, click the *Delete* button to its right.
8. Click *Apply*.

Configuring Dynamic DNS

Networks change, and so may an interface's IP address. When you connect your router to an ISP, the ISP may require it to receive a dynamic address. The ISP can change this address at any time.

Your customers may need to access devices on your network, such as Web servers, whose addresses are linked to the dynamic public address. However, if this address changes, the hostname stored in DNS servers throughout the Internet will no longer match the device's actual IP address.

To allow your customers to always use the same hostname to access a device with a dynamic address, you should receive a static hostname from a dynamic DNS service provider. The ProCurve Secure Router supports dynamic DNS with Dynamic Networking Services, Inc., also called DynDNS.

1. Before activating dynamic DNS on an interface, you should go to **www.dyndns.org** and open an account.
   a. When you open an account, you will select a username and password.
   b. You will also select a service type. DynDNS currently provides Dynamic and Static DNS services free of charge. If you select Dynamic or Static DNS, you must place the router in one of the 68 domains provided by DynDNS.

      Dynamic and Static DNS grant much the same services; however, Static DNS is designed for an interface with an address that does not change or rarely changes.

      If you purchase Custom DNS services, you can use your own domain name (either pre-existing or purchased from DynDNS). For more information on the various services, see *Chapter 12: Domain Name System (DNS) Services* or the DynDNS Web site at **www.dyndns.org**.
   c. When you open the account, you will also specify the domain name the router interface will use.

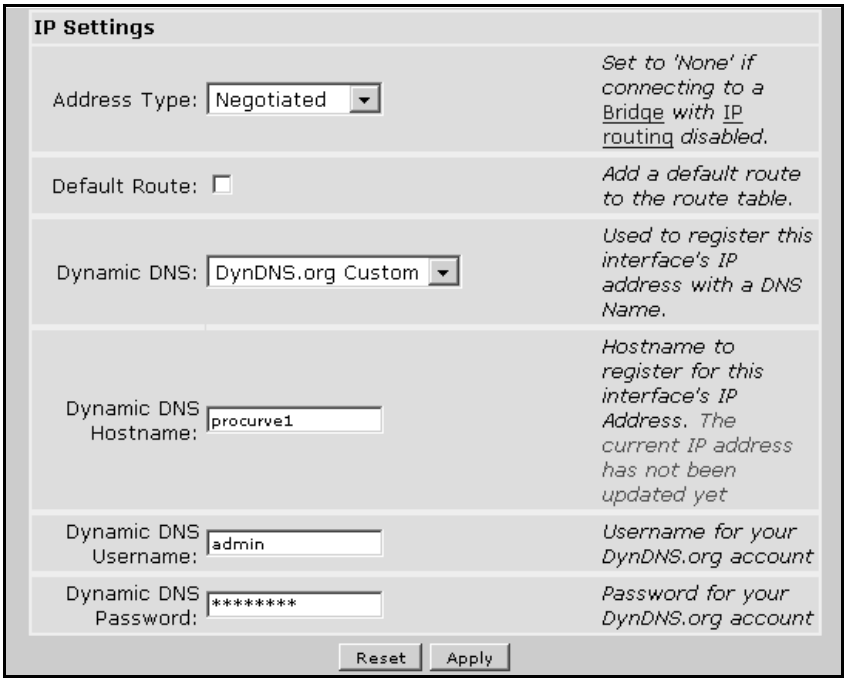

Figure 14-90. Configuring Dynamic DNS in the Configuration Window for an IP Interface

2. Return to the Web browser interface.
3. Click *IP Interfaces* under *Router/Bridge* in the navigation bar. (If you have not yet configured the logical interface for the connection to the Internet, you must do so. See "Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces" on page 14-62 or "Configuring Ethernet Interfaces" on page 14-40. The interface must also have an IP address, whether a dynamic address assigned by a connecting device or a static address.)
4. The configuration window for the interface will display.
5. By default, Dynamic DNS is disabled. To enable the interface to report to DynDNS when its IP address changes, click the arrow in the *Dynamic DNS* box. From the pull-down menu, choose the service for which you have registered:
   a. Choose *DynDNS.org* if you have selected Dynamic DNS services.
   b. Choose *DynDNS.org Static* if you have selected Static DNS services.
   c. Choose *DynDNS.org Custom* if you have selected Custom DNS services.

6. Enter the hostname for the device in the *Dynamic DNS Hostname* box.
7. Enter the username and password you created for your DynDNS account in the *Dynamic DNS Username* and *Dynamic DNS Password* boxes.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) allows hosts, acting as DHCP clients, to receive temporary configurations (such as an IP address, default gateway, and various server addresses) from a DHCP server. DHCP eases configuration and ensures that every device receives a unique address on the proper network. DHCP also conserves IP addresses by assigning them temporarily to active hosts only.

The ProCurve Secure Router can act as a DHCP server. Ethernet interfaces, bridged PPP interfaces, and Frame Relay and ATM subinterfaces can also act as DHCP clients.

Configuring a DHCP Server

You can configure the DHCP server to distribute configurations to an entire connected subnet. You can also configure it to assign a fixed address to a single host.

You create DHCP pools with the configurations that the router will issue to clients. Each pool must include:

- a network address and subnet mask
- a default gateway
- a DNS server
- a lease time

The pool can also include:

- a secondary DNS server
- primary and secondary NetBIOS Windows Internet Naming Service (WINS) servers
- a TFTP server
- an NTP server

Configuring a DHCP Pool for a Subnet

Complete these steps:

1. Under *System* in the navigation bar, select *DHCP Server*.
2. You should exclude all IP addresses permanently assigned to devices (such as routers, switches, and servers). Scroll to the second section in the window, *(Optional) Add/Delete DHCP Excluded Ranges*.

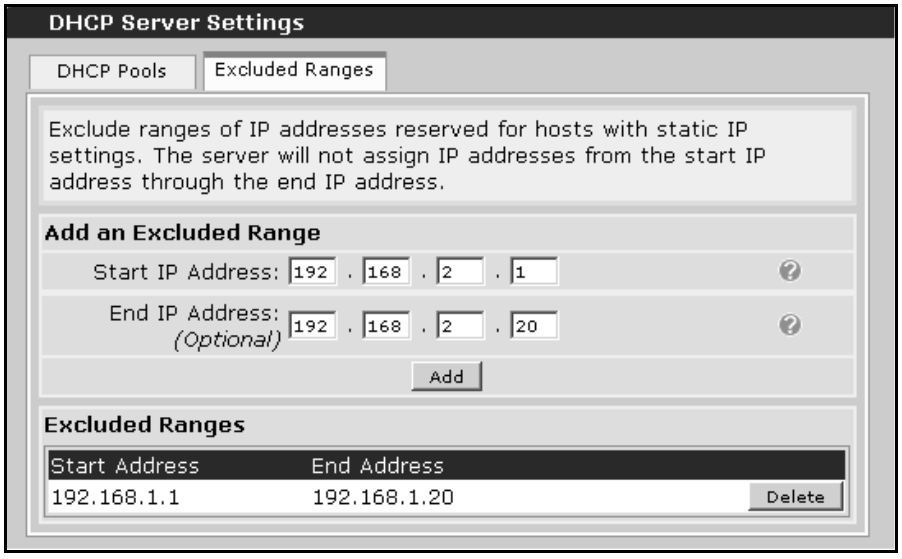

Figure 14-91. Excluding Static Addresses from DHCP Pools

3. Enter the first IP address in the range of excluded addresses in the *Start IP Address* field. Enter the last address in the range in the *End IP Address* field. If you want to exclude only one address, enter it in the *Start IP Address* field and leave the *End IP Address* field blank. Click *Add*.
4. You can repeat step 3 to configure multiple ranges of excluded addresses.
5. Move to the *Add/Modify/Delete DHCP Server Pool* window at the top of the window and create the pool:
   a. Under *Add New DHCP server pool*, enter a name in the *Pool Name* box that is significant for the subnet or group of users. Click *Add*.
   b. You can also modify an existing pool. The interface displays existing pools under *Modify/Delete DHCP server pool*. For each pool it lists the name and network address. To edit the pool, click the name.
6. You will move to the *DHCP Pool "<poolname>"* window.

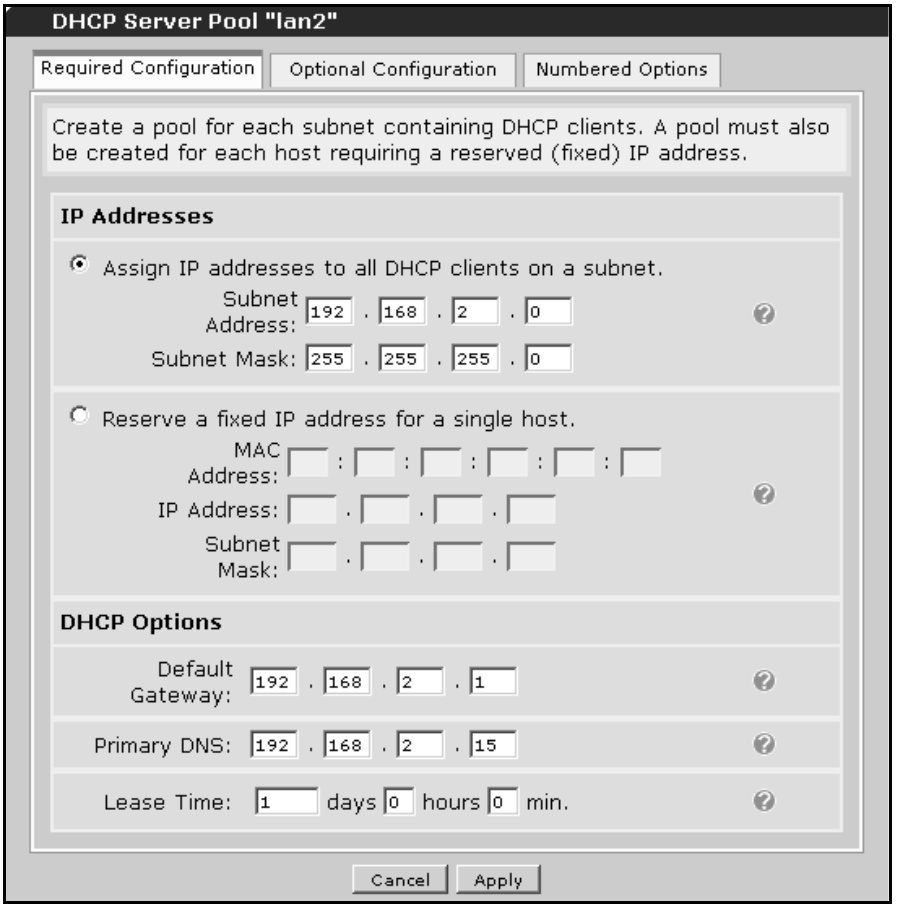

Figure 14-92. Required Configurations for a DHCP Pool

7. Click the *Required Configuration* tab:
   a. Under *IP Addresses*, select *Assign IP addresses to all DHCP clients on a subnet* and complete the *Subnet Address* and *Subnet Mask* fields.
   b. Under *DHCP Options*, enter the address for the *Default Gateway*. This address must be on the subnet specified for the *Subnet Address* and is typically the router interface that connects to the clients. If you are configuring a DHCP pool (or scope) for a VLAN, the default gateway address should be the IP address on the Ethernet subinterface associated with that VLAN.
   c. Enter the IP address for the DNS server that the client should use in the *Primary DNS* field under *DHCP Options*.

d. The default lease is 1 day. You can alter this time according to your organization's policies. Enter the lease time in days, hours, and minutes in the *Lease Time* field.

8. Click *Apply*.

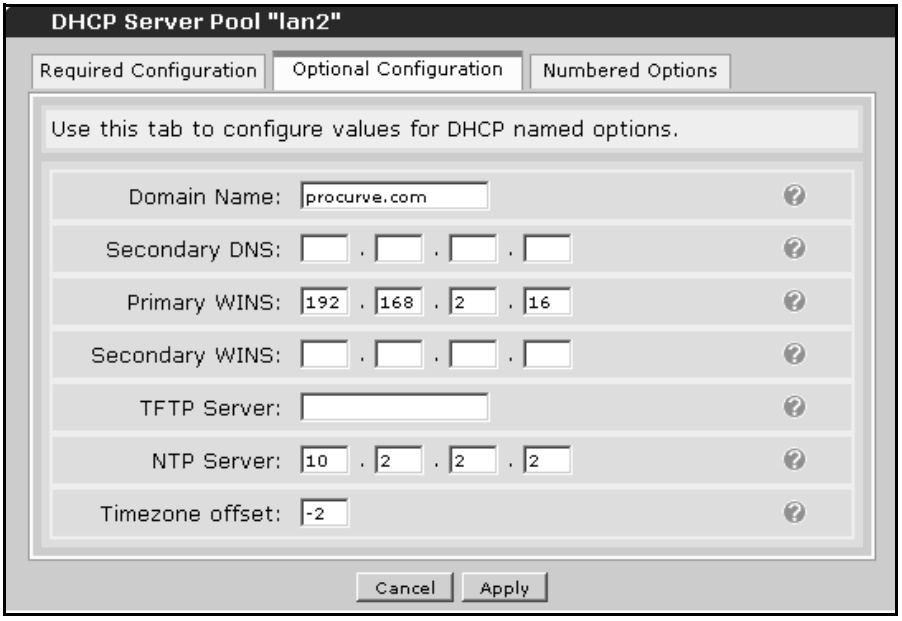

Figure 14-93. Optional Configurations for a DHCP Pool

9. Click the *Optional Configuration* tab to specify optional configurations that the router should send to clients, including:
   - domain name
   - addresses for:
     - secondary DNS server
     - primary WINS server (WINS servers translate NetBIOS names to DHCP IP addresses)
     - secondary WINS server
     - TFTP server
     - NTP server
   - timezone offset—used if the NTP server and client are in different timezones

10. Click *Apply*.

Assigning a Single Host a Fixed Address

Sometimes you may want to assign a host a fixed address through a DHCP server. For example, a device that is required to receive its address from a server may also need the stability of a static address to ensure that traffic is forwarded normally.

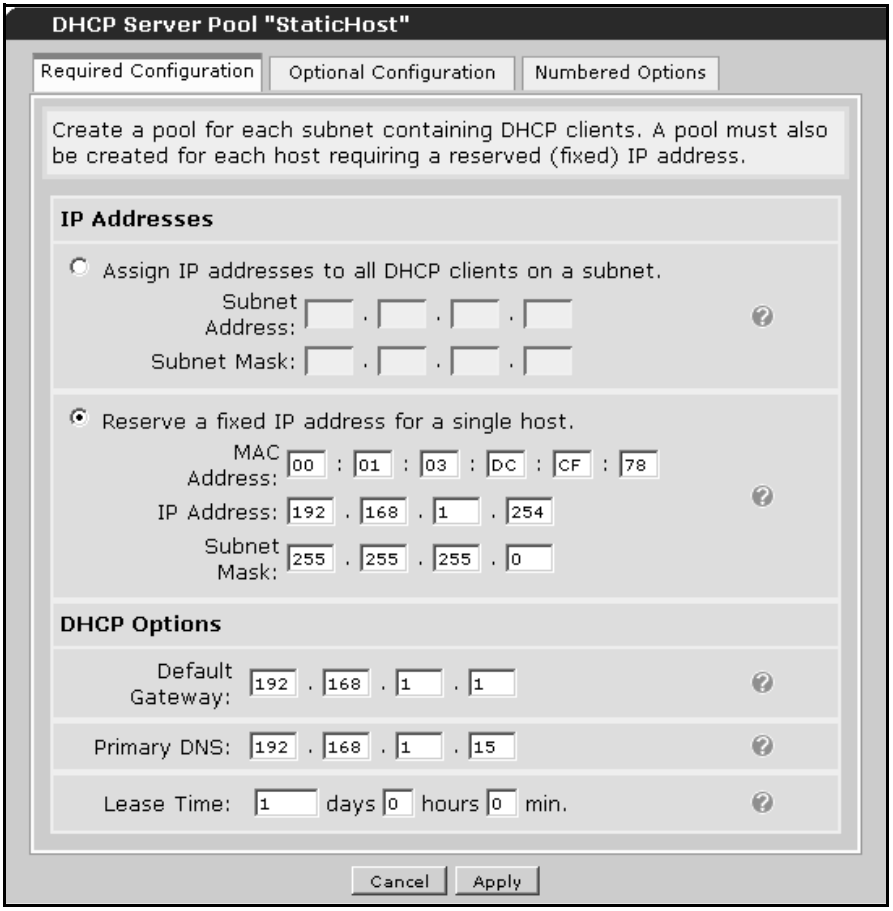

Figure 14-94. Assigning a Fixed Address to a Single Host

Follow the process outlined in "Configuring a DHCP Pool for a Subnet" on page 14-127. However, in step 7a, select *Reserve a fixed address for a single host*. Then enter the host's MAC address and the IP address you wish to assign it. Also enter the subnet mask for the network for the IP address.

Configuring an Interface as a DHCP Client

Some service providers, particularly ISPs, require you to take configurations from them. These configurations can include:

- a temporary IP address
- a default route
- a DNS server address
- a domain name

You can configure the following router interfaces to receive a dynamic address from a service provider or other DHCP server:

- Ethernet interfaces
- Frame Relay subinterfaces
- ATM subinterfaces
- bridged PPP interfaces

You can prevent the router from receiving a default route, DNS server address, or domain name from the external DHCP server, but you must do so from the CLI. See *Chapter 13: Dynamic Host Configuration Protocol (DHCP)*.

These instructions assume that you have already created the logical interface by selecting the encapsulation method for the physical interface. If you have not done so, see "Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces" on page 14-62. Stop before you assign the logical interface an IP address, and return to this section.

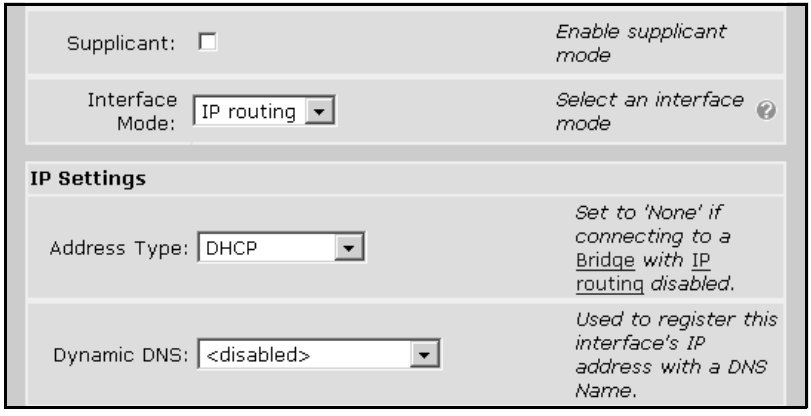

Figure 14-95. Enabling the DHCP Client on an Interface

To configure the interface to receive a dynamic address, follow these steps:

1. In the navigation bar, select *IP Interfaces* under *Router/Bridge*.
2. In the *IP Interfaces* window that is displayed, select the interface that you want to take the dynamic address. The *Configuration* window for that interface is displayed.
3. Scroll to the *IP Settings* section. Select *DHCP* from the *Address Type* pull-down menu.
4. Click *Apply*.

Configuring UDP Relay

You can configure the ProCurve Secure Router to forward packets destined to certain UDP ports to a helper address. For example, your LAN may include a DHCP server in only one of its VLANs. If your router will be routing between the VLANs, it might receive DHCP discover requests from some clients. You could configure the router to forward these requests to your network's DHCP server.

Follow these steps to configure UDP relay:

1. Select *UDP Relay* from the navigation bar.
2. Move to the *IP Helper Address* window.
3. Enter the IP address of the server to which the router should forward packets in the *IP Helper Address* fields.
4. From the *Interface* pull-down menu, select the interface on which the router will receive the packets that need to be forwarded.
5. Click *Add*.
6. If necessary, configure the helper address for a different interface. Repeat steps 3 through 5.

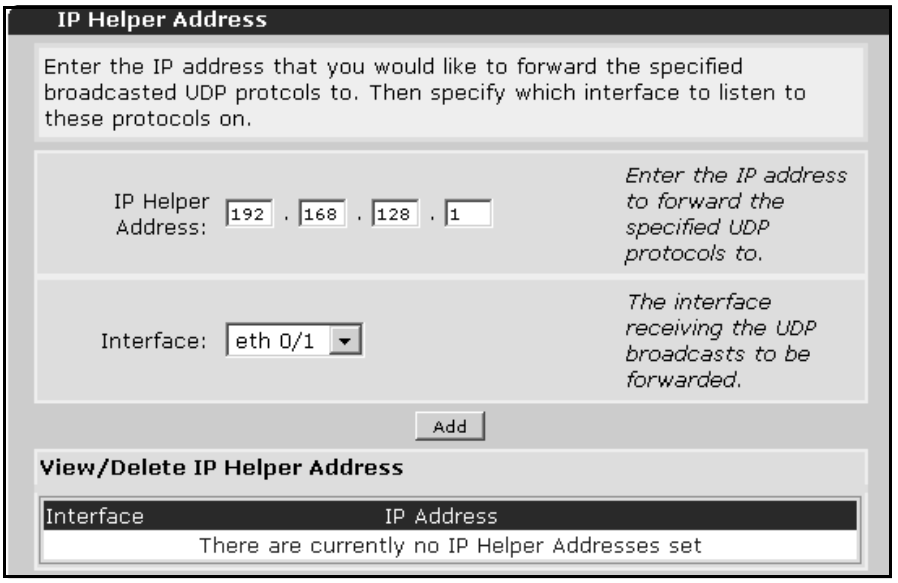

Figure 14-96. Configuring the Helper Address for UDP Relay

7. Move to the *UDP Forward Protocol* window.
8. Select the protocol for the packets that you want the router to forward from the *UDP Protocol* pull-down menu. For example, you could select *bootps (67)* to configure the router to forward DHCP requests.
9. Click *Add*.
10. You can specify multiple protocols by repeating steps 8 and 9.

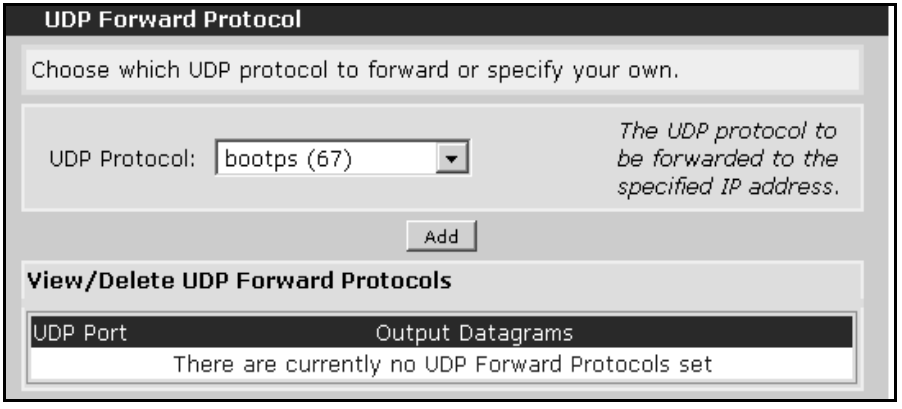

Figure 14-97. Configuring the Helper Address for UDP Relay