ProCurve Networking
HP Innovation

Management and Configuration Guide

ProCurve Wireless Access Point 530

www.procurve.com

invent

ProCurve
Wireless Access Point 530

Management and Configuration Guide

Publication Number

5991-2193
April 2006

Applicable Products

ProCurve Wireless Access Point 530 NA	(J8986A)
ProCurve Wireless Access Point 530 WW	(J8987A)

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, ProCurve Networking will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.
AP 530 Program
GNU GPL Source Code
Attn: ProCurve Networking Support
MS: 5550
Roseville, CA 95747 USA

Open source licenses pertaining to the open source software included with the product can be found in Appendix C in this guide.

Contents

4 Using the ProCurve Web Browser Interface

5 General System Configuration

6 Wireless Interface Configuration

7 Wireless Security Configuration

8 Special Features

9 Command Line Reference

A File Uploads, Downloads, and Resets

B Defaults

C Open Source Licenses

1

Getting Started

Contents

Introduction

This *Management and Configuration Guide* is intended to support the following access points:

- ProCurve Wireless Access Point 530 NA (J8986A)
- ProCurve Wireless Access Point 530 WW (J8987A)

This guide describes how to use the command line interface (CLI) and Web browser interface to configure, manage, and monitor access point operation. A troubleshooting chapter is also included.

The ProCurve Wireless Access Point 530 will be referenced as the Access Point 530 throughout the remainder of this document.

For information on other product documentation for this access point, refer to "Related Publications" on page 1-4.

The *Product Documentation CD-ROM* shipped with the access point includes a copy of this guide. You can also download a copy from the ProCurve Networking Web site, **http://www.procurve.com/**. (See "Getting Documentation From the Web" on page 1-6.)

Conventions

This guide uses the following conventions for command syntax and displayed information.

Command Syntax Statements

S*yntax*: radius-local *<username>* [disabled] [password *<password>*] [realname *<realname>*]

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces (< >) indicate a required choice.
- Curly brackets surrounding several sets of square brackets "{ [ ] | [ ] ..[ ] }" indicate at least one choice is required from the group of optional elements.
- Boldface indicate commands and keywords that are entered literally as shown. For example:

  "Use the **copy tftp** command to download the key from a TFTP server."

- *Italics* indicate arguments for which you must supply a variable value. For example, the command syntax, <*username*> indicates that you must provide a username:

  Syntax: radius-local <*username*>

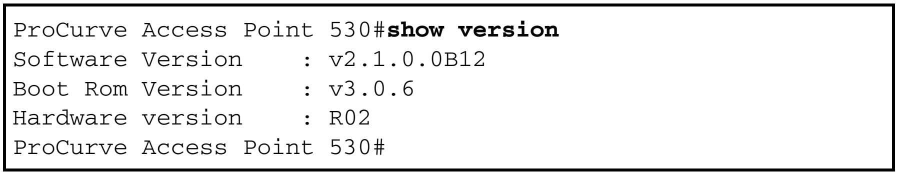
Command Prompts

In the default configuration, your access point displays the following CLI prompt:

```
ProCurve Access Point 530#
```

Screen Simulations

Figures containing simulated screen text and command output look like this:



```
ProCurve Access Point 530#show version
Software Version    : v2.1.0.0B12
Boot Rom Version    : v3.0.6
Hardware version    : R02
ProCurve Access Point 530#
```

Figure 1-1. Example of a Figure Showing a Simulated Screen

In some cases, brief command-output sequences appear outside of a numbered figure. For example:

```
ProCurve Access Point 530(ethernet)#ip address
192.168.1.2 255.255.255.0 192.168.1.253
ProCurve Access Point 530(ethernet)#dns primary-server
192.168.1.55
```

Related Publications

Installation and Getting Started Guide. Use the *Installation and Getting Started Guide* shipped with your access point to prepare for and perform the physical installation. This guide also steps you through connecting the access point to your network and assigning IP addressing, as well as describing the LED indications for correct operation and trouble analysis.

The *Installation and Getting Started Guide* and the *Management and Configuration Guide* are included as a PDF documents on the *Product Documentation CD-ROM* shipped with the access point. You can also download a copy from the ProCurve Networking Website. (See "Getting Documentation From the Web" on page 1-6.)

Release Notes. Release notes are posted on the ProCurve Networking Website and provide information on new software updates:

- New features and how to configure and use them
- Software management, including downloading software to the access point
- Software fixes addressed in current and previous releases

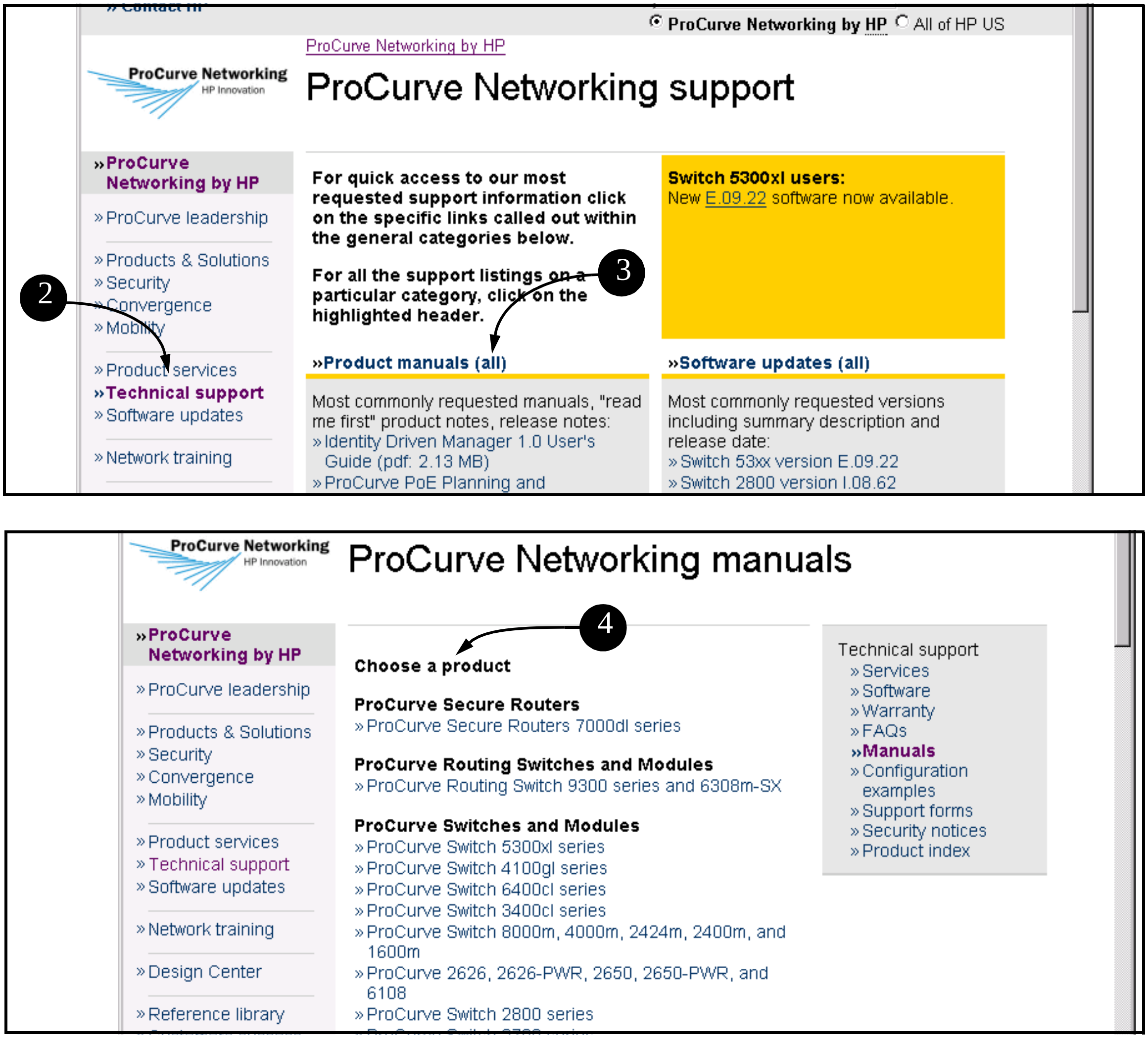
To view and download a copy of the latest release notes for your access point, see "Getting Documentation From the Web" on page 1-6.

Getting Documentation From the Web

1. Go to the ProCurve Networking Web site at

   http://www.procurve.com

2. Click on **Technical support**.
3. Click on **Product manuals**.
4. Click on the product for which you want to view or download a manual.



● ProCurve Networking by HP ○ All of HP US

ProCurve Networking by HP

ProCurve Networking support

» **ProCurve Networking by HP**
» ProCurve leadership
» Products & Solutions
» Security
» Convergence
» Mobility
» Product services
» **Technical support**
» Software updates
» Network training

For quick access to our most requested support information click on the specific links called out within the general categories below.

For all the support listings on a particular category, click on the highlighted header.

Switch 5300xl users:
New E.09.22 software now available.

»Product manuals (all)

Most commonly requested manuals, "read me first" product notes, release notes:
» Identity Driven Manager 1.0 User's Guide (pdf: 2.13 MB)
» ProCurve PoE Planning and

»Software updates (all)

Most commonly requested versions including summary description and release date:
» Switch 53xx version E.09.22
» Switch 2800 version I.08.62

ProCurve Networking manuals

» **ProCurve Networking by HP**
» ProCurve leadership
» Products & Solutions
» Security
» Convergence
» Mobility
» Product services
» Technical support
» Software updates
» Network training
» Design Center
» Reference library

Choose a product

ProCurve Secure Routers
» ProCurve Secure Routers 7000dl series

ProCurve Routing Switches and Modules
» ProCurve Routing Switch 9300 series and 6308m-SX

ProCurve Switches and Modules
» ProCurve Switch 5300xl series
» ProCurve Switch 4100gl series
» ProCurve Switch 6400cl series
» ProCurve Switch 3400cl series
» ProCurve Switch 8000m, 4000m, 2424m, 2400m, and 1600m
» ProCurve 2626, 2626-PWR, 2650, 2650-PWR, and 6108
» ProCurve Switch 2800 series

Technical support
» Services
» Software
» Warranty
» FAQs
» **Manuals**
» Configuration examples
» Support forms
» Security notices
» Product index

Figure 1-2. Finding Product Manuals on the ProCurve Networking Web site

Sources for More Information

- If you need information on specific features in the ProCurve Web Browser Interface, use the online help available for the Web browser interface. For more information on Web browser Help options, see "Online Help for the ProCurve Web Browser Interface" on page 4-8.
- If you need further information on the ProCurve access point technology, visit the ProCurve Networking Web site at:

  http://www.procurve.com

Need Only a Quick Start?

IP Addressing. If you just want to give the access point an IP address so that it can communicate on your network, HP recommends that you use the CLI to quickly configure IP addressing. To do so, do one of the following:

1. Login to the CLI Interface using the default username and password ("admin/admin").

   ```
   ProCurve Access Point 530 login#admin

   Password:admin

   ProCurve Access Point 530#
   ```

2. Enter **config** for global configuration at the CLI level prompt.

   ```
   ProCurve Access Point 530#config
   ```

3. Enter **ip address and subnet mask** at the CLI Ethernet Configuration level prompt.

   ```
   ProCurve Access Point 530(config)#interface
   ethernet

   ProCurve Access Point 530(ethernet)#ip address
   <address> <subnet_mask>
   ```

4. (Optional) Enter **an address for the default IP gateway** at the CLI Ethernet Configuration level prompt.

   ```
   ProCurve Access Point 530(ethernet)#ip default-
     gateway <gateway>
   ```

5. Save the current running configuration to the startup configuration.

   ```
   ProCurve Access Point 530(ethernet)#write mem
   ```

For more on using the CLI, see Chapter 9, "Using the Command Line Interface (CLI)".

To Set Up and Install the Access Point in Your Network

Important!

Use the *Installation and Getting Started Guide* shipped with your access point for the following:

- Notes, cautions, and warnings related to installing and using the access point
- Instructions for physically installing the access point in your network
- Quickly assigning an IP address, subnet mask, and gateway, set a Manager password, and (optionally) configure other basic features.
- Interpreting LED behavior.

For the latest version of the *Installation and Getting Started Guide* and other documentation for your access point, visit to the ProCurve Networking Website. (Refer to "Getting Documentation From the Web" on page 1-6.)

2

Selecting a Management Interface

Contents

Overview

This chapter describes the following:

- Access Point management interfaces
- Advantages of using each interface type

Understanding Management Interfaces

Management interfaces enable you to reconfigure the access point and to monitor its status and performance. Interface types include:

- **CLI**—a command line interface offering the full set of access point commands through the VT-100/ANSI console built into the access point. See "Advantages of Using the CLI" on page 5.
- **Web browser interface**—an access point interface offering status information and access point configuration, See "Advantages of Using the ProCurve 530 Browser Interface" on page 6.
- **SNMP**—a network management application such as the ProCurve Manager to manage the access point via the Simple Network Management Protocol (SNMP) from a network management station.

This manual describes how to use the CLI, the Web browser interface, and how to use these interfaces to configure and monitor the access point.

Advantages of Using the CLI

`ProCurve Access Point 530#`	Manager Exec Level
`ProCurve Access Point 530(config)#`	Global Configuration Level
`ProCurve Access Point 530(<interface>)#`	Interface Configuration Levels Context-specific configurations, such as (ethernet, wds1, radio1, radio1-wlan1).

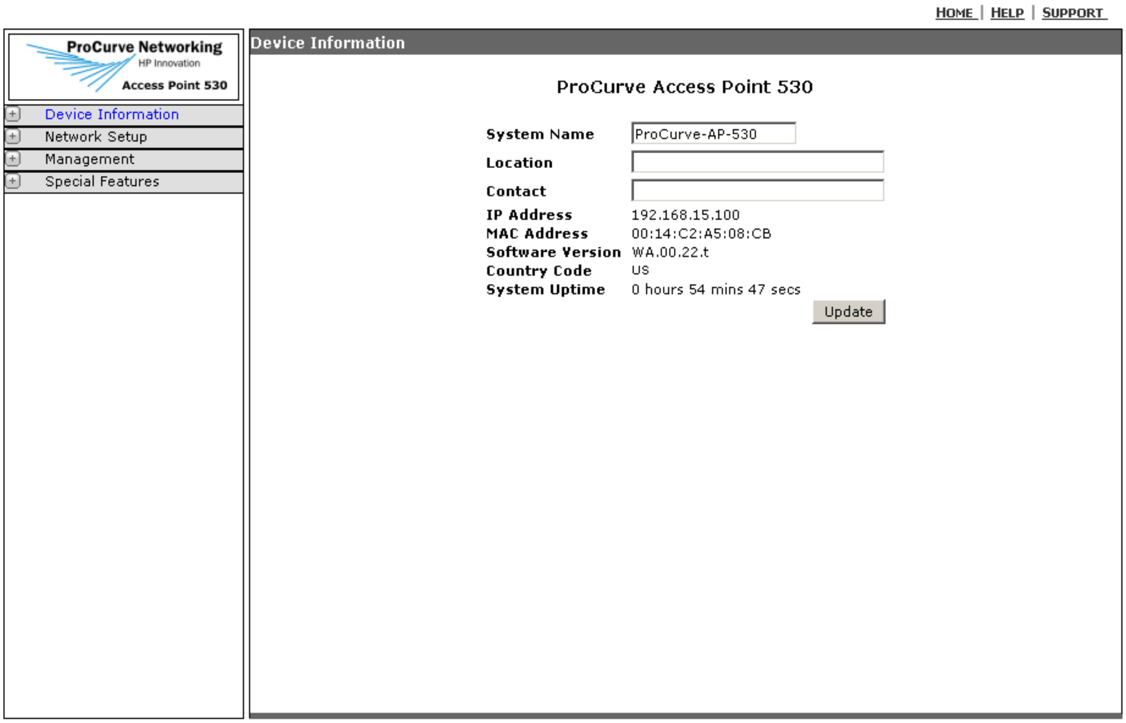
Figure 2-1. Command Prompt Examples

- Provides access to the complete set of the access point configuration features.
- Offers out-of-band access, through the RS-232 connection, or in-band access using Telnet or Secure Shell.
- Enables quick, detailed system configuration and management access to system operators and administrators experienced in command prompt interfaces.
- Provides help at each level for determining available options and variables.

CLI Usage

- For information on how to use the CLI, refer to Chapter 3, "Using the Command Line Interface (CLI)".
- To perform specific procedures (such as configuring IP addressing), use the Contents listing at the front of the manual to locate the information you need.
- For monitoring and analyzing access point operation, refer to the appropriate section in Chapter 5, “"General System Configuration".”
- For information on individual CLI commands, refer to Chapter 9, "Command Line Reference" or use the online Help provided in the CLI interface.

Advantages of Using the ProCurve 530 Browser Interface



Device Information

ProCurve Access Point 530

System Name: ProCurve-AP-530
Location:
Contact:
IP Address: 192.168.15.100
MAC Address: 00:14:C2:A5:08:CB
Software Version: WA.00.22.t
Country Code: US
System Uptime: 0 hours 54 mins 47 secs

Figure 2-2. Example of the ProCurve Access Point 530 Browser Interface

- **Easy access** to the access point from anywhere on the network.
- **Familiar browser interface**–locations of window objects consistent with commonly used browsers, uses mouse clicking for navigation, no terminal setup.
- **Many features have all their fields in one screen** so you can view all values at once.
- **More visual cues**, using colors, status bars, device icons, and other graphical objects instead of relying solely on alphanumeric values.
- **Display of acceptable ranges of values available** in configuration list boxes.

3

Using the Command Line Interface (CLI)

Contents

Overview

The Command Line Interface (CLI) is a text-based command interface for configuring and monitoring the access point. The CLI gives you access to the access point's full set of commands while providing the same password protection that is used in the Web browser interface.

Accessing the CLI

The CLI is accessed through the access point console. You can access the console out-of-band by directly connecting a terminal device to the access point, or in-band by using Telnet or a Secure Shell (SSH) client.

NOTE

Out-of-Band Requirements: To emulate the access point system console on a serial port connection, terminal emulation software needs to be installed on your PC (such as TeraTerm, which is available at http://www.ayera.com/teraterm).

In-Band Requirements: To emulate the access point system console through an in-band connection, SSH software needs to be installed on your PC (such as PUTTY, which is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/).

Direct Console Access

To connect a console directly to the access point, use a null-modem cable or an HP serial cable, part number 5184-1894 (shipped with many HP ProCurve switches). Connect the serial cable between a PC or VT-100 terminal to be used as a console and the access point's Console port. Configure the PC terminal emulator as a DEC VT-100 (ANSI) terminal or use a VT-100 terminal, and configure either one to operate with these settings:

- Port is COM1 (COM1 is the standard port, however, your PC might use a different COM port (e.g. COM2)
- 9600 baud (default is set to 9600)

  Note: If the Baud rate setting is not correct, the system console messages will become unreadable.
- 8 data bits, 1 stop bit, parity set to None, and flow control set to None.
- For the Windows Terminal program, also disable (uncheck) the “Use Function, Arrow, and Ctrl Keys for Windows” option.
- For the Hilgraeve HyperTerminal program, select the “Terminal keys” option for the “Function, arrow, and ctrl keys act as” parameter.

Hint

To clear unreadable console messages, change the Baud rate.
For example, on TeraTerm: (1) Access "Control" menu and select "Reset" terminal, (2) Change Baud rate, and if necessary, (3) Access "Setup" menu , select "Window" and change the "Scroll buffer" value.

When correctly connected to the access point, press **[Enter]** to initiate the console session.

For more information on connecting to the access point's Console port, refer to the *Installation and Getting Started Guide*.

Telnet Access

To access the console through a Telnet session, first make sure the access point is configured with an IP address and that it is reachable from the PC that is running the Telnet session (for example, use a **ping** command to the access point's IP address).

Start the Telnet program on the PC using the access point's IP address (or DNS name).

telnet 10.11.12.195 [Enter]*Example of an IP address.*

telnet AP530 [Enter] *Example of a DNS-type name.*

Secure Shell Access

If the network is already deployed and the access point has a configured IP address, you can access the console through an SSH session. The access point must also be configured with an IP address and be reachable from the management station PC (for example, use a **ping** command to the access point's IP address).

Using the access point through a SSH client provides a secured connection as traffic is encrypted.

Start the SSH program on the PC using the access point's IP address (or DNS name).

ssh 10.11.12.195 [Enter]*Example of an IP address.*

ssh AP530 [Enter] *Example of a DNS-type name.*

Note

The default Static IP address is 192.168.1.10. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup.

After boot up, the SSH server needs about two minutes to generate host encryption keys. The SSH server is disabled while the keys are being generated.

For more information on the Secure Shell, see "Setting Management Access Controls" on page 5-8.

Using the CLI

The CLI commands are organized into the following levels:

1. Manager EXEC
2. Global Configuration
3. Interface Configuration
4. Radio Configuration
5. WLAN Configuration

Note

Except for most of the user-entered parameters (e.g. SSID strings, passwords, etc.), CLI commands are not generally case-sensitive.

The access point supports one user account type, the Manager account with full privileges. The number of commands available are delineated by the configuration levels.

When you use the CLI to make a configuration change, you must save the configuration to retain the changes upon rebooting the access point.

Command Level at Logon

By default, the access point defaults the Manager user name to 'admin' for CLI access with the password defaulted to 'admin'. To secure management access to the access point, you must set the Manager password. *Without a Manager password configured, anyone having serial port or Telnet access to the access point can reach all CLI command modes.*

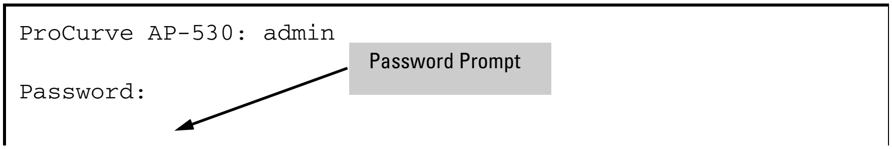
Caution

HP strongly recommends that you configure a Manager password. If a Manager password is not configured, the access point is not password-protected, and anyone having in-band or out-of-band access to the access point may be able to compromise access point and network security.

For additional security, it is also possible to disable CLI management access through the serial port, ssh, or Telnet. For more information, see "Web: Configuring Management Controls" on page 5-9.

When you log onto the access point CLI, you will be prompted to enter an account user name (the default is admin).

After entry of the user name, you will be prompted for the password. The default password is admin.
For example:



```
ProCurve AP-530: admin

Password:
```

Password Prompt

Figure 3-1. Example of CLI Log-On Screen with Password

When you successfully log onto the CLI, you will see the following command prompt:

```
ProCurve Access Point 530#_
```

Command Level Operation

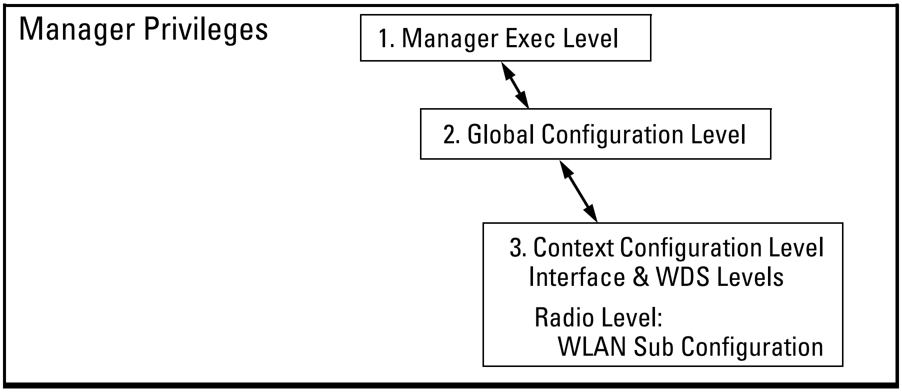


Figure 3-2. Access Sequence for Command Levels

Manager Privileges

Manager privileges allow you to examine the current configuration, make system configuration changes, and move between the three levels of access: Exec, Global Configuration, and Context Configuration. (See figure 3-2.) A "#" character delimits the Manager prompt. For example:

`ProCurve Acess Point 530#`_*Manager prompt.*_

- **Manager Exec level**: Allows you to examine the current configuration, perform basic system-level actions, reset the access point, and move to the configuration access levels. The prompt for the Manager Exec level contains only the system name and the "#" delimiter, as shown above.
- **Global Configuration level:** Enables you to make configuration changes to the access point's software features. The prompt for the Global Configuration level includes the system name and "`(config)`". To select this level, enter the **configure** command at the Exec prompt. For example:

  `ProCurve Acess Point 530#` *Enter* **configure** *at the Manager prompt.*
  `ProCurve Acess Point 530(config)#`*The Global Config prompt.*

- **Interface Configuration level:** Enables you to make configuration changes to a specific interface, such as the Ethernet interface or any of the WDS interfaces. To enter the Ethernet or WDS levels, use the **interface** command at the Exec prompt. The WDS name will have the format "wdsX" where "X" is a number from 1 to 6.
  For example:

`ProCurve Acess Point 530(config)#`*Enter* **interface ethernet** *at the Global Config prompt.*

`ProCurve Acess Point 530(ethernet)#, or`

`ProCurve Acess Point 530(config)#`*Enter* **interface wds2** *at the Global Config prompt.*

`ProCurve Acess Point 530(wds2)#`

- **Radio Configuration level:** Enables you to make configuration changes in the Radio context level and access the WLAN(BSS/SSID) context level.

`ProCurve Acess Point 530(config)#`*Enter* **radio 1** *at the Global Config prompt.*

`ProCurve Acess Point 530(radio1)#` *Enter* **wlan 1** *at the Radio Context prompt.*

`ProCurve Acess Point 530(radio1-wlan1)#`

Table 3-1. Command Level Hierarchy

Command Level	Example of Prompt and Permitted Operations	
Manager Privileges		For a list of available commands, enter ? at the prompt.
Manager Exec Level DEFAULT LEVEL	ProCurve Acess Point 530#	Perform system-level actions such as system control, monitoring, and diagnostic commands.
Global Configuration Level	ProCurve Acess Point 530(config)#	Execute configuration commands.
Interface Configuration Level	ProCurve Acess Point 530(ethernet)# ProCurve Acess Point 530(wds1)# ProCurve Acess Point 530(radio1)# ProCurve Acess Point 530 (radio1-wlan1)#	Execute context-specific configuration commands, such as a particular access point interface. This is useful for entering a series of commands for the same context. The name of the interface ("ethernet") or ("wds")is displayed in the parentheses. The WDS name will have the format "wdsX" where "X" is a number from 1 to 6. The name of the radio is displayed in the parentheses. The name of the radio is either "radio1" or "radio2." The name of the radio and WLAN (BSS/ SSID) are displayed in the parentheses. The WLAN name will have the format "wlanX" where "X" is a number from 1 to 16.

How To Move Between Levels

Change in Levels	Example of Prompt, Command, and Result
Manager Exec level *to* Global configuration level	ProCurve Acess Point 530#**config** ProCurve Acess Point 530(config)#
Global configuration level *to a* Context configuration level	ProCurve Acess Point 530(config)#**interface ethernet** ProCurve Acess Point 530(ethernet)#
Move from any level to the preceding level	ProCurve Acess Point 530(ethernet)#**exit** ProCurve Acess Point 530(config)#**exit** ProCurve Acess Point 530#
Move from any level to the Manager Exec level	ProCurve Acess Point 530(ethernet)#**end** ProCurve Acess Point 530# *—or—* ProCurve Acess Point 530(config)#**end** ProCurve Acess Point 530#

Changing Parameter Settings. Regardless of which interface is used (CLI, or Web browser interface), the most recently configured version of a parameter setting overrides any earlier settings for that parameter. For example, if you use the Web interface to configure an IP address of "*X*" for the Ethernet interface and later use the CLI to configure a different IP address of "*Y*", then "*Y*" replaces "*X*" as the IP address for the Ethernet interface.

Changes made through the Web interface are immediately applied to the startup configuration, whereas changes made through the CLI interface are only made to the running configuration, and must be saved using the "copy" or "write memory" command if they are to persist following a reboot.

To save the running configuration changes to the startup configuration using the CLI Interface:

```
ProCurve Acess Point 530(ethernet)#write memory
```

Listing Commands and Command Options

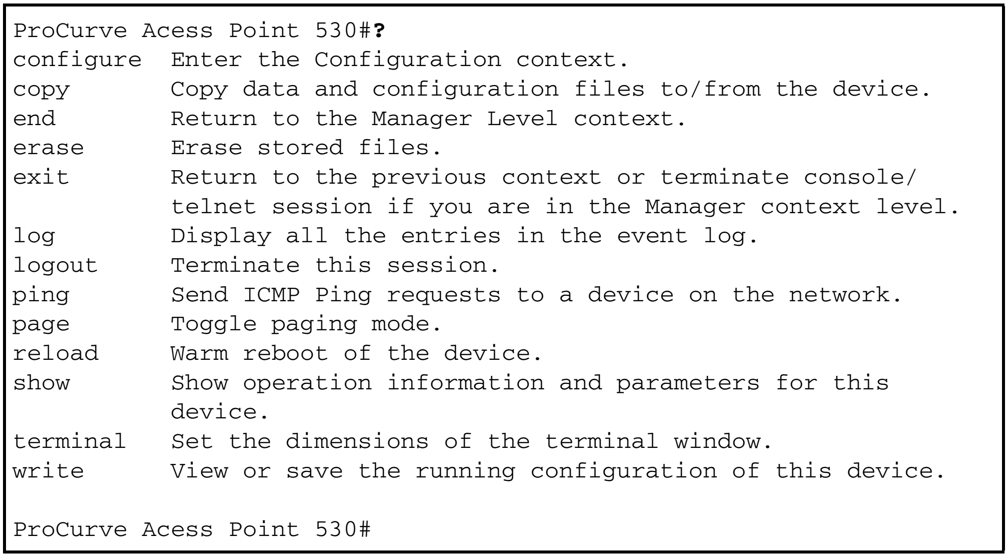
At any command level you can:

- List all of the commands available at that level
- List the options for a specific command

Listing Commands Available at Any Command Level

At a given command level you can list and execute the commands that level offers, plus any relevant commands available at preceding levels. For example, at the Manager Exec level, you can list and execute only the Exec level commands. However, at the Global Configuration level, you can list and execute the commands available at the Global Configuration level and the commands available at the Manager Exec level (except for the "configure [terminal]" command).

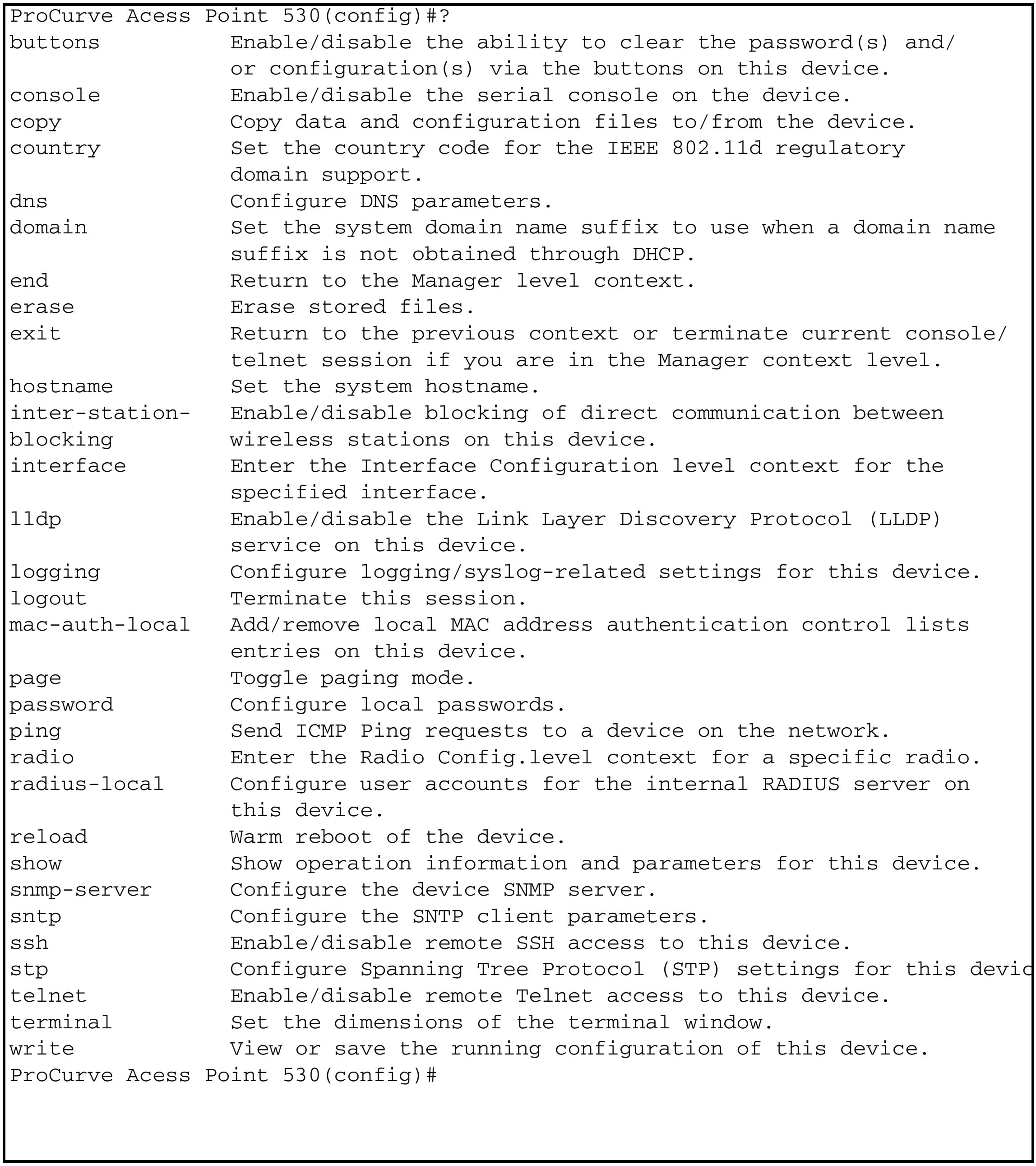
Type "?" or Press "Tab Key" To List Available Commands. Typing the **?** symbol or pressing the tab key lists the commands you can execute at the current level. For example, typing **?** at the Manager Exec level produces this listing:



```
ProCurve Acess Point 530#?
configure  Enter the Configuration context.
copy       Copy data and configuration files to/from the device.
end        Return to the Manager Level context.
erase      Erase stored files.
exit       Return to the previous context or terminate console/
           telnet session if you are in the Manager context level.
log        Display all the entries in the event log.
logout     Terminate this session.
ping       Send ICMP Ping requests to a device on the network.
page       Toggle paging mode.
reload     Warm reboot of the device.
show       Show operation information and parameters for this
           device.
terminal   Set the dimensions of the terminal window.
write      View or save the running configuration of this device.

ProCurve Acess Point 530#
```

Figure 3-3. Example of the Manager Exec Level Command Listing

Typing **?** at the Global Configuration level produces this listing:



```
ProCurve Acess Point 530(config)#?
buttons           Enable/disable the ability to clear the password(s) and/
                  or configuration(s) via the buttons on this device.
console           Enable/disable the serial console on the device.
copy              Copy data and configuration files to/from the device.
country           Set the country code for the IEEE 802.11d regulatory
                  domain support.
dns               Configure DNS parameters.
domain            Set the system domain name suffix to use when a domain name
                  suffix is not obtained through DHCP.
end               Return to the Manager level context.
erase             Erase stored files.
exit              Return to the previous context or terminate current console/
                  telnet session if you are in the Manager context level.
hostname          Set the system hostname.
inter-station-    Enable/disable blocking of direct communication between
blocking          wireless stations on this device.
interface         Enter the Interface Configuration level context for the
                  specified interface.
lldp              Enable/disable the Link Layer Discovery Protocol (LLDP)
                  service on this device.
logging           Configure logging/syslog-related settings for this device.
logout            Terminate this session.
mac-auth-local    Add/remove local MAC address authentication control lists
                  entries on this device.
page              Toggle paging mode.
password          Configure local passwords.
ping              Send ICMP Ping requests to a device on the network.
radio             Enter the Radio Config.level context for a specific radio.
radius-local      Configure user accounts for the internal RADIUS server on
                  this device.
reload            Warm reboot of the device.
show              Show operation information and parameters for this device.
snmp-server       Configure the device SNMP server.
sntp              Configure the SNTP client parameters.
ssh               Enable/disable remote SSH access to this device.
stp               Configure Spanning Tree Protocol (STP) settings for this devic
telnet            Enable/disable remote Telnet access to this device.
terminal          Set the dimensions of the terminal window.
write             View or save the running configuration of this device.
ProCurve Acess Point 530(config)#
```

Figure 3-4. Example of the Configuration-Level Command Listing

Typing **?** at the Context Configuration level produces similar results.

If **- - MORE - -** appears, there are more commands in the listing. To list the next page of commands, press the Space bar. To list the remaining commands one-by-one, repeatedly press **[Enter]**. To quit the listing, type **[Ctrl] [C]**.

Use [Tab] To Complete a Command Word. You can use **[Tab]** to quickly complete the current word in a command. To do so, type one or more consecutive characters for a command and then press **[Tab]** (with no spaces allowed). The CLI completes the current word (if you have typed enough of the word for the CLI to distinguish it from other possibilities). For example, at the Global Configuration level, if you press **[Tab]** immediately after typing "**s**", the CLI displays the command that begins with "s". For example:

```
ProCurve Acess Point 530(config)#s[Tab]
ProCurve Acess Point 530(config)#s
 show
 snmp-server
 sntp
 ssh
 stp
```

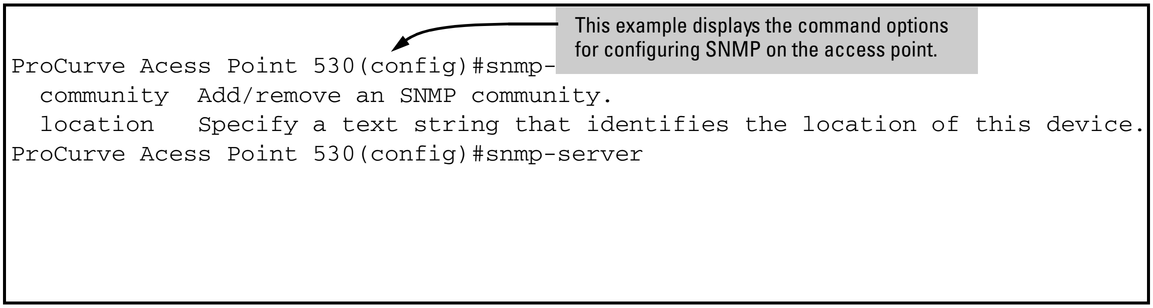
Use Shorthand Entries. You can abbreviate commands and options as long as they contain enough letters to be distinguished from any other currently available commands or options.

Command Option Displays

Conventions for CLI Syntax Used in Documentation. When you use the CLI to list options for a particular command, you will see one or more of the following conventions used in the documentation to help you interpret the command data:

- Braces (< >) or angled braces *(< >)* indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive options in a command.

Listing Command Options. You can use the CLI to remind you of the options available for a command by entering command keywords followed by**? or the Tab key**. For example, suppose you want to see the command options for configuring SNMP:



This example displays the command options for configuring SNMP on the access point.

```
ProCurve Acess Point 530(config)#snmp-
  community  Add/remove an SNMP community.
  location   Specify a text string that identifies the location of this device.
ProCurve Acess Point 530(config)#snmp-server
```

Figure 3-5. Example of How To List the Options for a Specific Command

Configuration Commands and the Context Configuration Modes

You can execute basic configuration commands in the global configuration mode. However, you must use a context mode to execute context-specific commands.

The configuration options include Manager Exec, Global, and Context Configuration context modes:

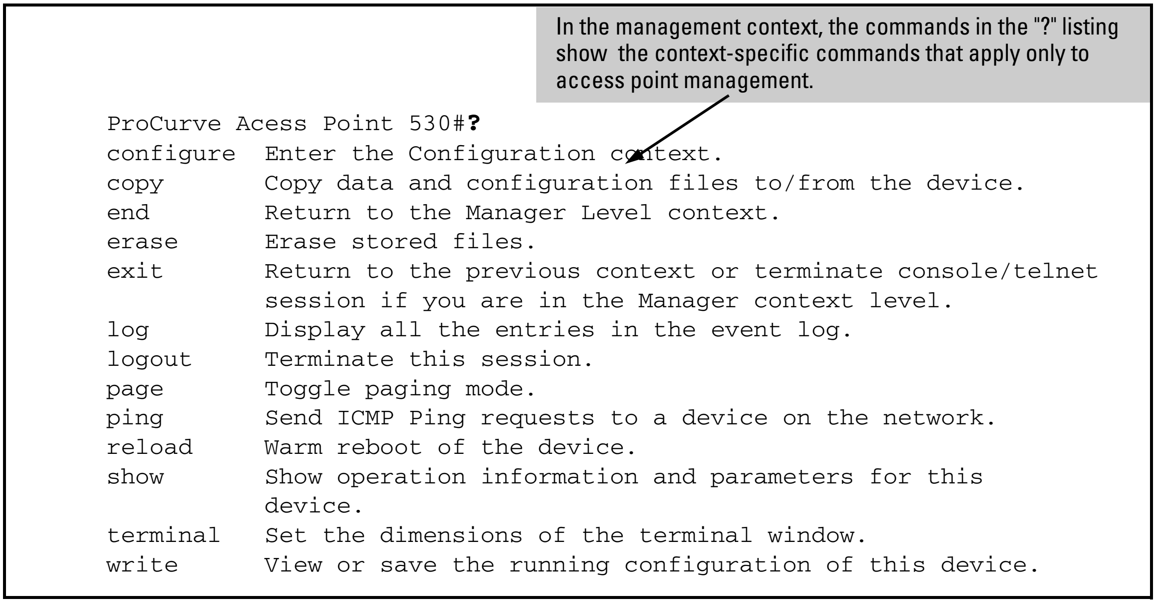
Management Context . Includes specific commands that apply only to management access to the access point. The prompt for this mode includes the identity of the context:

```
ProCurve Acess Point 530#
```

The prompt at login automatically defaults to the Manager Exec level.

```
ProCurve Acess Point 530#?
```

Lists the commands you can use in the management context.



In the management context, the commands in the "?" listing show the context-specific commands that apply only to access point management.

```
ProCurve Acess Point 530#?
configure  Enter the Configuration context.
copy       Copy data and configuration files to/from the device.
end        Return to the Manager Level context.
erase      Erase stored files.
exit       Return to the previous context or terminate console/telnet
           session if you are in the Manager context level.
log        Display all the entries in the event log.
logout     Terminate this session.
page       Toggle paging mode.
ping       Send ICMP Ping requests to a device on the network.
reload     Warm reboot of the device.
show       Show operation information and parameters for this
           device.
terminal   Set the dimensions of the terminal window.
write      View or save the running configuration of this device.
```

Figure 3-6. Context-Specific Commands Affecting the Manager Exec Context

Global Context . Includes commands applied globally. The prompt for this mode includes the identity of the Global interface:

```
ProCurve Acess Point 530#configure
```

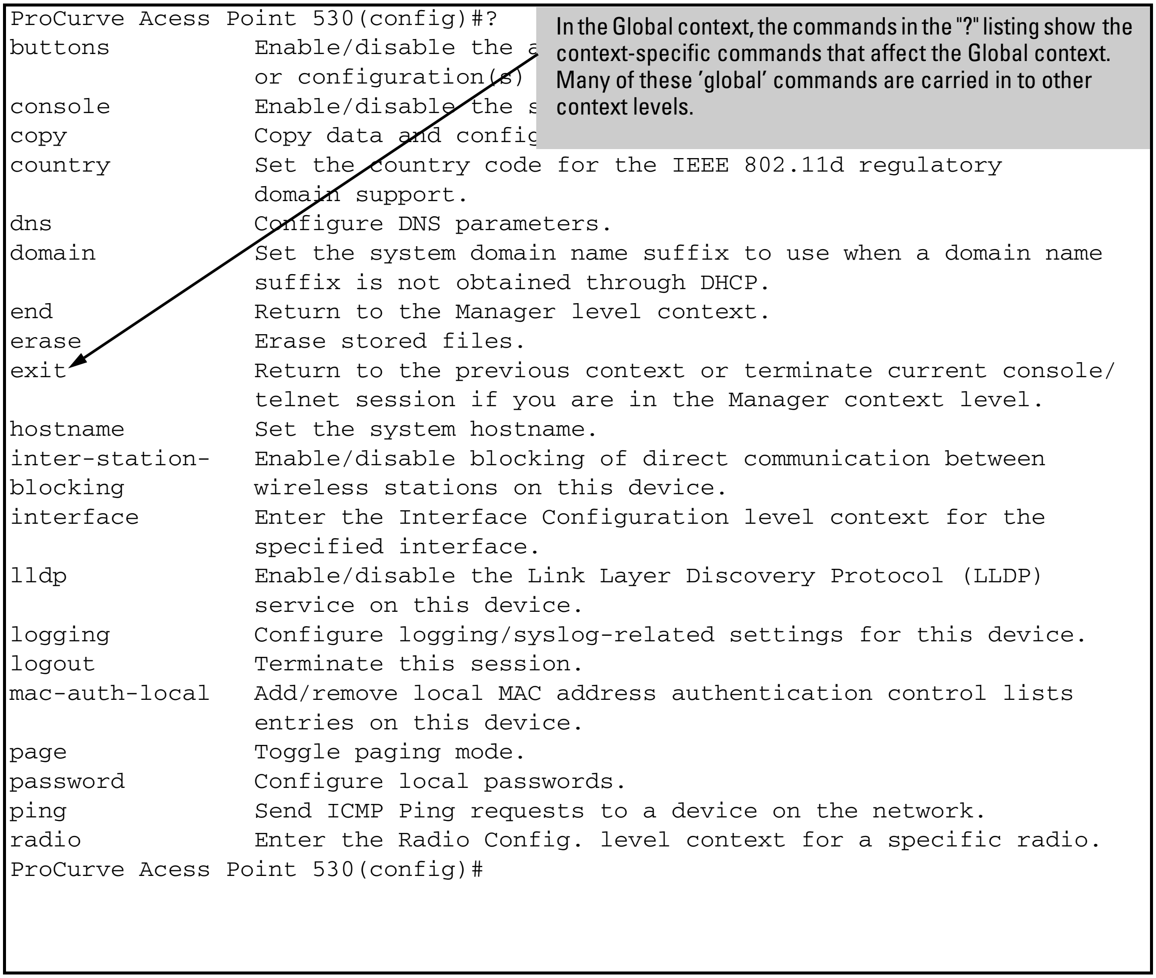
Command executed at configuration level for entering Global context.

```
ProCurve Acess Point 530(config)#
```

Resulting prompt showing Global context.

```
ProCurve Acess Point 530(config)#?
```

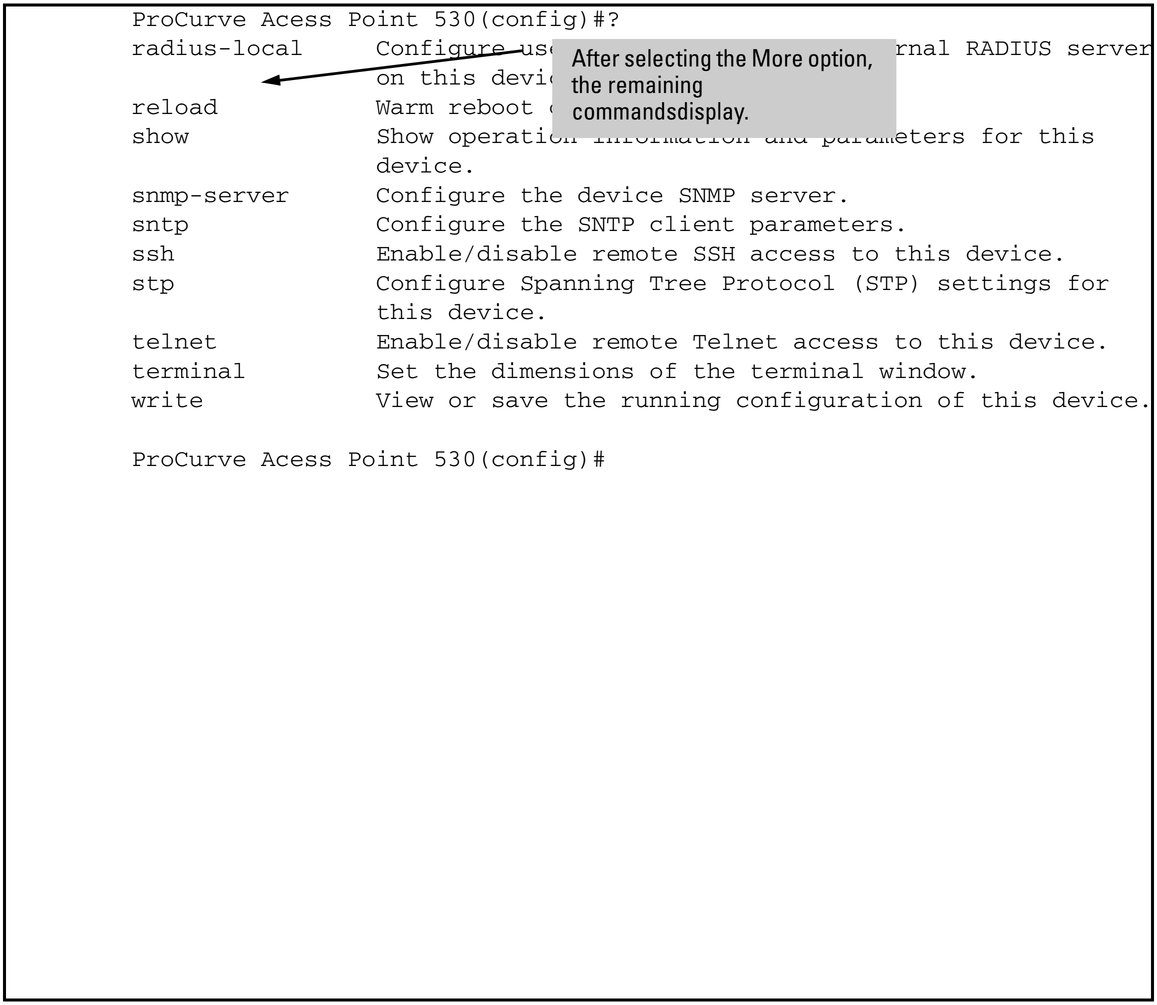
Lists the commands you can use in the Global context.



```
ProCurve Acess Point 530(config)#?
buttons            Enable/disable the a
                   or configuration(s)
console            Enable/disable the s
copy               Copy data and config
country            Set the country code for the IEEE 802.11d regulatory
                   domain support.
dns                Configure DNS parameters.
domain             Set the system domain name suffix to use when a domain name
                   suffix is not obtained through DHCP.
end                Return to the Manager level context.
erase              Erase stored files.
exit               Return to the previous context or terminate current console/
                   telnet session if you are in the Manager context level.
hostname           Set the system hostname.
inter-station-     Enable/disable blocking of direct communication between
blocking           wireless stations on this device.
interface          Enter the Interface Configuration level context for the
                   specified interface.
lldp               Enable/disable the Link Layer Discovery Protocol (LLDP)
                   service on this device.
logging            Configure logging/syslog-related settings for this device.
logout             Terminate this session.
mac-auth-local     Add/remove local MAC address authentication control lists
                   entries on this device.
page               Toggle paging mode.
password           Configure local passwords.
ping               Send ICMP Ping requests to a device on the network.
radio              Enter the Radio Config. level context for a specific radio.
ProCurve Acess Point 530(config)#
```

In the Global context, the commands in the "?" listing show the context-specific commands that affect the Global context. Many of these ’global’ commands are carried in to other context levels.

Figure 3-7. Context-Specific Commands Affecting Global Context



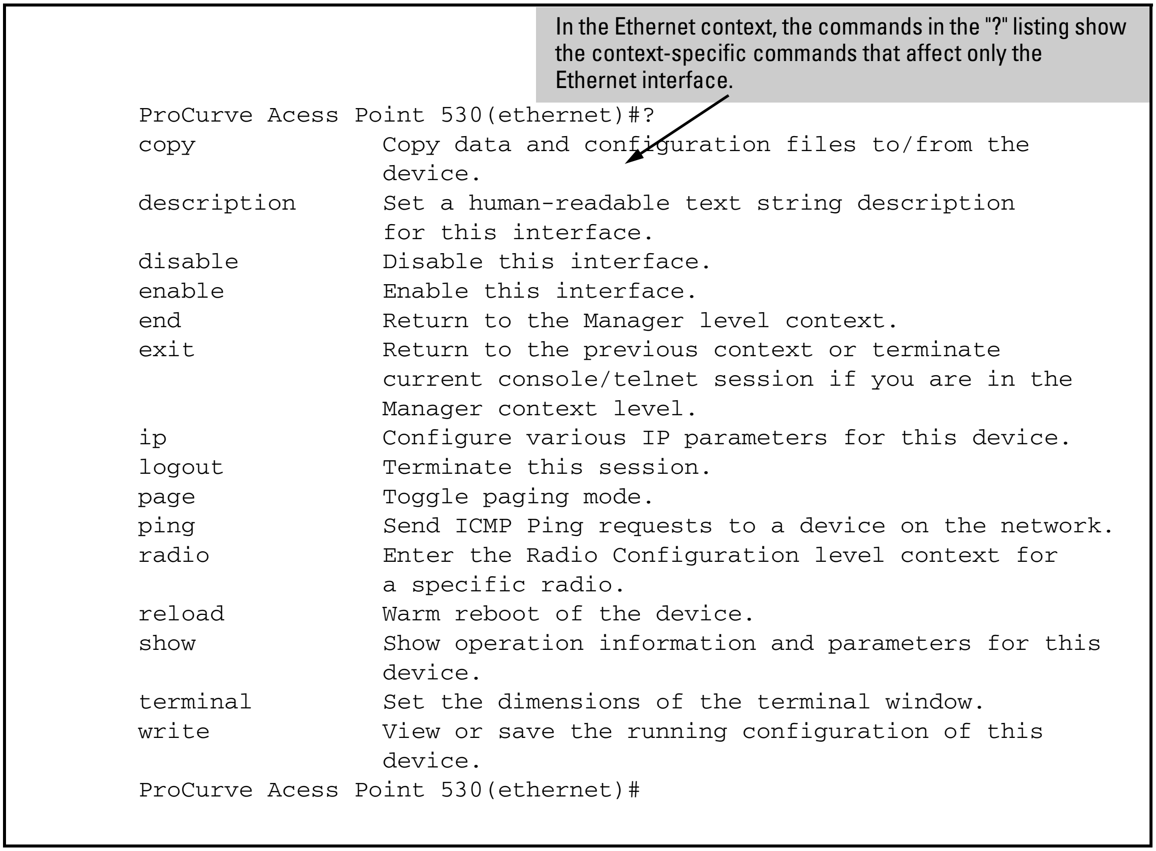
```
ProCurve Acess Point 530(config)#?
radius-local     Configure use                         rnal RADIUS server
                 on this devic
reload           Warm reboot c
show             Show operation information and parameters for this
                 device.
snmp-server      Configure the device SNMP server.
sntp             Configure the SNTP client parameters.
ssh              Enable/disable remote SSH access to this device.
stp              Configure Spanning Tree Protocol (STP) settings for
                 this device.
telnet           Enable/disable remote Telnet access to this device.
terminal         Set the dimensions of the terminal window.
write            View or save the running configuration of this device.

ProCurve Acess Point 530(config)#
```

After selecting the More option, the remaining commandsdisplay.

Figure 3-8. Context-Specific Commands Affecting Global Context [MORE]

Ethernet Interface Context . Includes interface-specific commands that apply only to the Ethernet interface. The prompt for this mode includes the identity of the Ethernet interface:

`ProCurve Acess Point 530(config)#interface ethernet`	Command executed at configuration level for entering Ethernet interface context.
`ProCurve Acess Point 530(ethernet)#`	Resulting prompt showing Ethernet interface context.
`ProCurve Acess Point 530(ethernet)#?`	Lists the commands you can use in the Ethernet interface context.



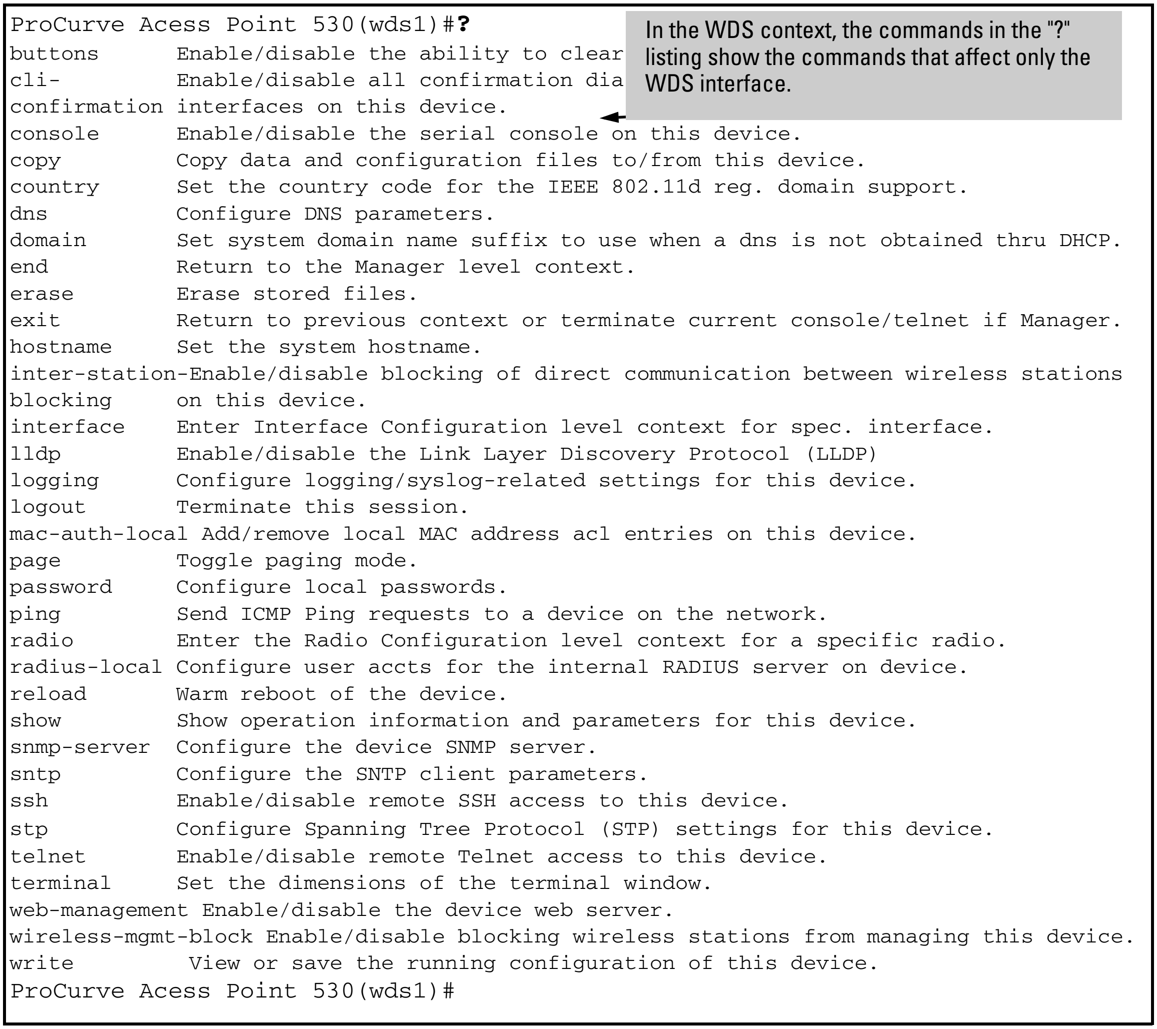
In the Ethernet context, the commands in the "?" listing show the context-specific commands that affect only the Ethernet interface.

```
ProCurve Acess Point 530(ethernet)#?
copy                Copy data and configuration files to/from the
                    device.
description         Set a human-readable text string description
                    for this interface.
disable             Disable this interface.
enable              Enable this interface.
end                 Return to the Manager level context.
exit                Return to the previous context or terminate
                    current console/telnet session if you are in the
                    Manager context level.
ip                  Configure various IP parameters for this device.
logout              Terminate this session.
page                Toggle paging mode.
ping                Send ICMP Ping requests to a device on the network.
radio               Enter the Radio Configuration level context for
                    a specific radio.
reload              Warm reboot of the device.
show                Show operation information and parameters for this
                    device.
terminal            Set the dimensions of the terminal window.
write               View or save the running configuration of this
                    device.
ProCurve Acess Point 530(ethernet)#
```

Figure 3-9. Context-Specific Commands Affecting Ethernet Interface Context

WDS Interface Context . Includes specific commands that apply only to the WDS wireless interface. The prompt for this mode includes the identity of the wireless interface:

`ProCurve Acess Point 530(config)#interface wds1`	Command executed at configuration level to enter wireless context.
`ProCurve Acess Point 530(wds1)#`	Resulting prompt showing the WDS wireless context.
`ProCurve Acess Point 530(wds1)#?`	Lists commands you can use in the WDS wireless context.



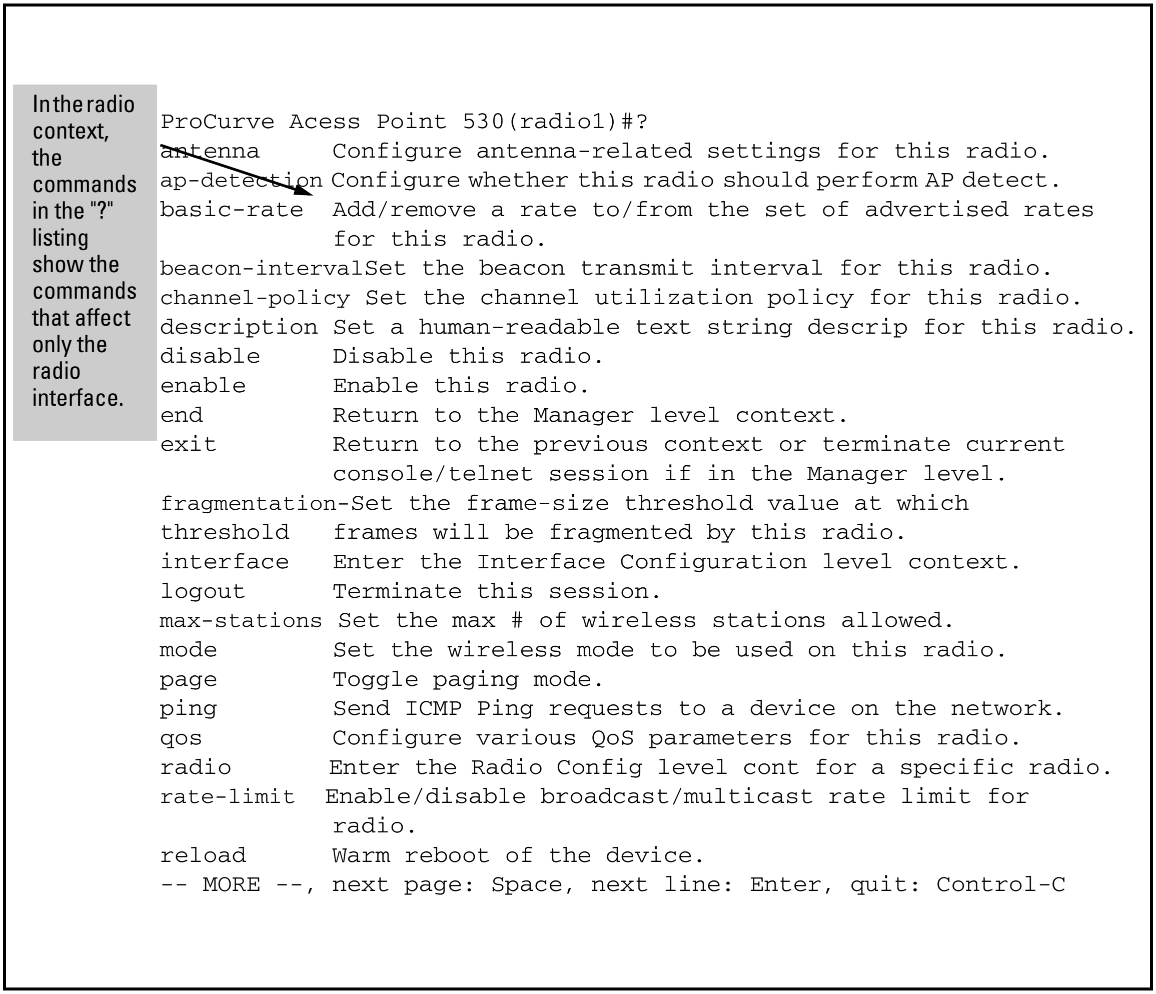
```
ProCurve Acess Point 530(wds1)#?
buttons       Enable/disable the ability to clear
cli-          Enable/disable all confirmation dia
confirmation interfaces on this device.
console       Enable/disable the serial console on this device.
copy          Copy data and configuration files to/from this device.
country       Set the country code for the IEEE 802.11d reg. domain support.
dns           Configure DNS parameters.
domain        Set system domain name suffix to use when a dns is not obtained thru DHCP.
end           Return to the Manager level context.
erase         Erase stored files.
exit          Return to previous context or terminate current console/telnet if Manager.
hostname      Set the system hostname.
inter-station-Enable/disable blocking of direct communication between wireless stations
blocking      on this device.
interface     Enter Interface Configuration level context for spec. interface.
lldp          Enable/disable the Link Layer Discovery Protocol (LLDP)
logging       Configure logging/syslog-related settings for this device.
logout        Terminate this session.
mac-auth-local Add/remove local MAC address acl entries on this device.
page          Toggle paging mode.
password      Configure local passwords.
ping          Send ICMP Ping requests to a device on the network.
radio         Enter the Radio Configuration level context for a specific radio.
radius-local Configure user accts for the internal RADIUS server on device.
reload        Warm reboot of the device.
show          Show operation information and parameters for this device.
snmp-server  Configure the device SNMP server.
sntp          Configure the SNTP client parameters.
ssh           Enable/disable remote SSH access to this device.
stp           Configure Spanning Tree Protocol (STP) settings for this device.
telnet        Enable/disable remote Telnet access to this device.
terminal      Set the dimensions of the terminal window.
web-management Enable/disable the device web server.
wireless-mgmt-block Enable/disable blocking wireless stations from managing this device.
write          View or save the running configuration of this device.
ProCurve Acess Point 530(wds1)#
```

In the WDS context, the commands in the "?" listing show the commands that affect only the WDS interface.

Figure 3-10. Context-Specific Commands Affecting WDS Interface Context

Radio Context . Includes radio-specific commands that apply to their respective radio. The prompt for this mode includes the identity of the radio:

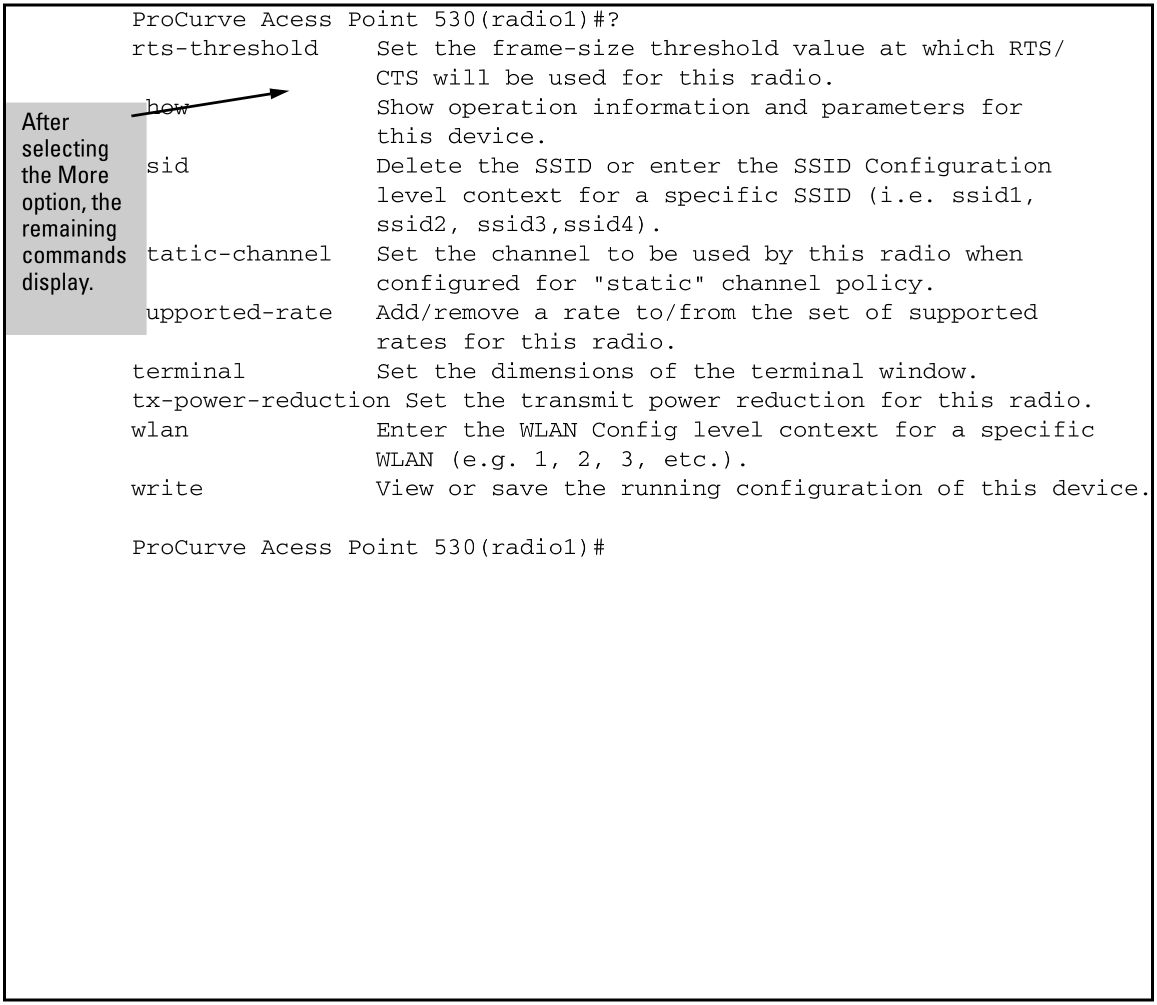
`ProCurve Acess Point 530(config)#radio 1`	Command executed at configuration level to enter a specific radio level.
`ProCurve Acess Point 530(radio1)#`	Resulting prompt showing wireless context.
`ProCurve Acess Point 530(radio1)#`**`?`**	Lists commands you can use in the wireless context.



In the radio context, the commands in the "?" listing show the commands that affect only the radio interface.

```
ProCurve Acess Point 530(radio1)#?
antenna       Configure antenna-related settings for this radio.
ap-detection Configure whether this radio should perform AP detect.
basic-rate    Add/remove a rate to/from the set of advertised rates
              for this radio.
beacon-intervalSet the beacon transmit interval for this radio.
channel-policy Set the channel utilization policy for this radio.
description Set a human-readable text string descrip for this radio.
disable       Disable this radio.
enable        Enable this radio.
end           Return to the Manager level context.
exit          Return to the previous context or terminate current
              console/telnet session if in the Manager level.
fragmentation-Set the frame-size threshold value at which
threshold     frames will be fragmented by this radio.
interface     Enter the Interface Configuration level context.
logout        Terminate this session.
max-stations Set the max # of wireless stations allowed.
mode          Set the wireless mode to be used on this radio.
page          Toggle paging mode.
ping          Send ICMP Ping requests to a device on the network.
qos           Configure various QoS parameters for this radio.
radio        Enter the Radio Config level cont for a specific radio.
rate-limit  Enable/disable broadcast/multicast rate limit for
              radio.
reload        Warm reboot of the device.
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

Figure 3-11. Context-Specific Commands Affecting Radio Context



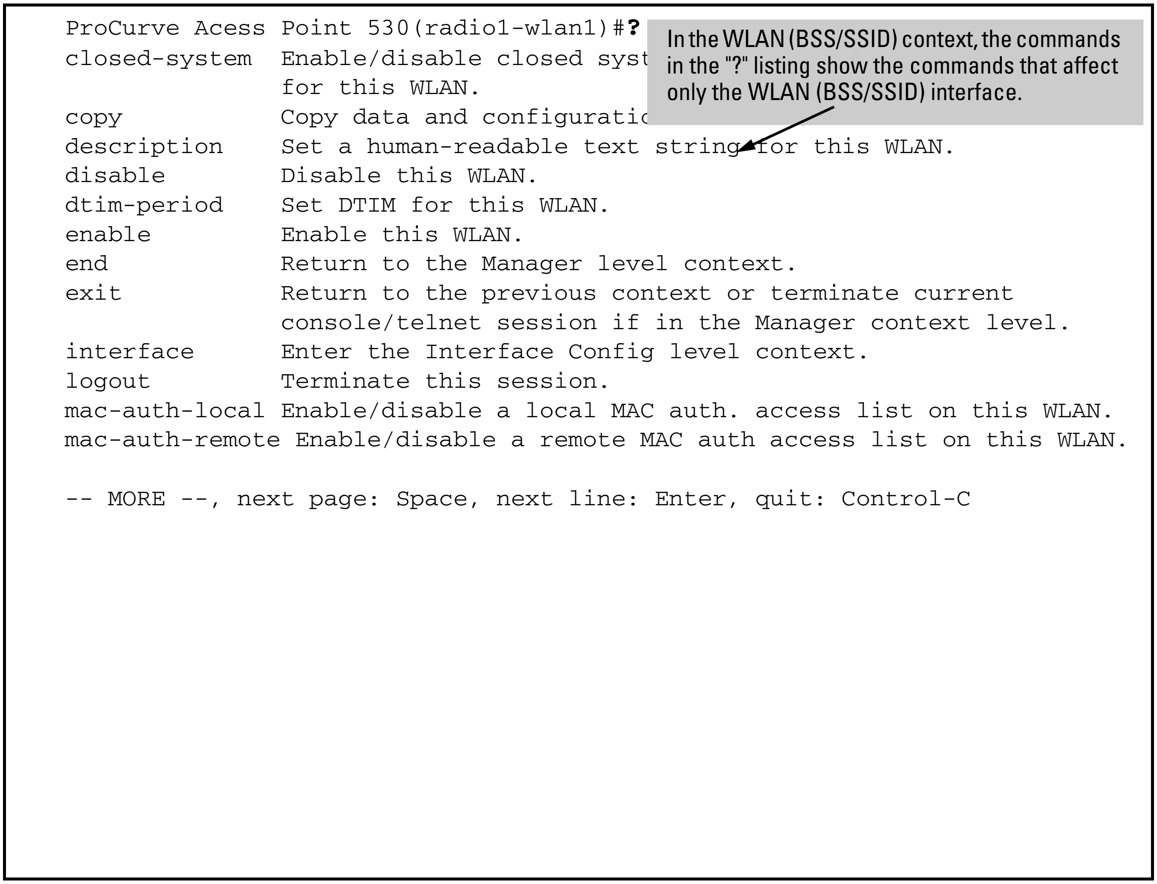
```
ProCurve Acess Point 530(radio1)#?
rts-threshold     Set the frame-size threshold value at which RTS/
                  CTS will be used for this radio.
show              Show operation information and parameters for
                  this device.
ssid              Delete the SSID or enter the SSID Configuration
                  level context for a specific SSID (i.e. ssid1,
                  ssid2, ssid3,ssid4).
static-channel    Set the channel to be used by this radio when
                  configured for "static" channel policy.
supported-rate    Add/remove a rate to/from the set of supported
                  rates for this radio.
terminal          Set the dimensions of the terminal window.
tx-power-reduction Set the transmit power reduction for this radio.
wlan              Enter the WLAN Config level context for a specific
                  WLAN (e.g. 1, 2, 3, etc.).
write             View or save the running configuration of this device.

ProCurve Acess Point 530(radio1)#
```

After selecting the More option, the remaining commands display.

Figure 3-12. Context-Specific Commands Affecting Radio Context [MORE]

WLAN (BSS/SSID) Context . Includes specific commands that apply only to the WLAN(BSS/SSID) wireless interface. The context changes depending on the radio. If you are in Radio 1, you have access to configure and enable/ disable the WLAN, if you are in Radio 2, you only have access to enable/disable:

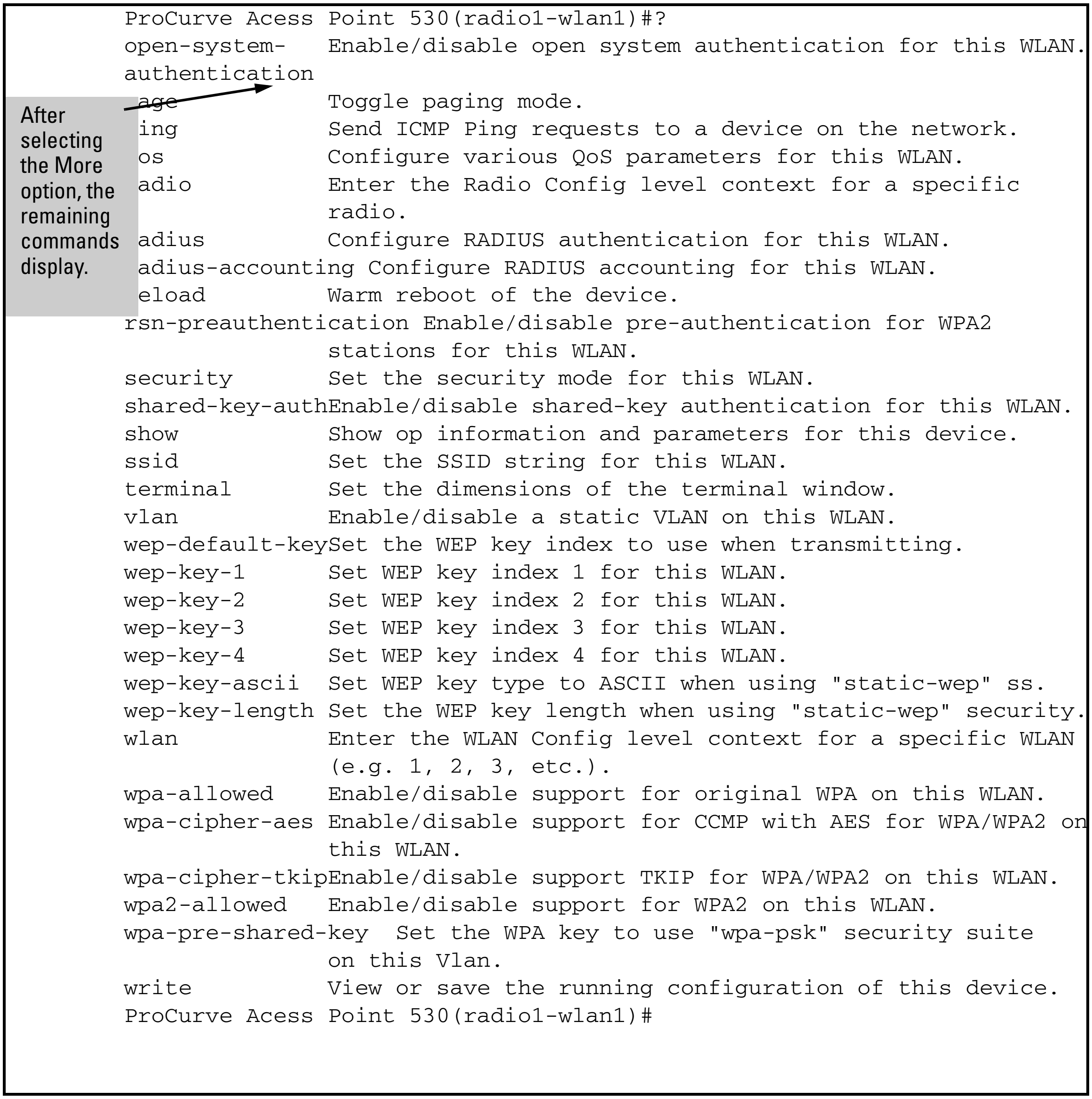
`ProCurve Acess Point 530(config)#radio 1`	Command executed at configuration level to enter radio context.
`ProCurve Acess Point 530(radio1)#wlan 1`	Command executed at wireless context level to enter WLAN(BSS/SSID) wireless context.
`ProCurve Acess Point 530(radio1-wlan1)#`	Resulting prompt showing the WLAN(BSS/ SSID) wireless context.
`ProCurve Acess Point 530(radio1-wlan1)#?`	Lists commands you can use in the WLAN(BSS/SSID) wireless context.



```
ProCurve Acess Point 530(radio1-wlan1)#?
closed-system  Enable/disable closed syst
               for this WLAN.
copy           Copy data and configuratic
description    Set a human-readable text string for this WLAN.
disable        Disable this WLAN.
dtim-period    Set DTIM for this WLAN.
enable         Enable this WLAN.
end            Return to the Manager level context.
exit           Return to the previous context or terminate current
               console/telnet session if in the Manager context level.
interface      Enter the Interface Config level context.
logout         Terminate this session.
mac-auth-local Enable/disable a local MAC auth. access list on this WLAN.
mac-auth-remote Enable/disable a remote MAC auth access list on this WLAN.

-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

In the WLAN (BSS/SSID) context, the commands in the "?" listing show the commands that affect only the WLAN (BSS/SSID) interface.

Figure 3-13. Context-Specific Commands Affecting the WLAN (BSS/SSID) Context



```
ProCurve Acess Point 530(radio1-wlan1)#?
open-system-   Enable/disable open system authentication for this WLAN.
authentication
 age           Toggle paging mode.
 ing           Send ICMP Ping requests to a device on the network.
 os            Configure various QoS parameters for this WLAN.
 adio          Enter the Radio Config level context for a specific
               radio.
 adius         Configure RADIUS authentication for this WLAN.
 adius-accounting Configure RADIUS accounting for this WLAN.
 eload         Warm reboot of the device.
rsn-preauthentication Enable/disable pre-authentication for WPA2
               stations for this WLAN.
security       Set the security mode for this WLAN.
shared-key-authEnable/disable shared-key authentication for this WLAN.
show           Show op information and parameters for this device.
ssid           Set the SSID string for this WLAN.
terminal       Set the dimensions of the terminal window.
vlan           Enable/disable a static VLAN on this WLAN.
wep-default-keySet the WEP key index to use when transmitting.
wep-key-1      Set WEP key index 1 for this WLAN.
wep-key-2      Set WEP key index 2 for this WLAN.
wep-key-3      Set WEP key index 3 for this WLAN.
wep-key-4      Set WEP key index 4 for this WLAN.
wep-key-ascii  Set WEP key type to ASCII when using "static-wep" ss.
wep-key-length Set the WEP key length when using "static-wep" security.
wlan           Enter the WLAN Config level context for a specific WLAN
               (e.g. 1, 2, 3, etc.).
wpa-allowed    Enable/disable support for original WPA on this WLAN.
wpa-cipher-aes Enable/disable support for CCMP with AES for WPA/WPA2 on
               this WLAN.
wpa-cipher-tkipEnable/disable support TKIP for WPA/WPA2 on this WLAN.
wpa2-allowed   Enable/disable support for WPA2 on this WLAN.
wpa-pre-shared-key  Set the WPA key to use "wpa-psk" security suite
               on this Vlan.
write          View or save the running configuration of this device.
ProCurve Acess Point 530(radio1-wlan1)#
```

After selecting the More option, the remaining commands display.

Figure 3-14. Context-Specific Commands Affecting the WLAN (BSS/SSID) Context [MORE]

CLI Control and Editing

Keystrokes	Function
[Ctrl] [A]	Jumps to the first character of the command line.
[Ctrl] [B] or ←	Moves the cursor back (to the left) one character.
[Ctrl] [C]	Terminates a task if one is running and displays the command line.
[Ctrl] [D]	Deletes the character at the cursor.
[Ctrl] [E]	Jumps to the end of the current command line (the character position after the last character in the CLI command input buffer).
[Ctrl] [F] or →	Moves the cursor forward (to the right) one character if the cursor is not at the end of the current command line.
[Ctrl] [H]	Deletes the first character to the left of the command line.
[Ctrl] [K]	Deletes from the cursor to the end of the command line.
[Ctrl] [L] or **[Ctrl] [R]**	Repeats current command line on a new line.
[Ctrl] [N] or ↓	Enters the next command line in the history buffer.
[Ctrl] [P] or ↑	Enters the previous command line in the history buffer.
[Ctrl] [R]	Repeats current command line on a new line.
[Ctrl] [U] or **[Ctrl] [X]**	Deletes from the cursor to the beginning of the command line.
[Ctrl] [W]	Deletes the last word typed.
[Ctrl] [Y]	Recalls the most recent entry in the delete buffer.
[Ctrl] [Z]	This character closes the current session, returning the operator to the previous context (config).
[Esc] [B]	Moves the cursor backward (to the left) one word.
[Esc] [D]	Deletes from the cursor to the end of the word.
[Esc] [F]	Moves the cursor forward (to the right) one word.
[Ctrl] [H], [Delete], or [Backspace]	Deletes the first character to the left of the command line.
Tab or "?"	Completes the current word of a command.

— This page is intentionally unused. —

4

Using the ProCurve Web Browser Interface

Contents

Overview

The Access Point 530 Web browser interface lets you easily access the access point from a browser-based PC on your network.

This chapter covers the following:

- Starting a Web browser interface session
- Description of the Web browser interface screen
- Tasks for your first Web browser interface session
- Overview of the Web interface windows
  - Device Information- screens detail reporting statistics
  - Network Setup - screens for IP, VLAN, WLAN (BSS/SSID), and Radio configuration
  - Management - screens for maintaining config and upgrade files, enabling access and password security, and configuring SNMP parameters
  - Special Features - screens for configuring QoS, WDS, Local RADIUS, AP Detection, and Time
  - Troubleshooting - screen for customer support details.

Starting a Web Browser Interface Session with the Access Point

You can start a Web browser session using a standalone Web browser on a network connection from a PC in the following ways:

- Directly connected to your network
- Connected through remote access to your network

This procedure assumes that you have a supported Web browser installed on your PC or workstation, and that an IP address has been configured on the access point. If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **AP530**) that you can type in the **Location or Address** field instead of the IP address. Using DNS names typically improves browser performance. See your network administrator for any name associated with the access point. (For more information on assigning an IP address, refer to "Configuring IP Parameters" on page 4-15.'

The operating and Web systems support recommended to manage the access point through the browser interface are as follows:

- Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000
- Netscape Mozilla 1.7.x on Redhat Linux version 2.4
- Mozilla/5.0 (Windows; U; Windows NT 5.1; rv:1.7.3) Gecko/20041001 Firefox/0.10.1

The administration Web browser must have JavaScript enabled to support the interactive features of the administration interface. It must also support HTTP uploads to use the software upgrade feature.

Note

Access point management can be limited to access from the Ethernet interface. For more on this feature, see "Setting Up Filter Control" on page 5-46.

Type the IP address (or DNS name) of the access point in the browser **Location or Address** field and press **[Enter]**. (It is not necessary to include **http://**.)

10.11.12.195 [Enter]	*Example of an IP address.*
AP530 [Enter]	*Example of a DNS-type name.*

Alternatively, the access point also supports a secure Web (HTTPS) browser connection. In this case, type **https://** followed by the IP address (or DNS name) in the browser **Location** or **Address** field and press **[Enter].**

https://10.11.12.195 [Enter]	*Example of an IP address.*
https://AP530 [Enter]	*Example of a DNS-type name.*

Note

To ensure proper screen refresh when using Internet Explorer with Windows XP, be sure that the browser options are configured as follows: Under the menu "Tools / Internet Options / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be set to "Automatically."

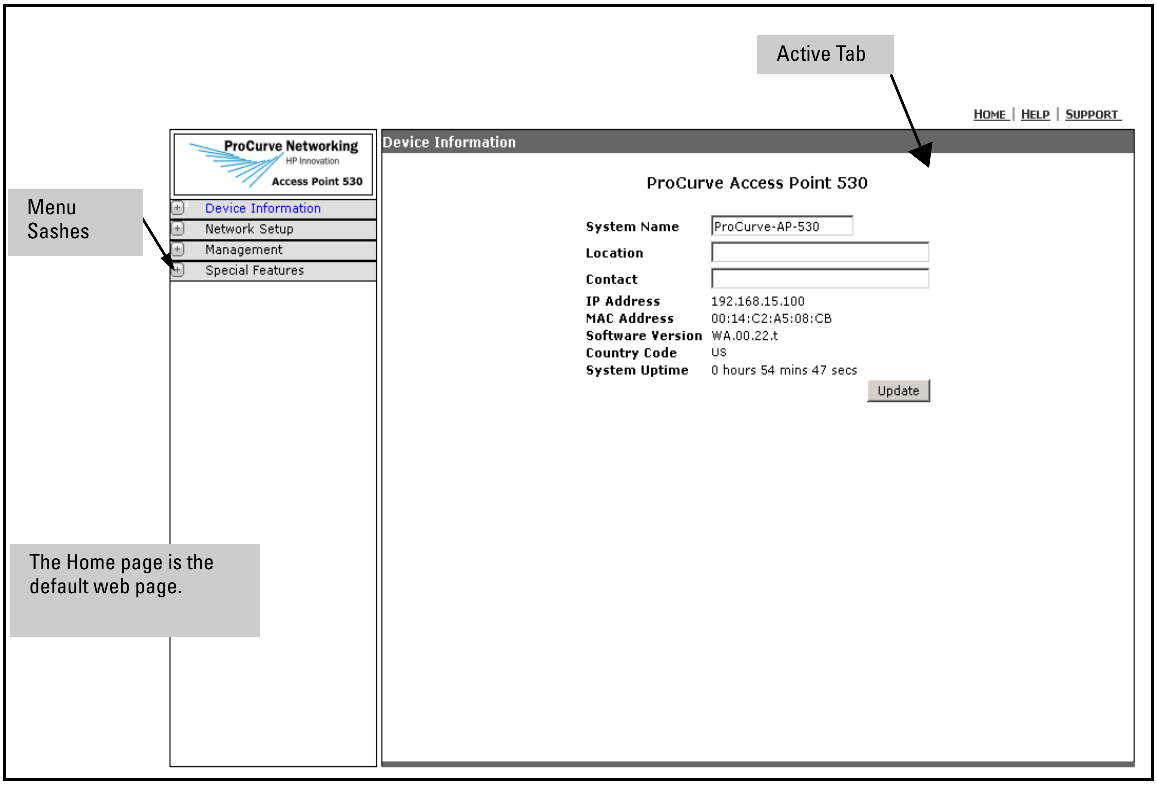
Description of Browser Interface

Browser elements covered in this section include:

- The Home Page
- The Support Page
- The Help button
- The Logout button

The Home Page

The home page is the entry point for the Web browser interface. The following figure identifies the various parts of the screen.



Active Tab

Menu Sashes

The Home page is the default web page.

ProCurve Access Point 530

System Name ProCurve-AP-530
Location
Contact
IP Address 192.168.15.100
MAC Address 00:14:C2:A5:08:CB
Software Version WA.00.22.t
Country Code US
System Uptime 0 hours 54 mins 47 secs

Figure 4-1. The Home Page

Support Page

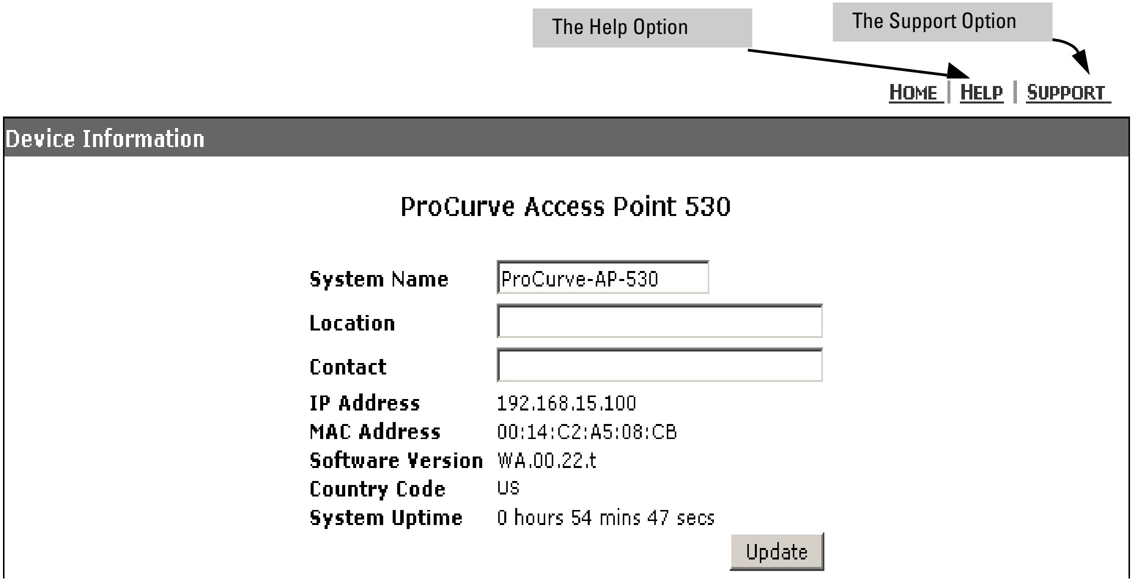
The support page for the access point's Web browser interface is accessed through the **Support** option in the upper-right corner of any of the Web browser interface screens. You can also access support using the **Technical Support** option through the left-menu bar:

http://www.procurve.com

The support page provides key information regarding your access point, including white papers, software updates, and more.

Online Help for the ProCurve Web Browser Interface

Online Help is available for the Web browser interface. The help is context sensitive and maps topics to the Web page you have accessed.


The Help Option

The Support Option

Device Information

ProCurve Access Point 530

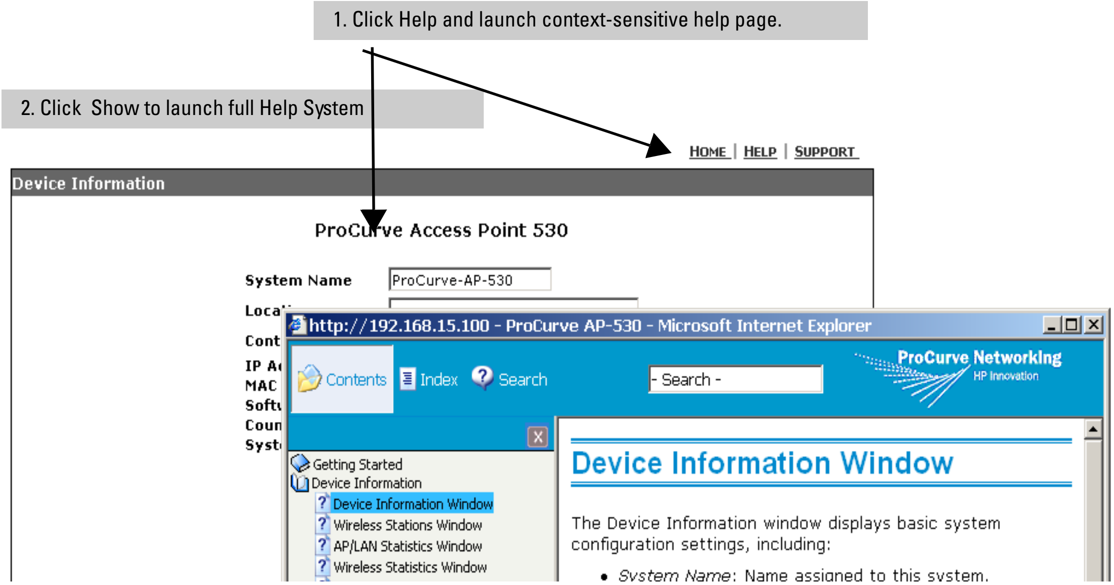
System Name	ProCurve-AP-530
Location	
Contact	
IP Address	192.168.15.100
MAC Address	00:14:C2:A5:08:CB
Software Version	WA.00.22.t
Country Code	US
System Uptime	0 hours 54 mins 47 secs

Figure 4-2. The Help and Support Options

Using the Help in the Browser Interface

You can use it by clicking on the Help option in the upper-right corner of any of the Web browser interface screens.

Once the help page launches, details related to the Web page you have accessed are displayed.



1. Click Help and launch context-sensitive help page.

2. Click Show to launch full Help System

ProCurve Access Point 530

System Name ProCurve-AP-530

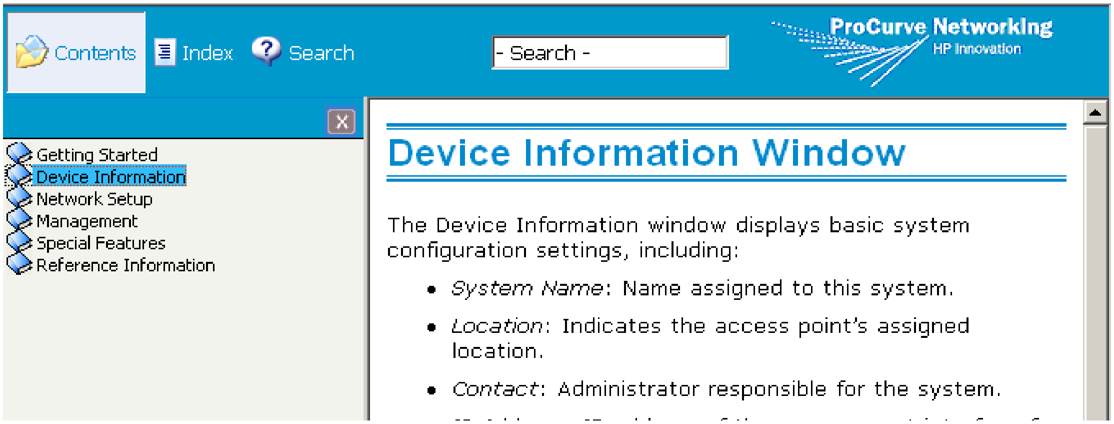
Loca
Cont
IP A
MAC
Softw
Coun
Syst

Device Information Window

The Device Information window displays basic system configuration settings, including:

- *System Name*: Name assigned to this system.

Any easy Topic and Menu bar display for easy access to information. Options include, Contents, Index, and Search.



Device Information Window

The Device Information window displays basic system configuration settings, including:

- *System Name*: Name assigned to this system.
- *Location*: Indicates the access point's assigned location.
- *Contact*: Administrator responsible for the system.

Tasks for Your First ProCurve Web Browser Interface Session

The first time you access the Web browser interface, there are a number of basic tasks that you should perform:

- Set passwords
- Set the SNMP community names
- Set the primary Service Set Identifier (SSID)
- Enable radio communications and select a channel
- Change TCP/IP settings
- Set radio security options

Changing the Password in the Browser Interface

You may want to change the password to enhance access security for the management interface on your access point. The password allows read and write access to the Web browser interface.

Note

If you want security beyond that achieved with user names and passwords, you can disable access to the Web browser interface. This is done by executing the Management Configuration level command prompt in the CLI. Then, management access is only from the CLI, console port, Telnet. or SSH.

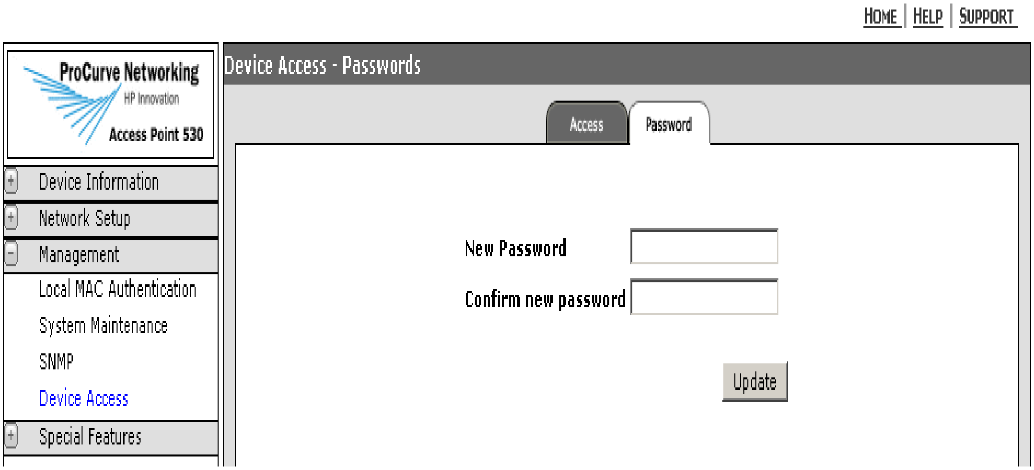


Figure 4-3. Setting a Password

To Set a Password:

1. Select Management > Device Access > Passwords tab.
2. In the New Password text field, enter a **new password**.

   Note: The password is case sensitive and must be at least 1 character and at most 32 characters long. However, only the first 8 characters of the password are used; character number 9 and above are ignored at log in.
3. In the Confirm Password text field, re-enter the **new password**.
4. Click **[Update]** to activate the new password.

Note

The password you assign in the Web browser interface will overwrite the previous settings assigned in either the Web browser interface or the access point console. That is, the most recently assigned user password is immediately effective for the access point, regardless of which interface was used to assign these parameters.

The Manager user name and password are used to control access to the CLI and Web browser management interfaces for the access point. Once set, you will be prompted to supply the user name and password every time you try to access the access point through these interfaces.

If You Lose the Password

If you lose the password, you can reset it by pressing the Clear button on the back of the access point for more than one second. This action resets the password to the factory default settings for all of the access point's interfaces. For details on resetting configuration files, see "File Uploads, Downloads, and Resets" on page A-1.

Reboot and Reset Options

You can also use the Web interface to:

- Reset the configuration file back to the factory default. Select Management > System Management > Configuration File > Reset Configuration area, select the Reset to Factory Default [Reset] option.
- Reboot the AP. Select Management > System Management > Configuration Files > Reboot tab, select the Reboot the Access Point [Reboot] option.

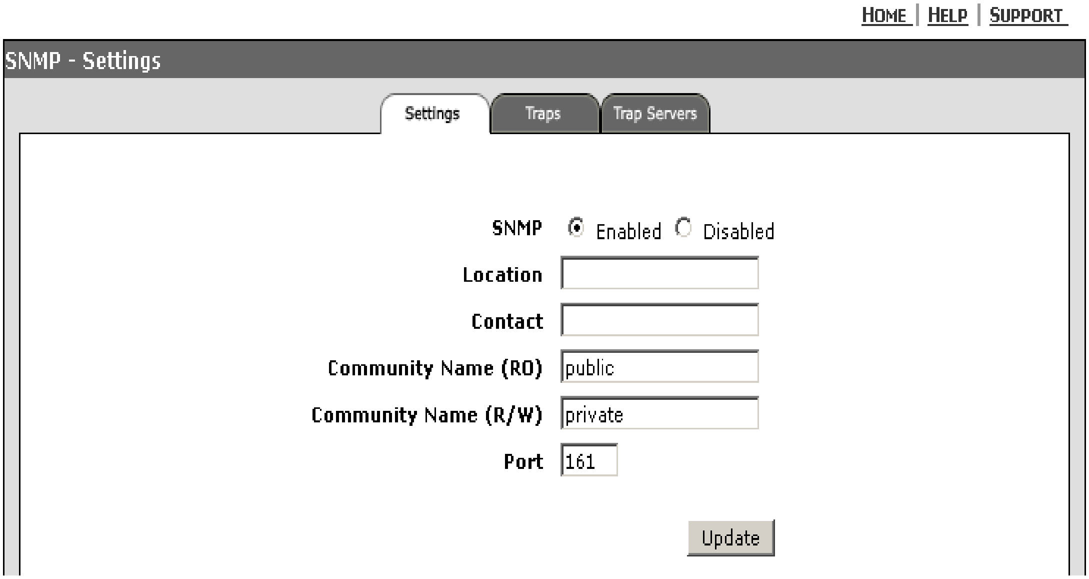
NOTE

For details on manual reset of the access point, reference the *Installation and Configuration Guide* and see "File Uploads, Downloads, and Resets" on page A-1.

Setting SNMP Community Names

You can manage the access point from a network management station running a Simple Network Management Protocol (SNMP) management application such as ProCurve Manager.

The access point SNMP agent supports SNMP versions 1 and 2c. Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with the access point, an SNMP v1 or v2c management station must first submit a valid community name for authentication. The default community names are "public" for read-only access and "private" for read/write access. If you intend to support SNMP v1 or v2c managers, it is recommended that you change the default community names to prevent unauthorized access. For SNMP parameter details, see "Web: Setting Basic SNMP Parameters" on page 5-23.



SNMP ● Enabled ○ Disabled

Location	
Contact	
Community Name (RO)	public
Community Name (R/W)	private
Port	161

Figure 4-4. Setting SNMP Community Names

To Change A Default SNMP Community Name:

1. Select Management > SNMP > Settings tab.
2. To activate the SNMP feature on the access point, select **Enabled.**
3. To establish a public read-only SNMP community, type a **name** text string to replace the default community name (public) in the Community Name (RO) text field.
4. To establish a private read-write SNMP community, type a **name** text string to replace the default community name (private) in the Community Name (R/W) text field.
5. Click **[Update]** to activate the new SNMP community name.

Setting the Radio Mode and Channel

The access point's radio channel settings are limited by local regulations, which determine the number of channels that are available. You can manually set the access point's radio channel or allow it to automatically select an unoccupied channel.

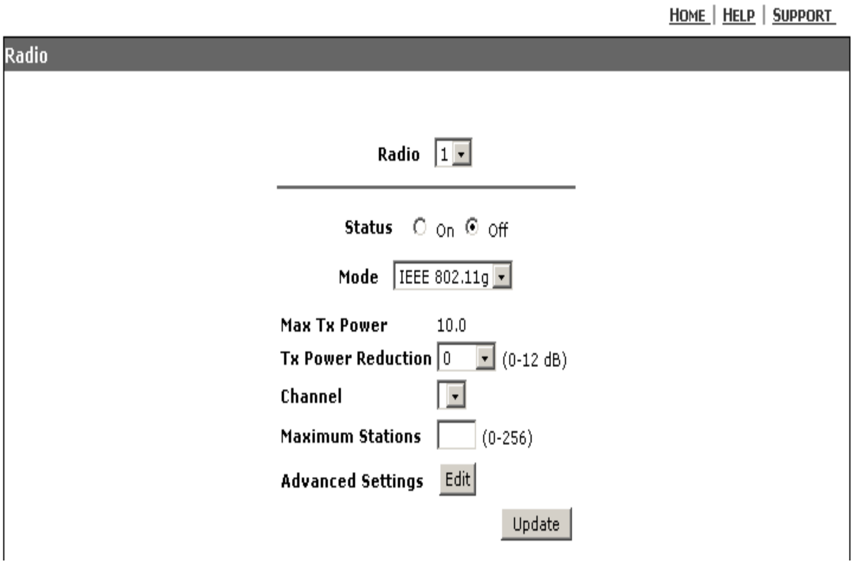
Note

Radio 1 operates in 802.11b/g mode, but Radio 2 operates in either 802.11b/g or 802.11a modes. If radio 2 is to be configured in 802.11b or 802.11g mode, it must be connected to an external antenna to ensure adequate separation between the two radios operating in the same frequency. See "Radio Configuration Summary Table" on page 6-5.

Note

If using the worldwide product, before configuring radio settings on the access point, you must first use the CLI to set the Country Code so that the radio channels used conform to your local regulations. It is your responsibility to select a correct country setting, otherwise radio operation may fail to comply with legal requirements for use of the access point in your country. See "Setting the Country Code" on page 6-3.

Adjacent access points operating in the same band should be configured to use non-overlapping channels. See "Radio Configuration Summary Table" on page 6-5 and "Web: Configuring Basic Radio Settings" on page 6-11.



Radio 1

Status ○ On ● Off

Mode IEEE 802.11g

Max Tx Power 10.0

Tx Power Reduction 0 (0-12 dB)

Channel

Maximum Stations (0-256)

Advanced Settings Edit

Figure 4-5. Setting Radio Mode and Channel

To Set Radio Mode and Channel:

Note

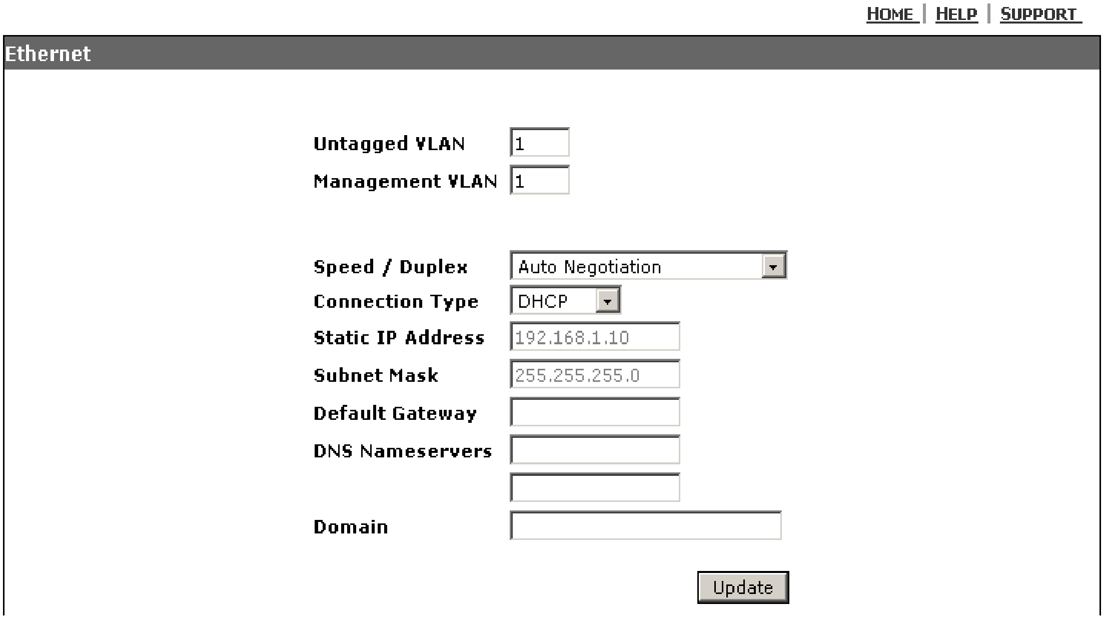
The Web Radio page is not available for configuration until the Country Code is set using the CLI.

1. Select Network Setup > Radio.
2. To enable the radio parameters, select **On** for the Status option.
3. Select the **Mode** (default is IEEE 802.11g).
4. Select the **Channel** (auto is the default).
5. Click **[Update]** to save the settings.

Configuring TCP/IP Settings

You can use the Web browser interface to manage the access point only if it already has an IP address that is reachable through your network. You can set an initial IP address for the access point by using the CLI interface.

After you have network access to the access point, you can then use the Web browser interface to modify the initial IP configuration. For IP parameter details, see "Web: Configuring IP Settings Statically or via DHCP" on page 5-18..



Untagged VLAN	1
Management VLAN	1
Speed / Duplex	Auto Negotiation
Connection Type	DHCP
Static IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	
DNS Nameservers	
Domain	

Figure 4-6. Configuring IP Parameters

To Set IP Parameters i:

1. Select Network Setup > Ethernet.
2. To set a dynamic connection, select **DHCP** in the Connection Type drop-down.
3. To set a manual connection, select **Static IP** in the Connection Type drop-down.
4. If you chose Static IP, enter the I**P address** and the **subnet mask** in the Static IP Address and Subnet Mask text fields. The defaults automatically populate.
5. If a management station exists on another network segment, enter the **IP address of a gateway** that can route traffic between these segments.
6. To set dynamic DNS nameservers, select **Dynamic.** To set the nameservers manually, select **Manual**.
7. If you chose to manually enter the DNS nameservers, enter the **IP address** for the primary and secondary DNS servers to be used for host-name to IP address resolution.
8. Click **[Update]** to save these IP settings.

Note

If you change the IP address using the Web interface, you must log in again using the new address.

Configuring Security Settings

Wireless stations can read the SSIDs from the access point's beacon frame. If the "closed system" option is selected when configuring the access point, the SSID is not broadcast in the beacon frame. For more secure data transmissions, the access point provides client authentication and data encryption based on shared keys that are distributed to all stations.

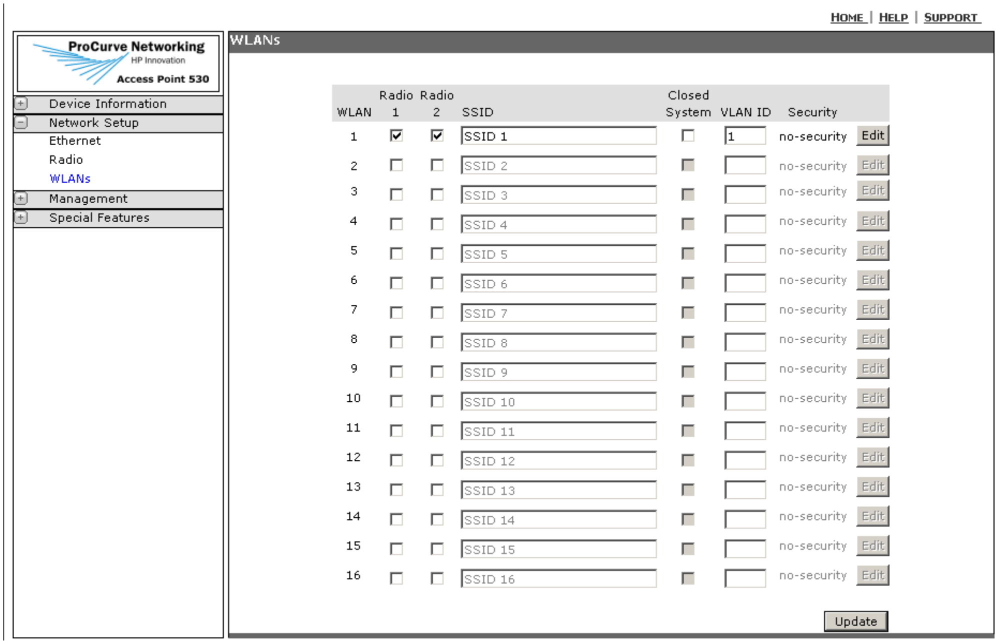
Wired Equivalent Privacy (WEP) is implemented to provide a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless stations and the access point.

The access point allows configuration of up to 16 SSIDs . The Web interface provides easy windows to configure SSID parameters, including: enabling, SSID names, closed system, VLAN IDs, and security settings. For Security parameter details, see "Web: Setting Security Options" on page 7-14.

NOTE

Configuring WLAN security establishes WDS Link Security. For a summary of the configuration relationship, see "Web: Setting Security Options" on page 7-14.

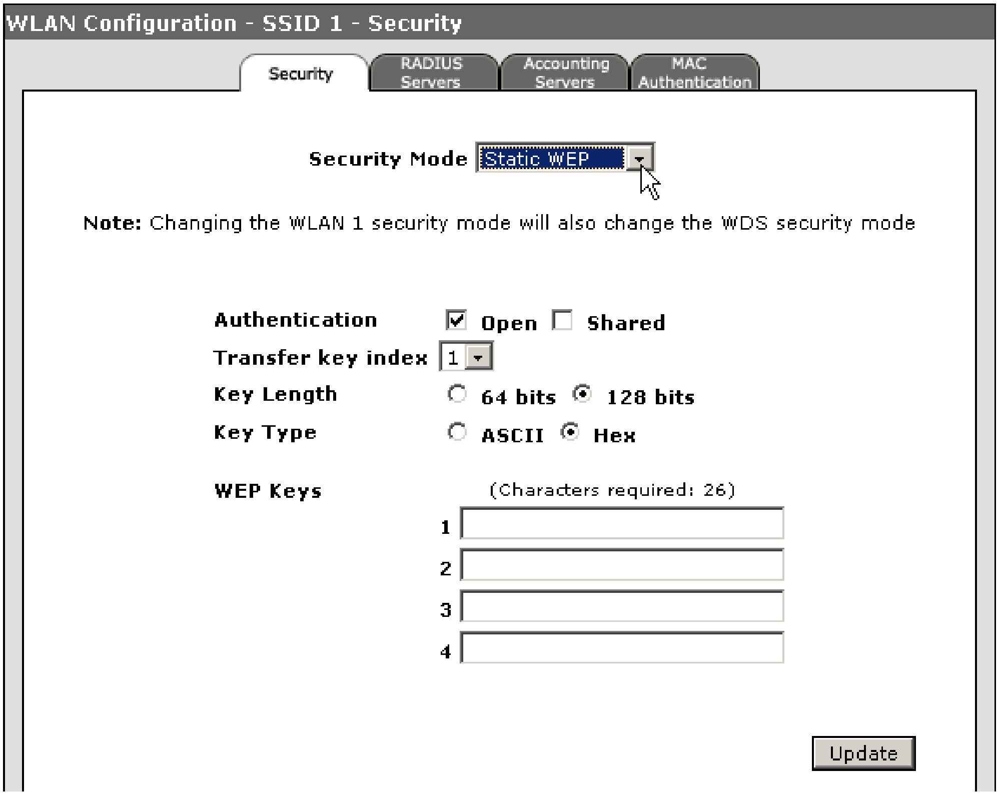
.



WLANs

WLAN	Radio 1	Radio 2	SSID	Closed System	VLAN ID	Security	
1	☑	☑	SSID 1	□	1	no-security	Edit
2	□	□	SSID 2	□		no-security	Edit
3	□	□	SSID 3	□		no-security	Edit
4	□	□	SSID 4	□		no-security	Edit
5	□	□	SSID 5	□		no-security	Edit
6	□	□	SSID 6	□		no-security	Edit
7	□	□	SSID 7	□		no-security	Edit
8	□	□	SSID 8	□		no-security	Edit
9	□	□	SSID 9	□		no-security	Edit
10	□	□	SSID 10	□		no-security	Edit
11	□	□	SSID 11	□		no-security	Edit
12	□	□	SSID 12	□		no-security	Edit
13	□	□	SSID 13	□		no-security	Edit
14	□	□	SSID 14	□		no-security	Edit
15	□	□	SSID 15	□		no-security	Edit
16	□	□	SSID 16	□		no-security	Edit

Figure 4-7. The WLANs Window



WLAN Configuration - SSID 1 - Security

Security Mode: Static WEP

Note: Changing the WLAN 1 security mode will also change the WDS security mode

Authentication: ☑ Open ☐ Shared
Transfer key index: 1
Key Length: ○ 64 bits ● 128 bits
Key Type: ○ ASCII ● Hex

WEP Keys (Characters required: 26)
1
2
3
4

Figure 4-8. Configuring WLAN Security

To Configure WEP Security:

1. Select Network Setup > WLANs.
2. Check the **Radio 1** option and the SSID name and VLAN ID fields populate with defaults.
3. Enter a **unique SSID name** in the SSID name text field and check the **Closed System** option to prevent broadcasting of the SSID.
4. Select [**Edit**] button to launch the Security window.
5. Select **Static WEP** in the Security Mode drop-down.
6. Check **Shared Key** for the Authentication option.
7. Select **1 key** in the Transfer Key Index drop-down to be used for the SSID interface.

8. Select the key length to be used by all stations either **64** or **128** (default) bits.

9. Select the Key Type, **Hex** (default) or **Ascii**.

10. Enter one **WEP key** conforming to the length and type already selected. You can enter up to 4 wep keys at a time.

11. Click **[Update]** to save these IP settings.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. While WEP provides a margin of security for environments with light network traffic, it is not sufficient for enterprise use where highly-sensitive data is transmitted.

For more robust wireless security, you should consider implementing other features supported by the access point. Wi-Fi Protected Access (WPA) and IEEE 802.1X-2004 (Port-based network access control using the physical access characteristics of IEEE 802® Local Area Networks (LAN) infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics) provide improved data encryption and user authentication. See "Wireless Security Configuration" on page 7-1.

Overview of the Web Interface

The Web interface provides logical window groups for easy access to common management, reporting, and configuration features. This section details each of the logical window groups, sub-tabs. and screen elements and parameters. Cross-references are provided to any configuration procedures.

The Web interface provides the following logical groups:

- Device Information
- Network Setup
- Management
- Special Features

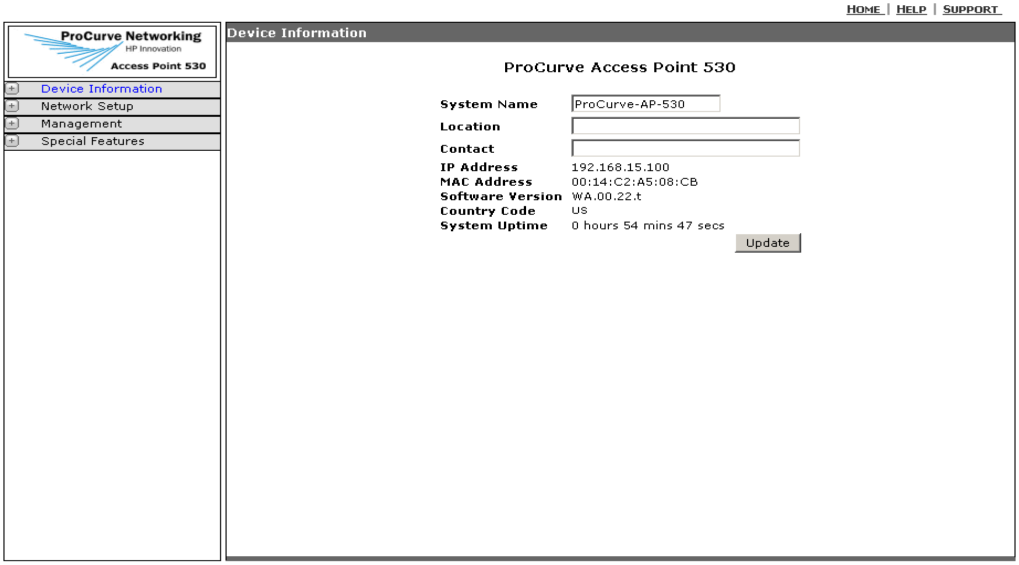
Device Information

The Device Information sash is the first logical group available on the Web-interface menu. Once accessed, it defaults to the Device Information window, also considered the Access Point 530 Home Page. This group provides access to the following windows:

- Device Information (Access Point 530 Home Page)
- Wireless Stations
- AP/LAN Statistics
- Wireless Statistics
- Event log

The Device Information Window

Accessed through the Device Information sash, the Device Information window displays basic system configuration settings.



System Name: ProCurve-AP-530
Location:
Contact:
IP Address: 192.168.15.100
MAC Address: 00:14:C2:A5:08:CB
Software Version: WA.00.22.t
Country Code: US
System Uptime: 0 hours 54 mins 47 secs

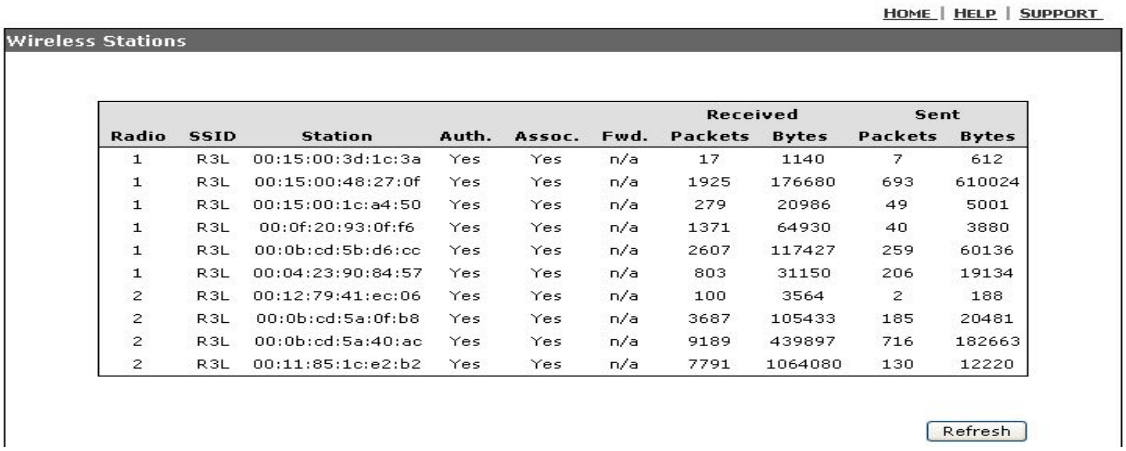
Figure 4-9. Device Information Window

Device Information. The Device Information window displays the basic system configuration settings:

- **System Name**: Name assigned to this system. Modifiable text field.
- **Location**: Indicates the access point's assigned location. Modifiable text field. Max length of 255 characters.
- **Contact**: Administrator responsible for the system. Modifiable text field. Max length of 255 characters.
- **IP Address**: IP address of the management interface for this device.
- **MAC Address**: The physical layer address for the Ethernet port interface.
- **Software Version**: Shows the version number for the runtime software.
- **Country Code**: Indicates the access point's current Country Code setting.
- **System Up Time**: Length of time the access point has been up (hours, minutes, seconds).
- **[Update]**: Updates the access point with the modifiable parameters.

The Wireless Stations Window

Accessed through the Wireless Stations option on the Device Information sash, the Wireless Stations window displays radio and network station status details.



						Received		Sent	
Radio	SSID	Station	Auth.	Assoc.	Fwd.	Packets	Bytes	Packets	Bytes
1	R3L	00:15:00:3d:1c:3a	Yes	Yes	n/a	17	1140	7	612
1	R3L	00:15:00:48:27:0f	Yes	Yes	n/a	1925	176680	693	610024
1	R3L	00:15:00:1c:a4:50	Yes	Yes	n/a	279	20986	49	5001
1	R3L	00:0f:20:93:0f:f6	Yes	Yes	n/a	1371	64930	40	3880
1	R3L	00:0b:cd:5b:d6:cc	Yes	Yes	n/a	2607	117427	259	60136
1	R3L	00:04:23:90:84:57	Yes	Yes	n/a	803	31150	206	19134
2	R3L	00:12:79:41:ec:06	Yes	Yes	n/a	100	3564	2	188
2	R3L	00:0b:cd:5a:0f:b8	Yes	Yes	n/a	3687	105433	185	20481
2	R3L	00:0b:cd:5a:40:ac	Yes	Yes	n/a	9189	439897	716	182663
2	R3L	00:11:85:1c:e2:b2	Yes	Yes	n/a	7791	1064080	130	12220

Figure 4-10. Wireless Stations Window

Wireless Stations. The Wireless Stations window displays client stations associated with a particular access point. The associated stations are displayed along with information about packet traffic transmitted and received for each station.

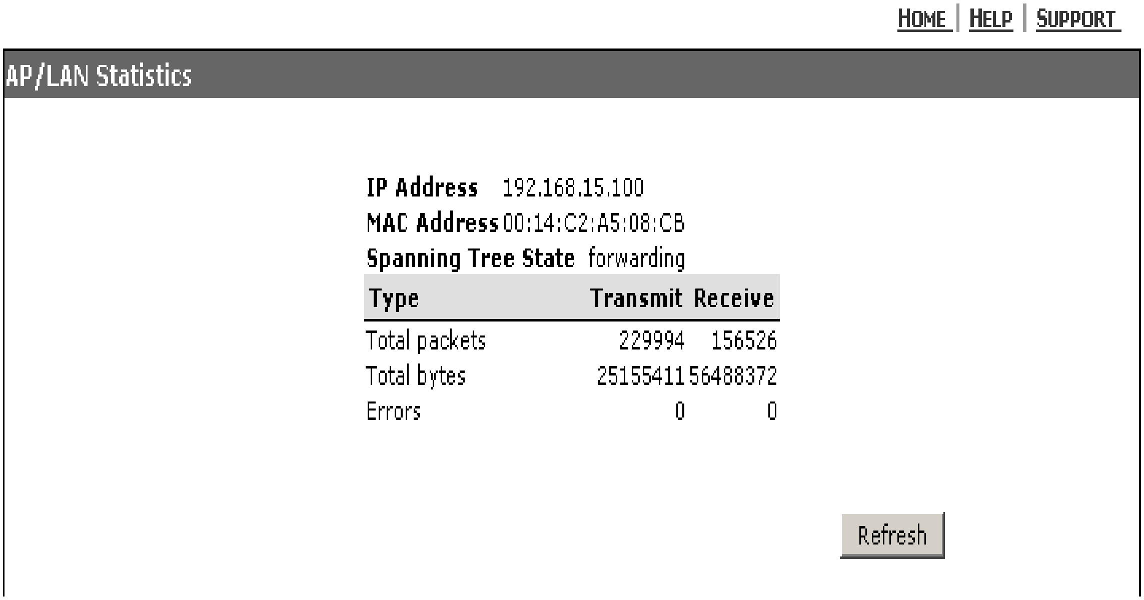
- **Radio:** Indicates the access point radio.
- **SSID:** Indicates the Service Set Identifier (SSID) of the WLAN to which the access point is connected.
- **Station**: The MAC address of the wireless client.
- **Auth.:** Shows if the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are "open system" and "shared key." Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to stations before attempting authentication.
- **Assoc.:** Shows if the station has been successfully associated with the access point. Once authentication is completed, stations can associate with the current access point, or reassociate with a new access point.

The association procedure allows the wireless system to track the location of each mobile client, and ensures that frames destined for each client are forwarded to the appropriate access point.

- **Fwd:** If 802.1X is used, this parameter indicates the station passed 802.1X authentication and traffic can be forwarded to the access point. It also indicates whether a wireless station has the correct WPA pre-shared key when the access point is using "wpa-psk" security on the WLAN. If the WLAN is set to “static-wep” or “no-security”, this parameter displays “n/a” as it does not apply.
- **Received Packets:** Indicates total packets received by this access point.
- **Received Bytes:** Indicates total bytes received by this access point.
- **Sent Packets:** Indicates total packets sent by this access point.
- **Sent Bytes:** Indicates total bytes sent by this access point.
- **[Refresh]:** Refreshes the Wireless station results.

The AP/LAN Statistics Window

Accessed through the AP/LAN Statistics option on the Device Information sash, the AP/LAN Statistics window displays transmit/receive details.



IP Address 192.168.15.100
MAC Address 00:14:C2:A5:08:CB
Spanning Tree State forwarding

Type	Transmit	Receive
Total packets	229994	156526
Total bytes	25155411	56488372
Errors	0	0

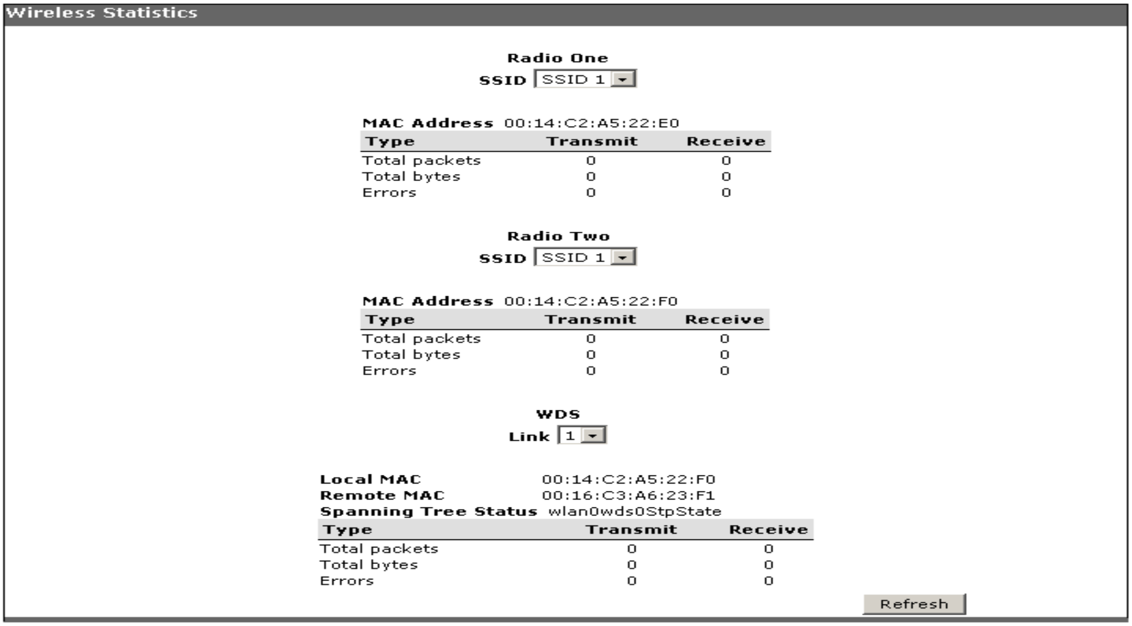
Figure 4-11. The AP/LAN Statistics Window

The AP/LAN Statistics window displays the following information:

- **IP Address**: IP address of the management interface for this device.
- **MAC Address**: The physical layer address for the Ethernet port interface.
- **Spanning Tree State:** Indicates the spanning tree state if used. Possible states include: disabled, listening, learning, forwarding, or blocking.
- **Transmit Total Packets:** Indicates total packets transmitted by this access point.
- **Receive Total Packets:** Indicates total packets received by this access point.
- **Transmit Total Bytes:** Indicates total bytes sent by this access point.
- **Receive Total Bytes:** Indicates total bytes received by this access point.
- **Transmit Errors:** Indicates the number of transmission errors.
- **Receive Errors:** Indicates the number of packet errors received.
- **[Refresh]:** Refreshes the AP/LAN statistics results.

The Wireless Statistics Window

Accessed through the Wireless Statistics option on the Device Information sash, the Wireless Statistics window displays transmit/receive details.



Wireless Statistics

Radio One

SSID SSID 1

MAC Address 00:14:C2:A5:22:E0

Type	Transmit	Receive
Total packets	0	0
Total bytes	0	0
Errors	0	0

Radio Two

SSID SSID 1

MAC Address 00:14:C2:A5:22:F0

Type	Transmit	Receive
Total packets	0	0
Total bytes	0	0
Errors	0	0

WDS

Link 1

Local MAC 00:14:C2:A5:22:F0
Remote MAC 00:16:C3:A6:23:F1
Spanning Tree Status wlan0wds0StpState

Type	Transmit	Receive
Total packets	0	0
Total bytes	0	0
Errors	0	0

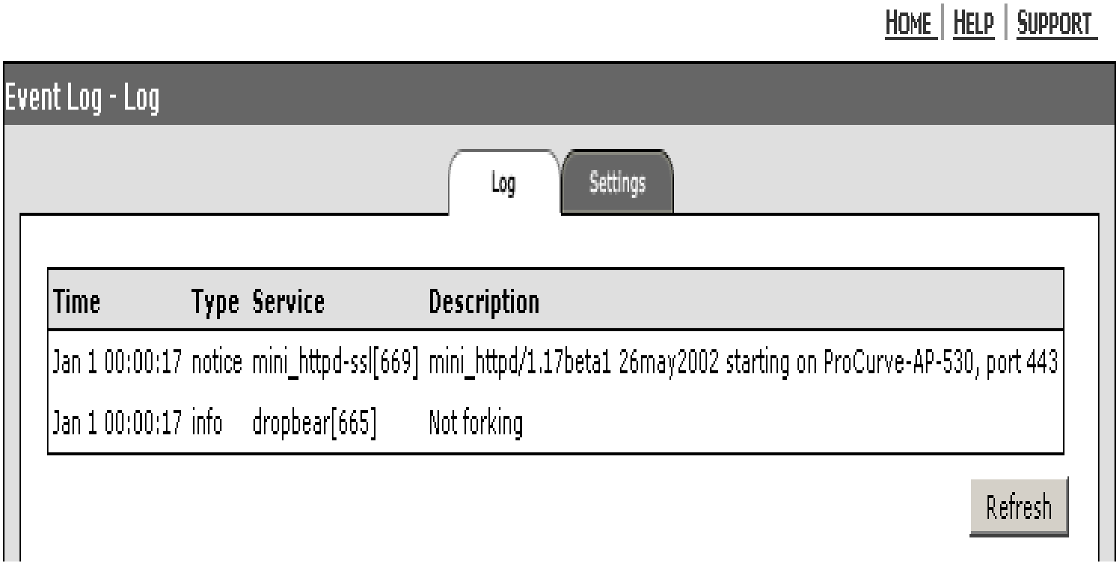
Figure 4-12. The Wireless Statistics Window

The Wireless Statistics window displays dual radio information:

- **Radio/SSID | WDS/LINK**
  - RADIO/SSID: Indicates either Radio 1 or Radio 2 with the Service Set Identifier (SSID) for the access point.
  - WDS LINK: Indicates the configured WDS link for the access point.
- **MAC Address**: Indicates the physical layer address for the Ethernet port interface.
- **Remote MAC Address:** Indicates the remote MAC address.
- **Spanning Tree Status:** Indicates the spanning tree status if used.
- **Transmit Total Packets:** Indicates total packets transmitted by this access point.
- **Receive Total Packets:** Indicates total packets received by this access point.
- **Transmit Total Bytes:** Indicates total bytes sent by this access point.
- **Receive Total Bytes:** Indicates total bytes received by this access point.
- **Transmit Errors:** Indicates total errors related to sending data.
- **Receive Errors:** Indicates total errors related to receiving data
- **[Refresh]:** Refreshes the Wireless statistics results.

Event Log

Accessed through the Event Log option on the Device Information sash, the Event Log tab displays the log messages generated by the access point and stored in memory.

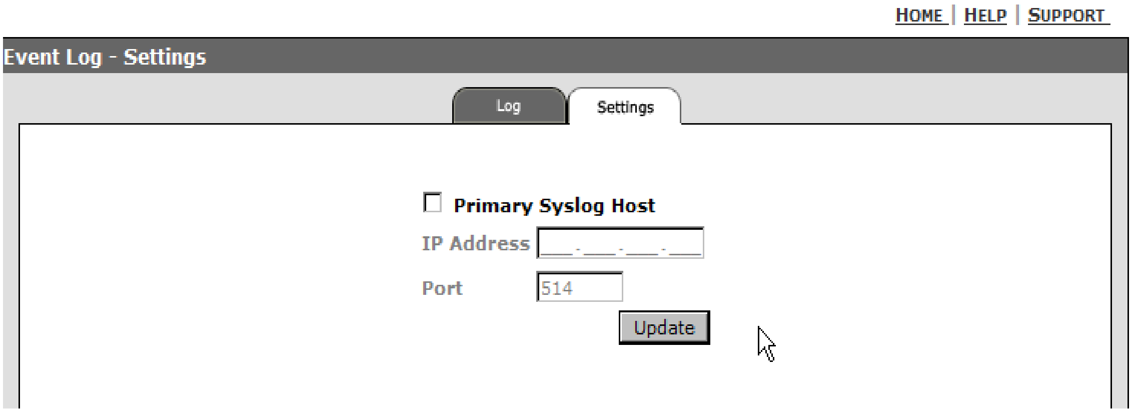


Time	Type	Service	Description
Jan 1 00:00:17	notice	mini_httpd-ssl[669]	mini_httpd/1.17beta1 26may2002 starting on ProCurve-AP-530, port 443
Jan 1 00:00:17	info	dropbear[665]	Not forking

Figure 4-13. The Event Log Tab

The Event Log tab displays the following information:

- **Time:** Indicates the time the log message was generated.
- **Type:** Indicates the logging (type) level associated with this message.
- **Service:** Indicates the service (type) associated with this message.
- **Description:** Indicates the content of the log message.
- **[Refresh]:** Refreshes the Event log results.



☐ Primary Syslog Host
IP Address ___.___.___.___
Port 514

Figure 4-14. The Event Log Settings Tab

The Event Log Settings tab allows the following configuration:

- **Primary Syslog Host:** Enables/disables the primary syslog host.
- **IP Address:** Allows entry of the syslog IP address.
- **Port:** Indicates the port number for the syslog host. (Default is 514)
- **[Update]**: Updates the modifiable parameters.

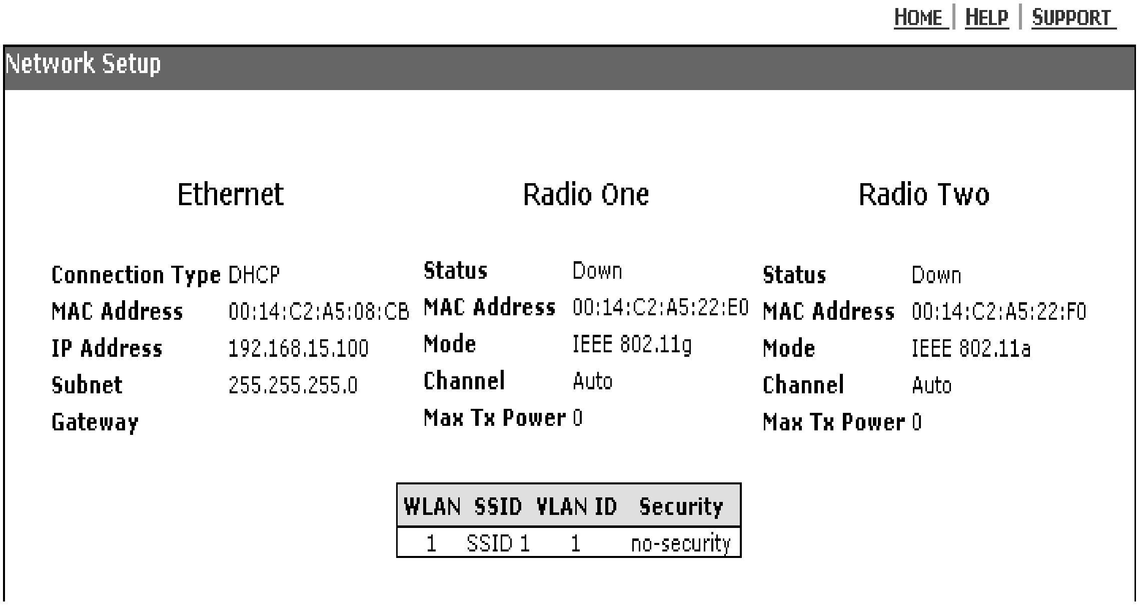
Network Setup

The Network Setup sash is the second logical group available on the Web-interface menu. Once accessed, it defaults to the Network Setup window. This group provides access to the following windows:

- Network Setup
- Ethernet
- Radio
- WLANs

The Network Setup Window

Accessed through the Network Setup sash, the Network Setup window displays the Ethernet and radio features within the network setup group.



Network Setup

Ethernet

Connection Type	DHCP
MAC Address	00:14:C2:A5:08:CB
IP Address	192.168.15.100
Subnet	255.255.255.0
Gateway	

Radio One

Status	Down
MAC Address	00:14:C2:A5:22:E0
Mode	IEEE 802.11g
Channel	Auto
Max Tx Power	0

Radio Two

Status	Down
MAC Address	00:14:C2:A5:22:F0
Mode	IEEE 802.11a
Channel	Auto
Max Tx Power	0

WLAN	SSID	VLAN ID	Security
1	SSID 1	1	no-security

Figure 4-15. The Network Setup Window

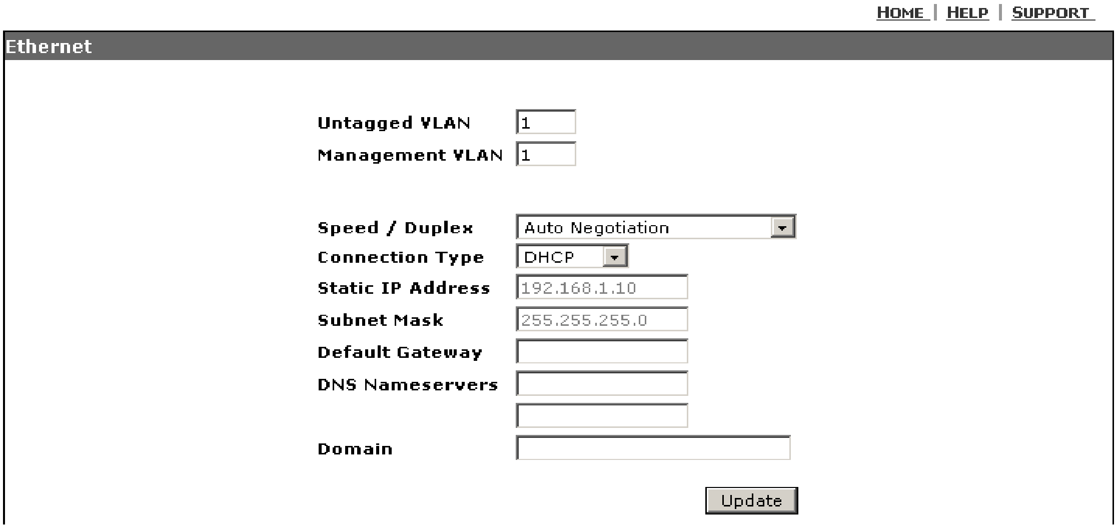
The Network Setup window summarizes:

- **Ethernet:** details basic Ethernet parameters.
  - **Connection Type:** Indicates the type of connection.
  - **MAC Address**: The physical layer address for the Ethernet port interface.
  - **IP Address**: IP address of this device.

  - **Subnet:** Subnet mask of this device.
  - **Gateway:** Gateway address of this device.
- **Radio One:** details basic Radio One parameters.
  - **Status:** Indicates if the radio is up or down.
  - **MAC Address**: The physical layer address.
  - **Mode:** Displays the radio mode for Radio One (IEEE 802.11b or IEEE 802.11g).
  - **Channel:** Displays the channel on which the access point is currently broadcasting.
  - **Max Tx Power:** Displays the maximum radio power level for the selected mode in dBm.
- **Radio Two:** details basic Radio Two parameters.
  - **Status:** Indicates if the radio is up or down.
  - **MAC Address**: The physical layer address.
  - **Mode:** Displays the radio mode for Radio Two (IEEE 802.11a, IEEE 802.11b, or IEEE 802.11g).
  - **Channel:** Displays the channel on which the access point is currently broadcasting.
  - **Max Tx Power:** Displays the maximum radio power level for the selected mode in dBm.
- **WLAN/SSID/VLAN ID/Security:** details basic WLAN parameters.
  - **WLAN:** Indicates the WLAN identifier for the access point. There can be up to 16 WLANs.
  - **SSID:** Indicates the Service Set Identifier (SSID) for the access point.
  - **VLAN ID:** Indicates the VLAN the SSID is operating on.
  - **Security:** Indicates the configured security for the access point.

The Ethernet Window

Accessed through the Ethernet option on the Network Setup sash, the Ethernet window displays the configuration the utilized Ethernet local area network (LAN). For IP configuration procedures, see "Web: Configuring IP Settings Statically or via DHCP" on page 5-18.



Untagged VLAN	1
Management VLAN	1
Speed / Duplex	Auto Negotiation
Connection Type	DHCP
Static IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	
DNS Nameservers	
Domain	

Figure 4-16. The Ethernet Window

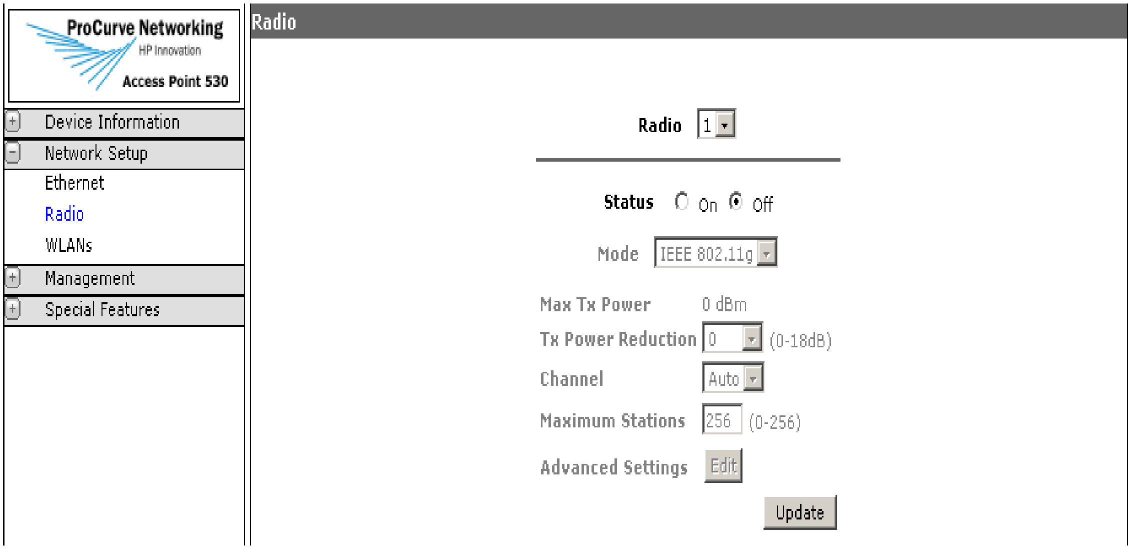
Ethernet Window. The Ethernet window allows configuration of the IP parameters on this device.

- **Untagged VLAN:** Allows input of a VLAN identifier to be associated with untagged packets that are received by or sent from the access point over the Ethernet link.
- **Management VLAN:** Allows designation of a VLAN used for management access.
- **Speed / Duplex**: Allows manual configuration of speed and duplex settings of the Ethernet interface. The access point must be restarted if this setting is changed.
- **Connection Type:** Allows selection of a static IP or DHCP setting. If Static IP is selected, the Static IP Address and and Subnet Mask fields must be assigned.
- **Static IP Address:** The IP address of the access point. (Default is 192.168.1.10)
- **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets. (Default is 255.255.255.0)

- **Default Gateway:** The default gateway is the IP address of the next-hop gateway router for the access point, which is used if the requested destination address is not on the local subnet.
- **Primary and Secondary DNS Address:** The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
- **Domain:** The Doman on the network. The length is between 1 - 64 characters and must contain a "." in the string.
- **[Update]:** Updates the IP settings.

The Radio Window

Accessed through the Radio option on the Network Setup sash, the Radio window allows configuration of radio parameters that directly control the behavior of the radio device in the access point. For Radio configuration procedures, see "Web: Configuring Basic Radio Settings" on page 6-11.



Radio 1

Status ○ On ● Off

Mode IEEE 802.11g

Max Tx Power 0 dBm

Tx Power Reduction 0 (0-18dB)

Channel Auto

Maximum Stations 256 (0-256)

Advanced Settings Edit

Update

Figure 4-17. The Radio Window

The Radio window displays the following information:

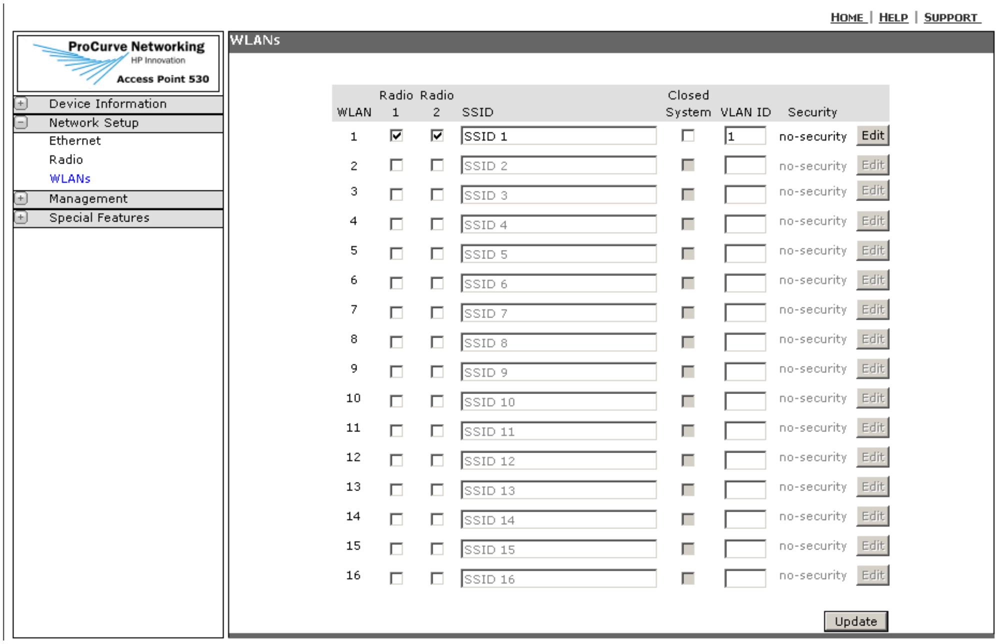
- **Radio:** Allows toggling to either Radio 1 or 2 parameter sets.
- **Status:** Allows enabling/disabling of the respective radio.
- **Mode:** Selects an 802.11 operating mode for the respective radio.

- **Max Tx Power:** Displays the maximum power in dBm of the radio, taking into account the 802.11 operating mode, Tx Power Reduction setting and regulatory constraints of the configured country code.

  Note: 'dBm' notation represents a measured power level relative to 1mW.
- **Tx Power Reduction:** Adjusts the amount of radio attenuation. This control should be used to reduce the AP radio cell size, or compensate for higher gain external antennas. If set to 0 dBm, the radio is operating at maximum power. (Default is 0). See "Web: Setting the Tx Power Reduction" on page 6-21.
- **Channel:** Radio channel the access point uses to communicate. Selecting "Auto" configures the access point to automatically select a channel at startup based on low noise/interference levels and channel utilization by other neighboring access points.
- **Maximum Stations:** Specifies the maximum number of stations that can associate to the applicable radio. (Default is 256).
- **[Advanced Settings]:** Launches the pop-up window for configuring the advanced radio parameters. See"Web: Configuring Advanced Radio Settings" on page 6-13.
- **[Update]:** Updates the radio parameters.

The WLANs Window

Accessed through the WLANs option on the Network Setup sash, the WLANs window details the BSSID unit that consists of an SSID, VLAN, security settings, MAC Authentication, and RADIUS servers. For SSID configuration procedures, see "Web: Configuring SSID Interfaces" on page 6-27 and for Security configuration procedures, see "Web: Setting Security Options" on page 7-14.



WLAN	Radio 1	Radio 2	SSID	Closed System	VLAN ID	Security	
1	☑	☑	SSID 1	□	1	no-security	Edit
2	□	□	SSID 2	□		no-security	Edit
3	□	□	SSID 3	□		no-security	Edit
4	□	□	SSID 4	□		no-security	Edit
5	□	□	SSID 5	□		no-security	Edit
6	□	□	SSID 6	□		no-security	Edit
7	□	□	SSID 7	□		no-security	Edit
8	□	□	SSID 8	□		no-security	Edit
9	□	□	SSID 9	□		no-security	Edit
10	□	□	SSID 10	□		no-security	Edit
11	□	□	SSID 11	□		no-security	Edit
12	□	□	SSID 12	□		no-security	Edit
13	□	□	SSID 13	□		no-security	Edit
14	□	□	SSID 14	□		no-security	Edit
15	□	□	SSID 15	□		no-security	Edit
16	□	□	SSID 16	□		no-security	Edit

Figure 4-18. The WLANs Window

The WLANs window displays configured information:

- **WLAN:** Displays the WLAN identifier.
- **Radio 1/ Radio 2:** Configures the access point to enable WLAN access using either or both radios (when the appropriate box is checked).
- **SSID:** Configures the WLAN's SSID identifier string. SSID is 1-32 characters in length.
- **Closed-System**: Prohibits the broadcasting of the WLAN’s SSID.
- **VLAN ID**: Sets the default VLAN ID for the SSID interface.
- **Security**: Displays the Security Mode for this VLAN.
- **[Edit]**: Launches the Security window with access to security configuration.
- **[Update]:** Updates the WLAN data.

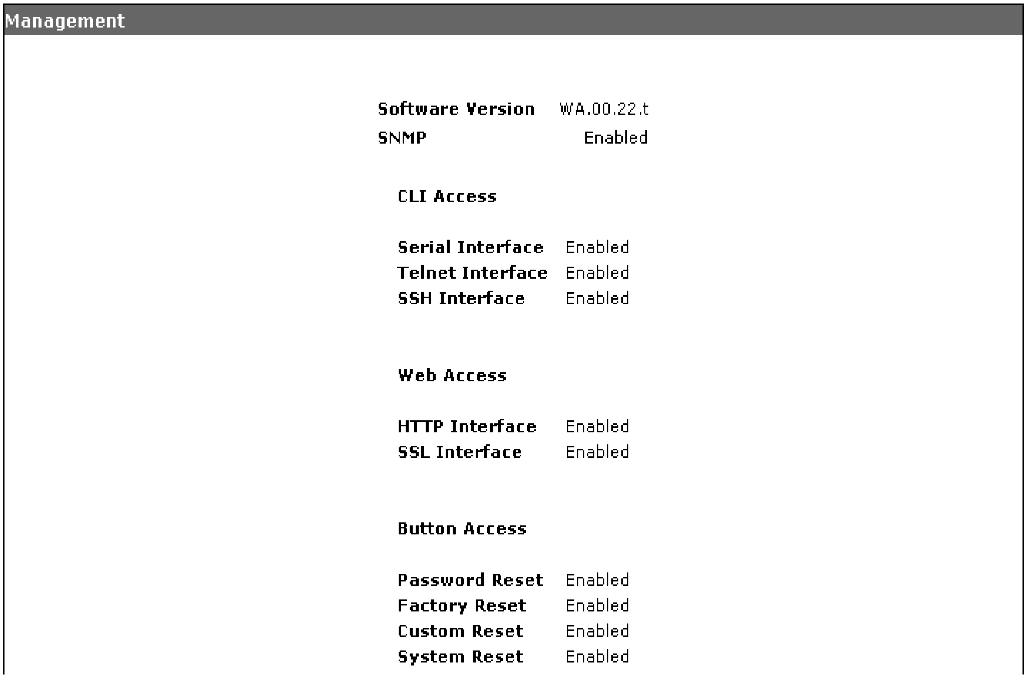
Management

The Management sash is the third logical group available on the Web interface menu. Once accessed, it defaults to the Management window. This group provides access to the following windows:

- Local MAC Authentication
- System Maintenance
- SNMP
- Device Access

The Management Window

Accessed through the Management sash, the Management window displays a summary of access point statistics.



Management

```
Software Version   WA.00.22.t
SNMP                  Enabled

  CLI Access

  Serial Interface   Enabled
  Telnet Interface   Enabled
  SSH Interface      Enabled


  Web Access

  HTTP Interface     Enabled
  SSL Interface      Enabled


  Button Access

  Password Reset     Enabled
  Factory Reset      Enabled
  Custom Reset       Enabled
  System Reset       Enabled
```

Figure 4-19. The Management Window

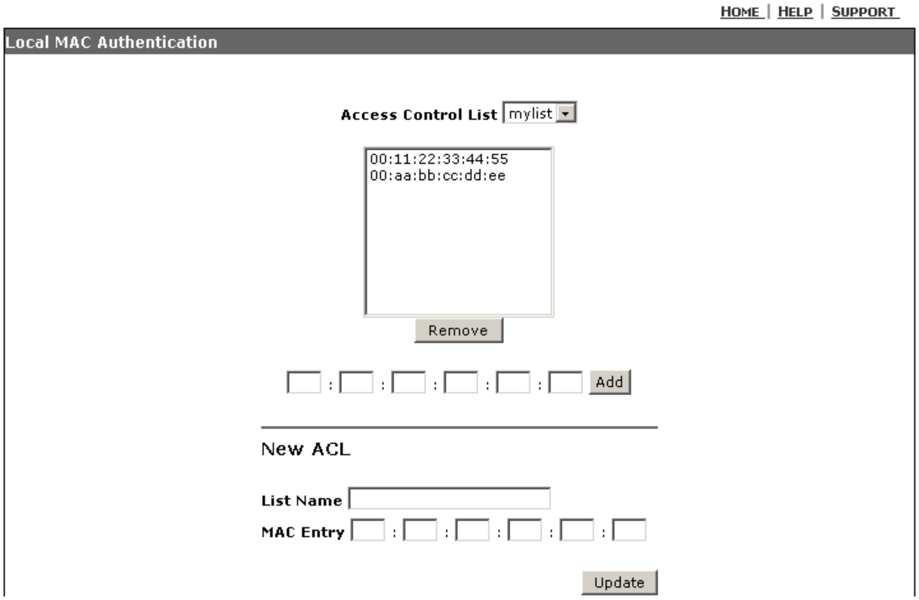
The Management window summarizes:

- **Software Version:** Displays the version of the running software.
- **SNMP:** Indicates if SNMP is enabled or disabled.

- **CLI Access:** Indicates the status (enable or disable) for password and configuration reset using the buttons on the back of the access point, for access to the management CLI through the serial port, and for remote access to the CLI using Telnet or SSH.
- **Web Access:** Indicates the status (enable or disable) for access point support of a Web (HTTP) browser interface and Secure Socket Layer (SSL) which provides a secure encrypted connection to the access point's Web interface.
- **Button Access:** Indicates the status (enable or disable) for password and configuration reset using the buttons on the back of the access point.

Local MAC Authentication

Accessed through the Local MAC Authentication option on the Management tab, the Local MAC Authentication window details all the parameters and events needed for configuring an Access Control List (ACL), which is a mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resource. For ACL configuration procedures, see "Web: Configuring Access Control List" on page 7-38.



Access Control List mylist

00:11:22:33:44:55
00:aa:bb:cc:dd:ee

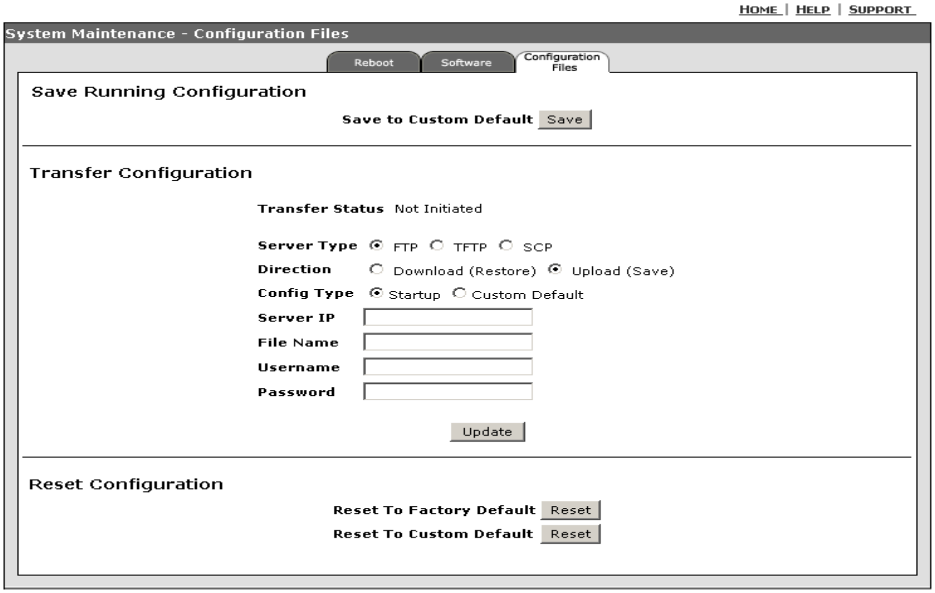
Figure 4-20. The Local MAC Authentication Window

The Web interface enables you to modify these parameters:

- **Access Control List:** Allows creation and maintenance of ACLs which can be directly applied to each WLAN for access control.
  - **[Remove]:** Removes a selected station address from the list.
  - **[Add]:** Field entry for the station MAC address to be listed. Enter six pairs of hexadecimal digits separated by hyphens, for example, 00:11:AA:22:BB:33.
- **New ACL:** Allows development of new ACLs through MAC address entries.
  - **List Name:** Field entry for the name of the new ACL.
  - **MAC Entry:** Field entry for the station MAC address to be listed. Enter six pairs of hexadecimal digits separated by hyphens, for example, 00:11:AA:22:BB:33.
  - **[Update]**: Updates the WLAN (BSS/SSID) interface with the listed MAC configuration.

System Maintenance

Accessed through the System Maintenance option on the Management sash, the System Maintenance window details all the parameters and events needed for controlling the system configuration files. For System configuration procedures, see "Web: Configuration File Upload and Download" on page A-8.



Save Running Configuration

Save to Custom Default [Save]

Transfer Configuration

Transfer Status Not Initiated

Server Type ● FTP ○ TFTP ○ SCP

Direction ○ Download (Restore) ● Upload (Save)

Config Type ● Startup ○ Custom Default

Server IP

File Name

Username

Password

[Update]

Reset Configuration

Reset To Factory Default [Reset]

Reset To Custom Default [Reset]

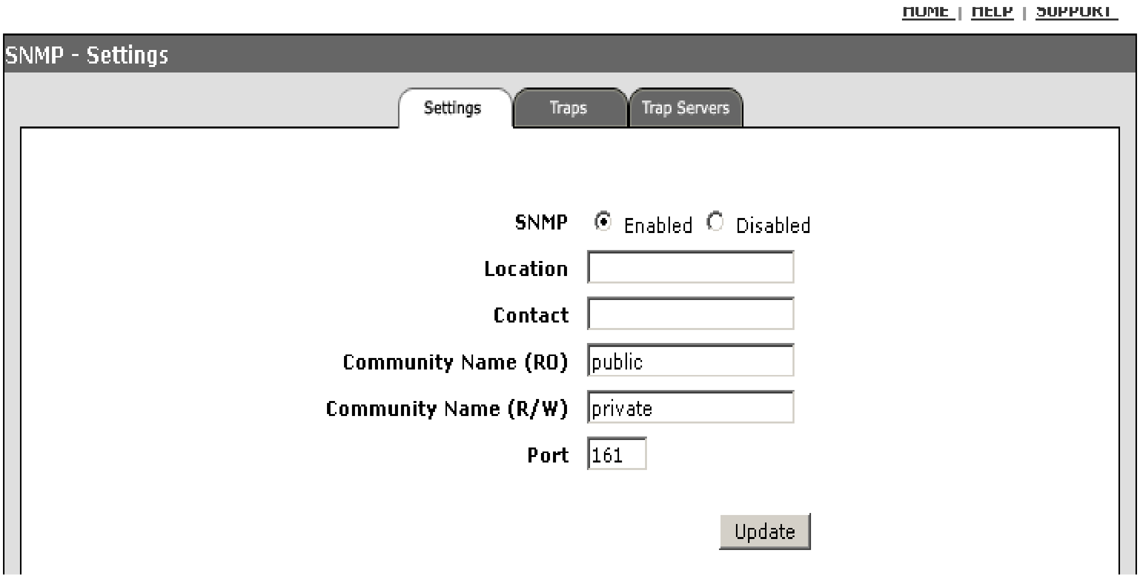
Figure 4-21. The System Maintenance Window

The System Maintenance window has three tabs with the following information:

- **Reboot Tab -** Allows rebooting of the device. See "Web: Configuration File Upload and Download" on page A-8.
- **Software Tab -** Allows remote and local uploading/downloading of software upgrade file. See "Web: Configuration File Upload and Download" on page A-8.
- **Configuration Files Tab -** Allows upload or download of startup and custom configuration files, and resetting to a factory or custom default configuration. See "Web: Configuration File Upload and Download" on page A-8.

SNMP

Accessed through the SNMP option on the Management sash, the SNMP window allows configuration of the SNMP settings for managing the access point. For SNMP configuration procedures, see "Web: Setting Basic SNMP Parameters" on page 5-23.



SNMP - Settings

SNMP	● Enabled ○ Disabled
Location	
Contact	
Community Name (RO)	public
Community Name (R/W)	private
Port	161

Figure 4-22. The SNMP Window

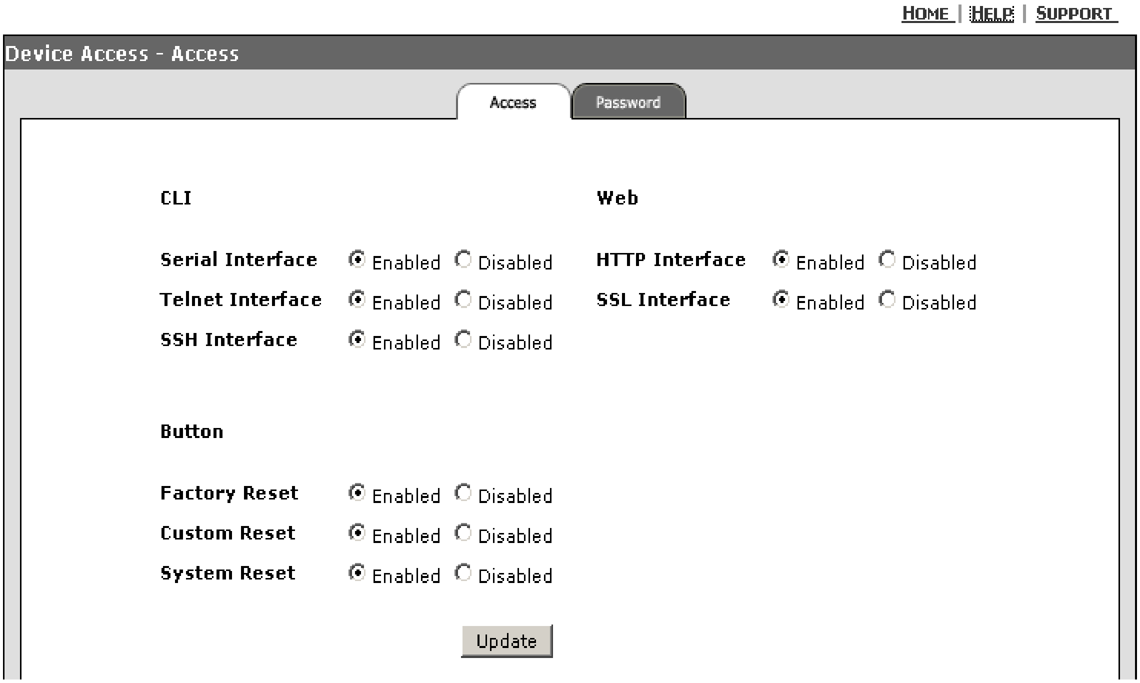
The SNMP window has three tabs with the following information:

- **Settings Tab -** Allows enabling of SNMP, setting location, contact and community SNMP parameters. See "Web: Setting Basic SNMP Parameters" on page 5-23.

- **Traps Tab -** Allows selection of traps to be enabled. See "Web: Configuring SNMP v1 and v2c Trap Destinations" on page 5-28.
- **Trap Servers Tab -** Allows setting of the SNMP trap servers. See "Web: Configuring SNMP v1 and v2c Trap Destinations" on page 5-28.

Device Access

Accessed through the Device Access option on the Management sash, the Device Access window allows configuration for managing access to the access point. For Device Access configuration procedures, see "Web: Configuring Management Controls" on page 5-9.



Device Access - Access

CLI

Serial Interface ● Enabled ○ Disabled
Telnet Interface ● Enabled ○ Disabled
SSH Interface ● Enabled ○ Disabled

Web

HTTP Interface ● Enabled ○ Disabled
SSL Interface ● Enabled ○ Disabled

Button

Factory Reset ● Enabled ○ Disabled
Custom Reset ● Enabled ○ Disabled
System Reset ● Enabled ○ Disabled

Figure 4-23. The Device Access Window

The Device Access window has two tabs with the following information:

- **Access Tab -** Allows enabling of management methods to access the device. See "Web: Configuring Management Controls" on page 5-9
- **Passwords Tab -** Allows modification of a management password. See "Web: Setting Access Point Passwords" on page 5-5

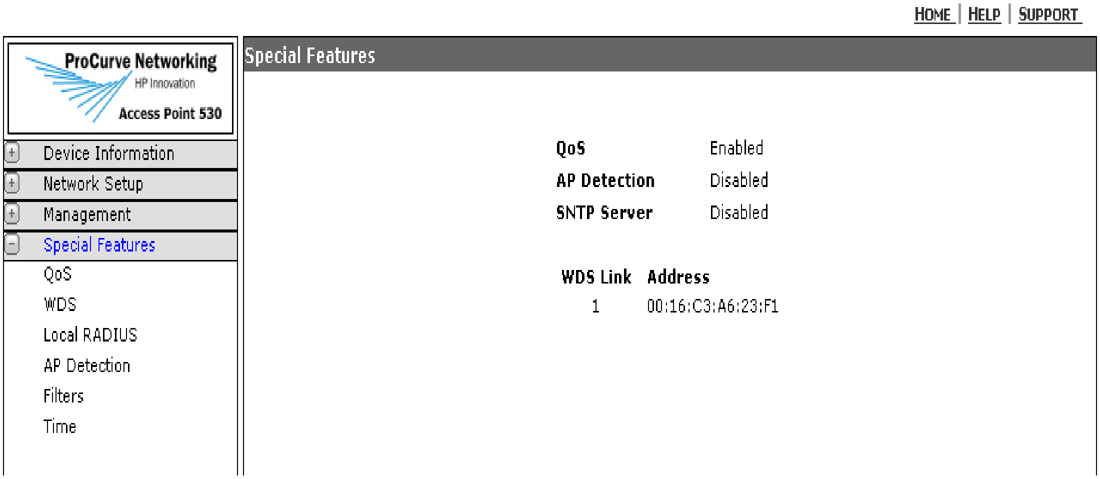
Special Features

The Special Features sash is the fourth logical group available on the Web interface menu. Once accessed, it defaults to the Special Features window. This group provides access to the following windows:

- QoS
- WDS
- Local RADIUS
- AP Detection
- Filters
- Time

The Special Features Window

Accessed through the Special Features sash, the Special Features window displays a summary of special feature statistics.



QoS	Enabled
AP Detection	Disabled
SNTP Server	Disabled

WDS Link	**Address**
1	00:16:C3:A6:23:F1

Figure 4-24. The Special Features Window

The Special Features window summarizes:

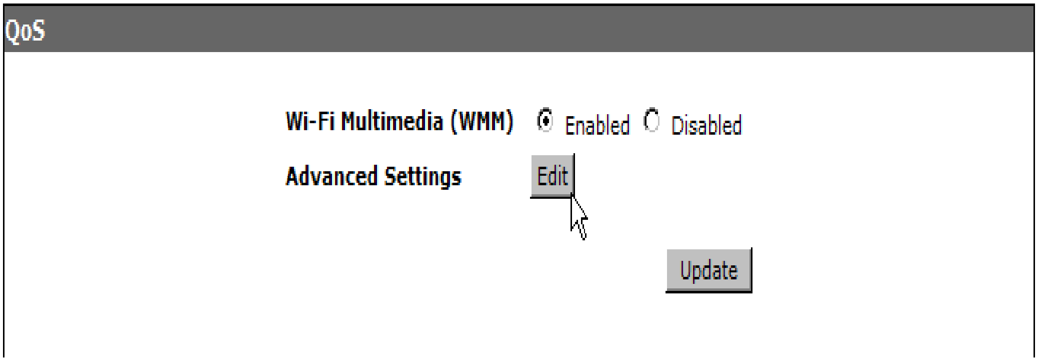
- **QoS:** Indicates if Quality of Service packet prioritization (also referred to as WiFi Multimedia or WMM) is enabled or disabled.
- **AP Detection:** Indicates if AP Detection is enabled or disabled.
- **SNTP Server:** Indicates if the SNTP Server is enabled or disabled.
- **WDS Link/Address:** Indicates the WDS interface number and the configured remote MAC address for each respective enabled WDS link.

QoS

Accessed through the QoS option on the Special Features sash, the QoS window allows configuration of Quality of Service for enhanced throughput and performance on the access point. For QoS configuration procedures, see "Web: Configuring QoS Parameters" on page 8-3.

Note

SVP (SpectraLink Voice Protocol) QoS is enabled at all times and does not require any configuration options.



Wi-Fi Multimedia (WMM) ● Enabled ○ Disabled

Figure 4-25. The QoS Window

The QoS window details the following:

- **WiFi Multimedia (WMM):** Enables/Disables QoS prioritization and coordination of wireless medium access.
- **[Edit]:** Launches the Advanced Settings window to configure specific queue QoS parameters. See "Web: Configuring QoS Parameters" on page 8-3.

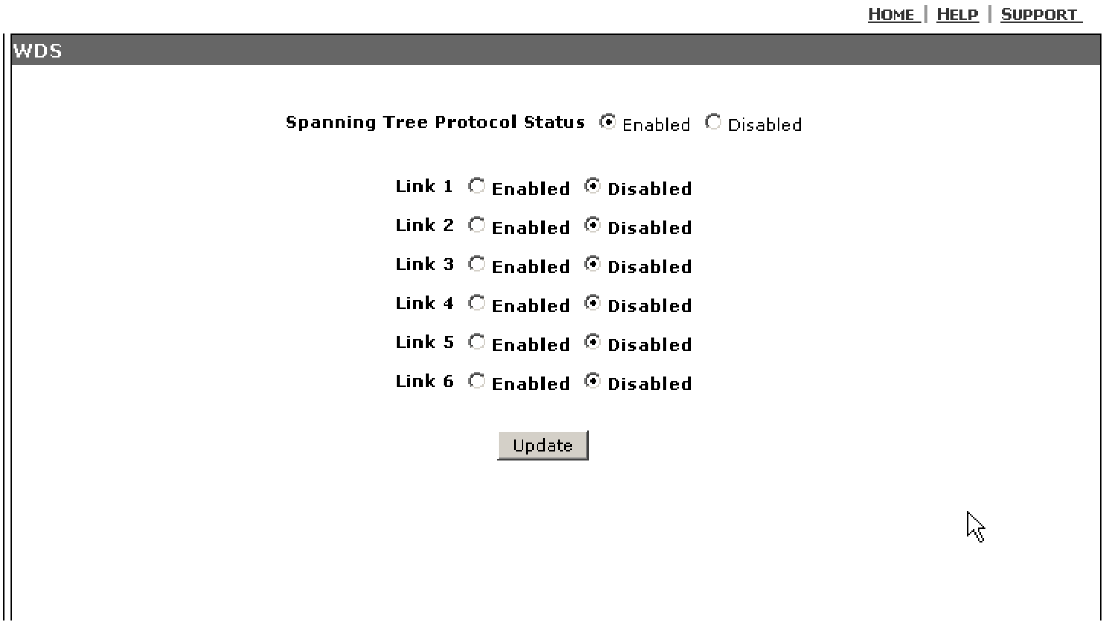
CAUTION

The default WMM parameters settings are usually adequate for WMM operation. Incorrect WMM settings can adversely affect network performance. Changes to WMM parameters should be reserved for someone with an advanced knowledge of how WMM operates. For more on WMM, see the IEEE 802.11e standard.

- **[Update]:** Updates the access point with the QoS details.

WDS

Accessed through the WDS option on the Special Features sash, the WDS window allows configuration of WDS parameters for enhanced throughput and performance on the access point. For WDS configuration procedures, see "Web: Configuring WDS Parameters" on page 8-14.



Spanning Tree Protocol Status ● Enabled ○ Disabled

Link 1 ○ Enabled ● Disabled
Link 2 ○ Enabled ● Disabled
Link 3 ○ Enabled ● Disabled
Link 4 ○ Enabled ● Disabled
Link 5 ○ Enabled ● Disabled
Link 6 ○ Enabled ● Disabled

Figure 4-26. Configuring WDS Parameters

The WDS window details the following:

- **Spanning Tree Protocol Status:** Enables/Disables STP capabilities on the access point.
- **Link (1-6):** Enables/Disables WDS link (1 to 6) capabilities on the access point. Enabling the links provides additional WDS configuration parameters. See"Web: Configuring WDS Parameters" on page 8-14.
- **[Update]:** Updates the WDS link parameters. See"Web: Configuring WDS Parameters" on page 8-14.

Local RADIUS

Accessed through the Local Radius option on the Special Features sash, the Local Radius window allows configuration of RADIUS parameters for local accounts on the access point. For Local RADIUS configuration procedures, see "Web: Establishing Local RADIUS Accounts" on page 7-31.

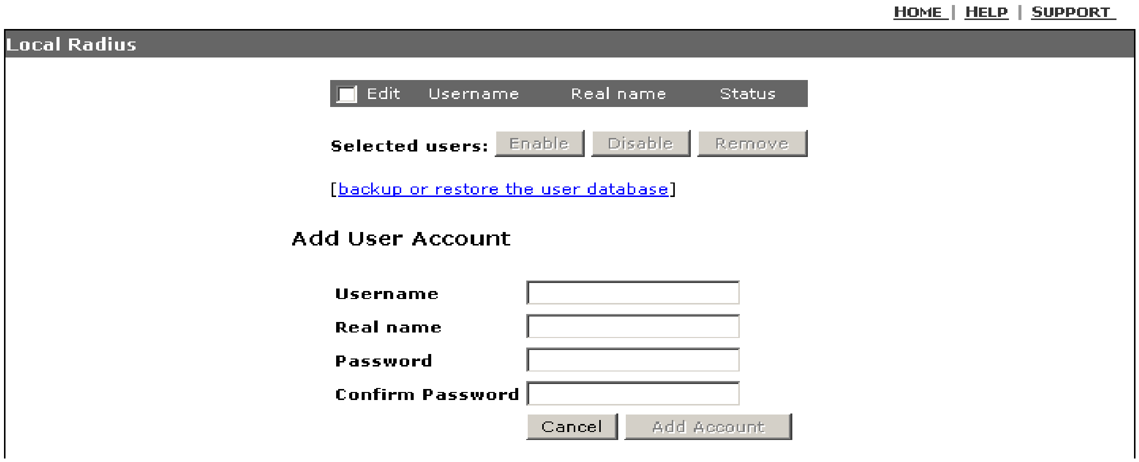


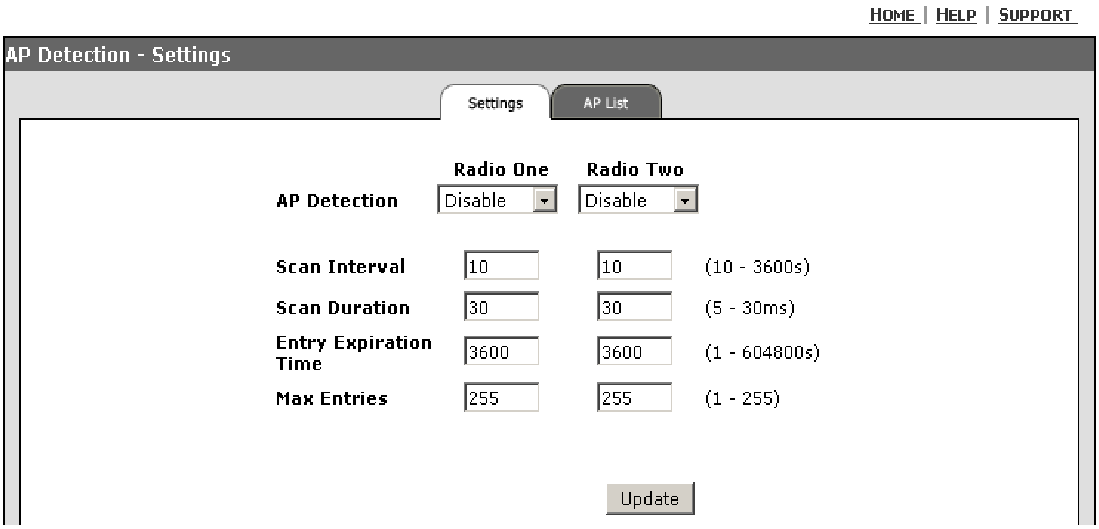
Figure 4-27. Local Radius Window

The Local Radius window provides the following:

- **Edit:** Allows selection established accounts for modification. See "To Add Local RADIUS User Accounts:" on page 7-33.
  - **[Enable] -** Allows enabling of selected user.
  - **[Disable] -** Allows disabling of selected user.
  - **[Remove] -** Allows removal of selected user.
- **Add User Account:** Allows adding local RADIUS user accounts and passwords. See"To Add Local RADIUS User Accounts:" on page 7-33.
  - **Username -** Allows entry of a user name.
  - **Real name -** Allows entry of a real name of a user.
  - **Password** - Allows entry of a user account password.
  - **Confirm Password -** Allows re-entry of a user account password. The entries made to the Password and Confirm Password fields must match exactly, or else the new account is not added.
  - **[Cancel] -** Cancels a pending addition of a new account and clears the User Name, Real Name and password fields.
  - **[Add Account] -** Adds new account.

AP Detection

Accessed through the AP Detection option on the Special Features sash, the AP Detection window allows configuration of AP detection on the access point. Each radio can be independently configured to be a dedicated or background scanner. Dedicated scanning provides the best AP detection results. Background scanning allows the radio to service clients in addition to detecting neighboring access points. For AP Detection configuration procedures, see "Web: Configuring AP Detection Parameters" on page 8-25.



AP Detection - Settings

	Radio One	Radio Two	
AP Detection	Disable	Disable	
Scan Interval	10	10	(10 - 3600s)
Scan Duration	30	30	(5 - 30ms)
Entry Expiration Time	3600	3600	(1 - 604800s)
Max Entries	255	255	(1 - 255)

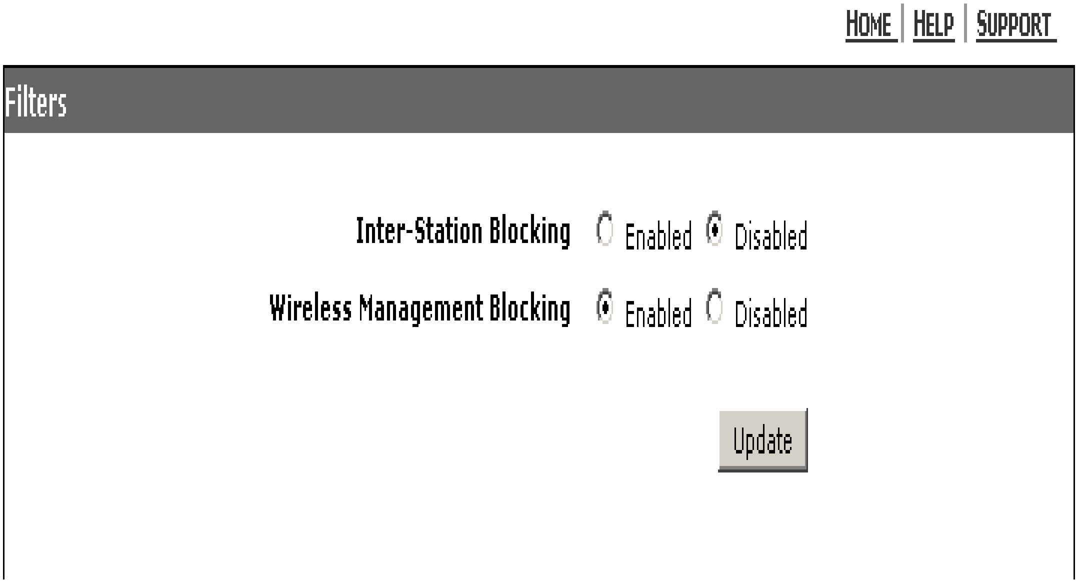
Figure 4-28. The AP Detection Window

The AP Detection window provides two tabs detailing:

- **Settings Tab:** Allows enabling of AP detection and scan parameter setting. "To Enable AP Detection Parameters :" on page 8-27.
- **AP List Tab:** Allows refreshing of scanned and detected access point stations. See"To Enable AP Detection Parameters :" on page 8-27.

Filters

Accessed through the Filters option on the Special Features sash, the Filters window allows enabling of traffic blocking. For Traffic Filter procedures, see "Web: Setting Traffic Filters" on page 5-46.



Inter-Station Blocking ○ Enabled ● Disabled

Wireless Management Blocking ● Enabled ○ Disabled

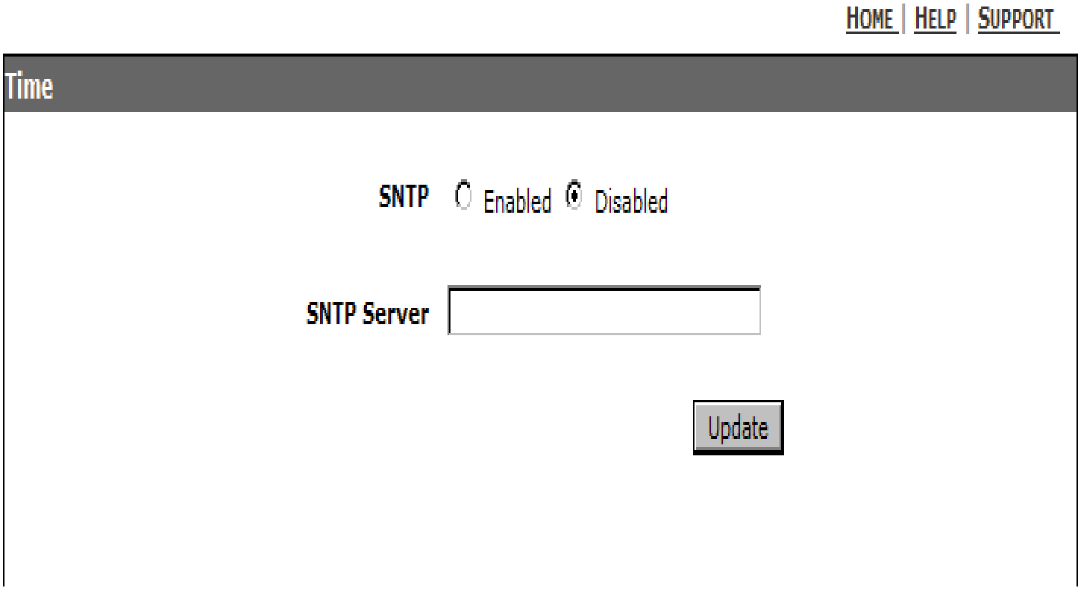
Figure 4-29. The Filters Window

The Filters window details the following:

- **Inter-Station Blocking:** Enables/Disables the blocking of communications between wireless stations. (Default is Disabled)
- **Wireless Management Blocking:** Enables/Disables the blocking of a wireless station's access to the access point.
- **[Update]:** Updates the filter settings on the access point.

Time

Accessed through the Time option on the Special Features sash, the Time window allows enabling of Simple Network Time Protocol (SNTP) parameters. For SNTP procedures, see "Web: Setting SNTP Parameters" on page 5-39.



Time

SNTP ○ Enabled ● Disabled

SNTP Server

Figure 4-30. Configuring SNTP Settings

The SNTP window details the following:

- **SNTP:** Enables/Disables the access point to operate as an SNTP station.
- **SNTP Server:** The IP address or hostname of an SNTP server that the access point attempts to poll for a time update.
- **[Update]:** Updates the SNTP settings on the access point.

— This page is intentionally unused. —

5

General System Configuration

Contents

Overview

This Chapter describes how to:

- Secure your access point
- Modify system management passwords
- Set management access controls
- View and modify access point system information
- Configure IP, SNMP, SNTP, RADIUS Accounting, and VLAN parameters
- Set up filter control between wireless stations, between wireless stations and the management interface, or for specified protocol types

AP Network Configuration Checklist

In setting up your Access Point for network installation, this manual covers many of the tasks that should be considered for proper security and management. Each of these tasks are detailed in their respective sections, however, this summary is provided as an aid for establishing your network.

Table 5-1. Network Installation & Security Configuration Summary

Physical Security	
Using a Kensington Lock. See the *ProCurve AP 530 Installation and Getting Started Guide* provided on the CD.	
Using back panel covers to hide access to buttons and cable connections. See the *ProCurve AP 530 Installation and Getting Started Guide* provided on the CD.	
Disabling device reset and clear buttons.	page A-17
Disabling console access to the CLI interface.	page 5-8
Management Interfaces	
Changing the default settings for password.	page 5-5
Limiting management access to the Ethernet side of the AP (disabling wireless access to remote management interfaces).	page 5-8
Disabling unused remote management interfaces (Web, Telnet, SSH, SNMP).	page 5-8
Changing the default settings for SNMP read and read/write community names.	page 5-23
Configuring capture of operating events to a Syslog server.	page 5-37
Configuring the access point to limit remote management to a management VLAN.	page 5-48
Wireless LAN Security	
Setting WLAN security to utilize WPA/WPA2.	page 5-48
Configuring multiple SSIDs to utilize separate VLANs.	page 5-48
Configuring local user authentication.	page 5-48
Configuring primary and secondary remote RADIUS user authentication.	page 5-48
Configuring Identity-Driven Management features.	page 5-48
Restricting access between wireless client devices associated with the same access point.	page 5-48

Modifying Management Passwords

Management access to the access point's CLI and Web interfaces is controlled through an administrator password.

Additional in-band access security can also be gained by setting management access controls (see "Setting Management Access Controls" on page 5-8) and using traffic filters (see "Setting Up Filter Control" on page 5-46).

Caution

HP strongly recommends that you configure a new Manager password and not use the default. If a Manager password is not configured, then the access point is not password-protected, and anyone having in-band or out-of-band access to the access point may be able to compromise access point and network security.

Pressing the Clear button on the back of the access point for more than two seconds removes password protection.

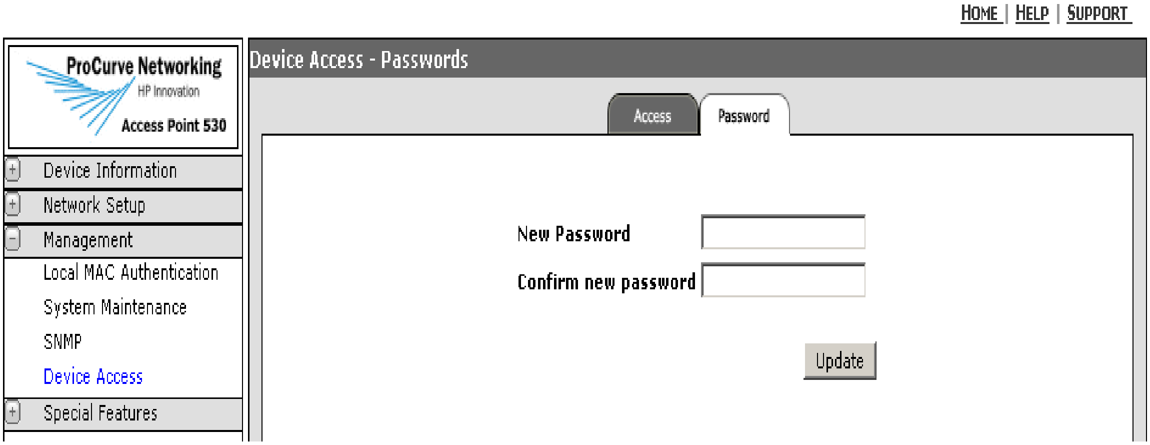
Web: Setting Access Point Passwords

The Passwords window enables the access point's passwords to be set.

The Web interface enables you to modify these parameters:

- **New Password:** New password to gain access to the administration of the access point.

  Note: The password is case sensitive and must be at least 1 character and at most 32 characters long. However, only the first 8 characters of the password are used; character number 9 and above are ignored at log in.
- **Confirm New Password:** Re-entered new password to gain access to the administration of the access point.
- **[Update]:** Updates the new password.



To Create a Password:

1. Select Management> Device Access > Passwords tab.
2. In the Current Password text field, enter the **current password**.
3. In the New Password text field, enter a **new password.**

   Note: The password is case sensitive and must be at least 1 character and at most 32 characters long. However, only the first 8 characters of the password are used; character number 9 and above are ignored at log in.
4. In the Confirm Password text field, re-enter the **new password**.
5. Click **[Update]** to activate the new password.

Note

The password you assign in the Web browser interface will overwrite the previous settings assigned in either the Web browser interface or the access point console. That is, the most recently assigned user password is immediately effective for the access point, regardless of which interface was used to assign these parameters.

CLI: Setting Management Password

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
password manager <*password*>	9-20

This example shows how to create a manager password.

Caution

If you modify the password through CLI, you also modify the Web password.

Note

The password is case sensitive and must be at least 1 character and at most 32 characters long. However, only the first 8 characters of the password are used; character number 9 and above are ignored at log in.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# password manager password

ProCurve Access Point 530(config)#
```

Setting Management Access Controls

To provide more security for the access point, management interfaces that are not required can be disabled. This includes the Web, Telnet, and Secure Shell (SSH), as well as the serial console port and Reset button.

Note

The access point's serial port and Reset button cannot be disabled at the same time. When the Reset button is disabled, it is not possible to disable the serial port.

HTTP and HTTPS. The access point supports both a Web (HTTP) and secure Web (HTTPS) browser interface. The secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL) provides a secure encrypted connection to the access point's Web interface. Both the HTTP and HTTPS service can be enabled independently.

Note

The HTTP and HTTPs services do not allow modification of the configured port numbers.

Secure Shell (SSH). Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, Telnet is not secure from hostile attacks. SSH can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station stations and ensures that data traveling over the network arrives unaltered. stations can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Note

The access point supports only SSH version 2.0.

After boot up, the SSH server needs about one minute to generate host encryption keys. The SSH server is disabled while the keys are being generated.

Web: Configuring Management Controls

The Remote Access tab on the Management window enables management and button access controls to be configured.

The Web interface enables you to modify these parameters:

CLI Access

- **Serial Interface**: Enables or disables management access through the access point's serial console port. (Default is Enabled)

NOTE

You can not disable the serial interface, if you already have disabled the Factory Reset option.

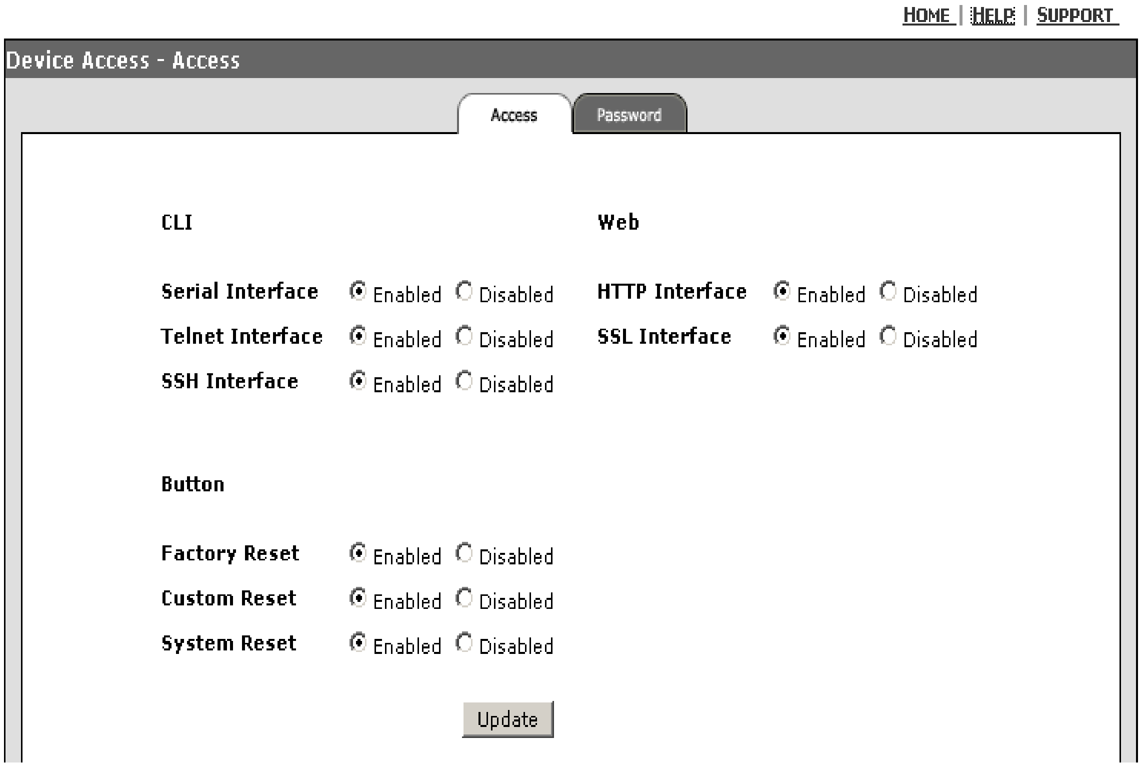
- **Telnet Interface**: Enables or disables management access through Telnet. (Default is Enabled)
- **SSH Interface**: Enables or disables management access through a Secure Shell version 2.0 client. (Default is Enabled)

Web Access

- **HTTP Interface**: Enables or disables management access through and HTTP interface . (Default is Enabled)
- **SSL Interface**: Enables or disables management access through an SSL interface. (Default is Enabled)

Button Access - For managing button access see, "Disabling the Access Point Push Buttons" on page A-17.

- **Factory Reset**: Enables or disables button control access (back panel of the access point) to a factory default file reset. (Default is Enabled)
- **Custom Reset**: Enables or disables button control access (back panel of the access point) to a custom config file reset. (Default is Enabled)
- **System Reset**: Enables or disables button control access (back panel of the access point) to a system reset. (Default is Enabled)



Device Access - Access

CLI

Serial Interface ● Enabled ○ Disabled

Telnet Interface ● Enabled ○ Disabled

SSH Interface ● Enabled ○ Disabled

Web

HTTP Interface ● Enabled ○ Disabled

SSL Interface ● Enabled ○ Disabled

Button

Factory Reset ● Enabled ○ Disabled

Custom Reset ● Enabled ○ Disabled

System Reset ● Enabled ○ Disabled

Figure 5-1. Configuring Management Controls

To Configure Management Control Settings:

1. Select Management> Device Access > Remote Access tab.
2. As required, enable or disable the serial, Telnet, or SSH interfaces.
   If using SSH for secure access to the CLI over a network connection, you may want to disable the Telnet server.
3. As required, enable or disable the HTTP or SSL interfaces.
4. As required, enable or disable the manual push button options on the access point.
   The access point does not allow you to disable Factory Reset and the Serial Interface at the same time.
5. Click **[Update]** to ensure management controls are set.

CLI: Configuring Management Controls

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] console	9-22
[no] ssh	9-24
[no] telnet	9-23
show console	9-27
show system	9-27

The following example shows how to enter management configuration context and control access to the Access Point device.

This example shows how to disable the console access to this device using the **no ssh** command and display the current status of the access routes using the **show console** command.

Note

Enter management commands, one per line.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# no console
ProCurve Access Point 530(config)# show console
------------------------------------------------------------
CLI Access:
 Serial Interface           Disabled
 Telnet Interface           Enabled
 SSH Interface              Enabled

 CLI Confirmation Dialogs   Enabled


Web Access:
 HTTP Interface             Enabled
 SSL Interface              Enabled
ProCurve Access Point 530(config)#
```

The following example demonstrates the **no ssh** command to disable the serial SSH port, and the **show ssh** command to display the current status.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# no ssh
ProCurve Access Point 530(config)# show ssh
------------------------------------------------------------
CLI Access:
 Serial Interface           Disabled
 Telnet Interface           Enabled
 SSH Interface              Disabled

 CLI Confirmation Dialogs   Enabled


Web Access:
 HTTP Interface             Enabled
 SSL Interface              Enabled
ProCurve Access Point 530(config)#
```

The following example shows using the **no telnet** command to disable the serial Telenet connection to this device.

Caution

You should use the **no telnet** command, only when you are connected to the access point through another method. Once you disable the Telnet, the Telnet connection is immediately lost .

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# no telnet
------------------------------------------------------------
C:connection is lost
```

To display the current status for management access controls, use the **show system** command.

```
ProCurve Access Point 530# show system
-------------------------------------------------------------------
Serial Number          TW547VV07X
System Name            ProCurve-AP-530
System Up Time         2 days 23 hours 35 mins 18 secs
System Location        not set
System Country Code    us
Software Version       WA.01.00
Ethernet MAC Address   00:14:C2:A5:08:CB
IP Address             192.168.15.100
Subnet Mask            255.255.255.0
Default Gateway        192.168.15.1
DHCP Client            Enabled
Management VLAN ID     1
Untagged-VLAN ID       1
Radio 1 MAC Address    00:14:C2:A5:22:E0
Radio 1 Status         Disabled (802.11g)
Radio 2 MAC Address    00:14:C2:A5:22:F0
Radio 2 Status         Disabled (802.11a)
HTTP Interface         Enabled
SSL Interface          Enabled
SSH Interface          Enabled
Telnet Interface       Enabled
Serial Interface       Enabled

ProCurve Access Point 530#
```

Modifying System Information

The access point's system name can be left at its default setting. However, modifying this parameter can help you to more easily distinguish one device from another in your network.

Note

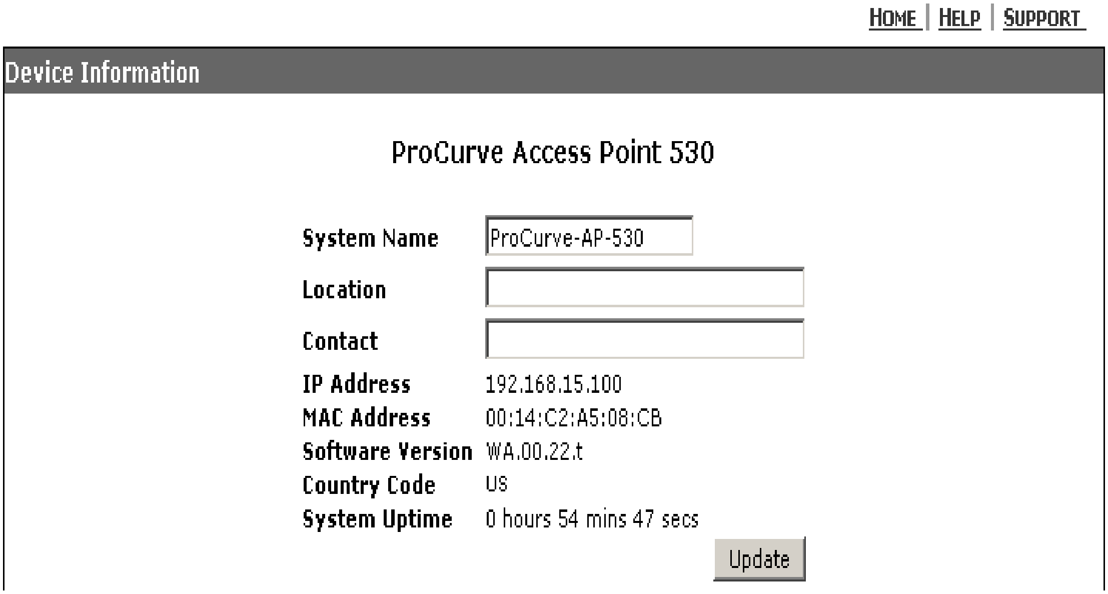
You should also set the applicable WLANs (BSS/SSID) to identify the wireless network service provided by the access point. See "Configuring the Radio" on page 6-5.

Web: Setting the System Name, Location, and Contact

To modify the access point's system parameters, use the Device Information window (the Home page or default window).

The Web interface enables you to modify these parameters:

- **System Name**: An alias for the access point only, enabling the device to be uniquely identified on the network. Setting can has to be at least 1 character and a maximum of 63 characters long . (Default is ProCurve AP-530)
- **Location**: The access point's assigned location. (Default is not set)
- **Contact**: The name of the Administrator responsible for the system. (Default is not set)
- **[Update]:** Updates the system information.



ProCurve Access Point 530

System Name: ProCurve-AP-530
Location:
Contact:
IP Address: 192.168.15.100
MAC Address: 00:14:C2:A5:08:CB
Software Version: WA.00.22.t
Country Code: US
System Uptime: 0 hours 54 mins 47 secs

Figure 5-2. Configuring System Information

To Configure System Information:

1. Select the Device Information tab.
2. Type a **name** to uniquely identify the access point in the **System Name** text field.
3. Type a **location** to identify where the access point it located in the **Location** text field.
4. Type a **name** to identify the contact in the **Contact** text field.
5. Click **[Update]** to modify the system information.

CLI: Setting the System Name

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
hostname *<hostname>*	9-19
show system-information	9-27

The following example shows using the **hostname** *<hostname>* syntax to set the name of the system.

Note Enter management commands, one per line.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# hostname ProCurve-AP530

ProCurve Access Point 530(config)#
```

To display the configured system name, use the **show system-information** command.

```
ProCurve Access Point 530# show system-information
-------------------------------------------------------------------
Serial Number         TW547VV07X
System Name           ProCurve-AP-530
System Up Time        2 days 23 hours 35 mins 18 secs
System Location       not set
System Country Code   us
Software Version      WA.01.00
Ethernet MAC Address  00:14:C2:A5:08:CB
IP Address            192.168.15.100
Subnet Mask           255.255.255.0
Default Gateway       192.168.15.1
DHCP Client           Enabled
Management VLAN ID    1
Untagged-VLAN ID      1
Radio 1 MAC Address   00:14:C2:A5:22:E0
Radio 1 Status        Disabled (802.11g)
Radio 2 MAC Address   00:14:C2:A5:22:F0
Radio 2 Status        Disabled (802.11a)
HTTP Interface        Enabled
SSL Interface         Enabled
SSH Interface         Enabled
Telnet Interface      Enabled
Serial Interface      Enabled

ProCurve Access Point 530#
```

Configuring Ethernet Settings

Configuring the access point with an IP address expands your ability to manage the access point and use its features. A number of access point features depend on IP addressing to operate.

Note

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

By default, the access point is configured to automatically receive IP addressing from a Dynamic Host Configuration Protocol (DHCP) server. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values. After you have network access to the access point, you can use the Web browser interface to modify the initial IP configuration, if needed.

Note

If there is no DHCP server on your network, or DHCP fails, the access point will automatically start up with a default IP address of 192.168.1.10.

Web: Configuring IP Settings Statically or via DHCP

The Ethernet window on the Network Configuration tab allows the DHCP client to be enabled or the Transmission Control Protocol/Internet Protocol (TCP/IP) settings to be manually specified.

The Web interface enables you to modify these parameters:

- **Untagged VLAN:** Allows input of a VLAN identifier.
- **Speed Duplex:** Allows selection of the ethernet interface. (Default is 'Use Auto Negotiation').

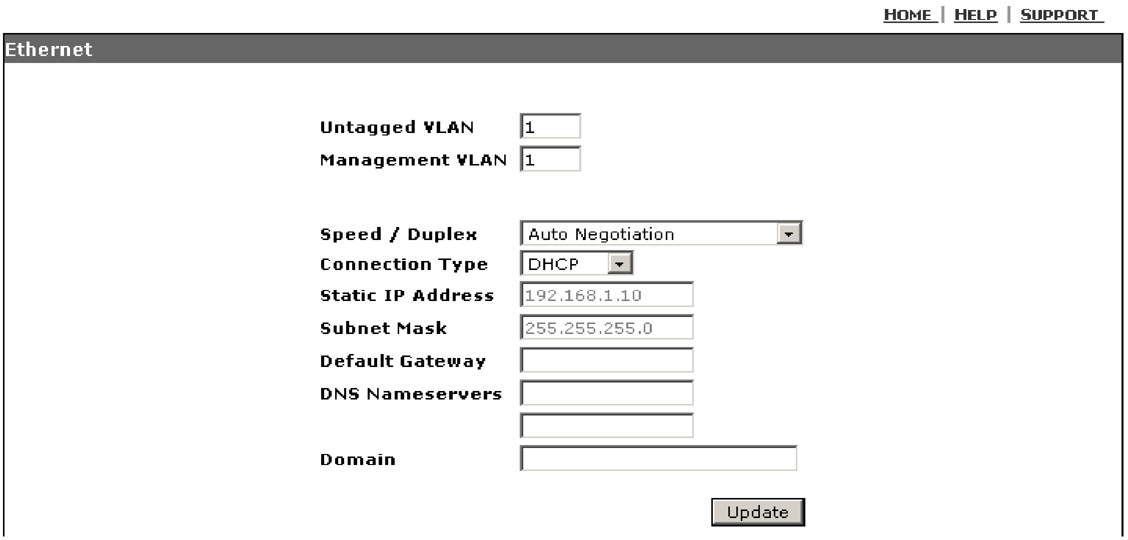
  If the Ethernet port to which the access point is connected requires a fixed speed or duplex setting, you can set the speed and duplex from the Speed/Duplex pick list.

  You can fix the speed to 10 or 100 Mbps (megabites per second), and the duplex mode to full, half or auto.

  The most common setting is "auto-negotiate" for which the access point and switch port will negotiate to the best speed and duplex supported.

  Note: After changing the speed/duplex setting, the access point reboots.

- **Connection Type:** Allows selection of a static or DHCP setting.
  - **DHCP:** The DHCP client is defaulted. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) addresses are dynamically assigned to the access point by the network DHCP server.
  - **Static IP**: If selected, the DHCP client is disabled and the IP address settings are auto populated.
    - **IP Address:** The IP address of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default is 192.168.1.10) Required field.
    - **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets. (Default is 255.255.255.0) Required field.
    - **Default Gateway:** The default gateway is the IP address of the next-hop gateway router for the access point, which is used if the requested destination address is not on the local subnet. Required field.
    - **DNS Nameservers:** Select Dynamic or Manual. The primary and secondary IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
- **[Update]:** Updates the IP settings.



Ethernet

Untagged VLAN	1
Management VLAN	1
Speed / Duplex	Auto Negotiation
Connection Type	DHCP
Static IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	
DNS Nameservers	
Domain	

Figure 5-3. Configuring IP Settings

To Enable the DHCP Client i:

1. Select Network Setup > Ethernet.
2. To configure the VLAN (untagged), enter **value** in the VLAN text field.
3. To set the mode and speed of data transmission, select **Speed/Duplex** in the drop-down.
4. To set a dynamic connection, select **DHCP** in the Connection Type drop-down.
5. Click **[Update]** to save the DHCP settings.

To Configure IP Settings Manually:

1. Select Network Setup > Ethernet.
2. To configure the VLAN (untagged), enter **value** in the VLAN text field.
3. To set the mode and speed of data transmission, select **Speed/Duplex** in the drop-down.
4. To set a manual connection, select **Static IP** in the Connection Type drop-down.
5. If you chose Static IP, the IP address and subnet mask auto populates with the system defaults. You can manually enter a new **IP address** and **subnet mask** in the Static IP Address and Subnet Mask text fields. These are required fields.
6. If a management station exists on another network segment, enter the **IP address of a gateway** that can route traffic between these segments. This is a required field.
7. To set dynamic DNS nameservers, select **Dynamic.** To set the nameservers manually, select **Manual**.
8. If you chose to manually enter the DNS nameservers, enter the **IP address** for the primary and secondary DNS servers to be used for host-name to IP address resolution.
9. Click **[Update]** to save these IP settings.

CLI: Configuring IP Settings Statically or via DHCP

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
interface <*interface*>	9-66
[no] ip address dhcp <ip> [<mask>] <ip>/<bits> <dhcp>	9-70
ip default-gateway	9-71
dns primary <*server_1*>	9-68
dns secondary <*server_2*>	9-69
show interfaces<*interface*>	9-73

The following example shows how to enable the DHCP client and automatically set the ip address for the DHCP client using the **interface** and **ip address** commands.

Note

Enter ethernet commands, one per line.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#ip address dhcp

ProCurve Access Point 530(ethernet)#
```

Note

To ensure the access point doesn’t overwrite the static IP address, you must first disable the DHCP client with the ‘no ip address dhcp’ command.

The following example shows how to disable the DHCP client and then specify an IP address, subnet mask, default gateway, and DNS server addresses.

Caution

In order to disable the DHCP and assign a Static IP address, you must have a serial port connection to the access point. Otherwise, you will lose connectivity during the process of assigning a new static IP address.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#no ip address dhcp
ProCurve Access Point 530(ethernet)#ip address 192.168.1.105
255.255.255.2
ProCurve Access Point 530(ethernet)#ip default-gateway
192.168.1.1
ProCurve Access Point 530(ethernet)#exit
ProCurve Access Point 530(config)#dns primary 204.127.202.0
ProCurve Access Point 530(config)#dns secondary
216.148.227.00
ProCurve Access Point 530(config)#
```

To display the current IP settings, use the **show ip** command as shown in the following example.

```
ProCurve Access Point 530#show ip
IP Address Information:
-------------------------------------------------
System Host Name  ProCurve-AP-530
IP Address        192.168.1.105
Subnet Mask       255.255.255.2
Default Gateway   192.168.1.1
DHCP Client       Enabled

DNS Information (Obtained from DHCP):
Domain Name Suffix   example.ca.example.net.
Primary DNS Server   204.127.202.0
Secondary DNS Server 216.148.227.00


ProCurve Access Point 530#
```

Configuring SNMP

You can use a network management application such as the ProCurve Manager to manage the access point via the Simple Network Management Protocol (SNMP) from a network management station. Simple Network Management Protocol (SNMP) is an industry standard protocol for managing network devices, such as hubs, bridges, and switches. SNMP is a collection of specifications for network management that includes the protocol itself, the definition of a database, and associated concepts. SNMP minimizes network traffic and firmware code size and allows control of retry rates and reporting of detected events, using SNMP traps.

To implement SNMP management, the access point must have an IP address and subnet mask, configured either manually or dynamically.

You can configure the access point to respond to SNMP requests and generate SNMP traps. When SNMP management stations send GET or SET requests to the access point, the SNMP responds with the requested data or the status of the set operation. The access point can also be configured to send information to SNMP managers through trap messages.

Note

The access point is shipped with a default read-only community name. Please change the community name or disable SNMP to prevent unauthorized access to the access point.

The access point's SNMP agent supports SNMP versions 1 and 2c. Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with the access point, an SNMP v1 or v2c management station must first submit a valid community name for authentication. If you intend to support SNMP v1 or v2c managers, you must configure the read-only and read-write community names.

Note

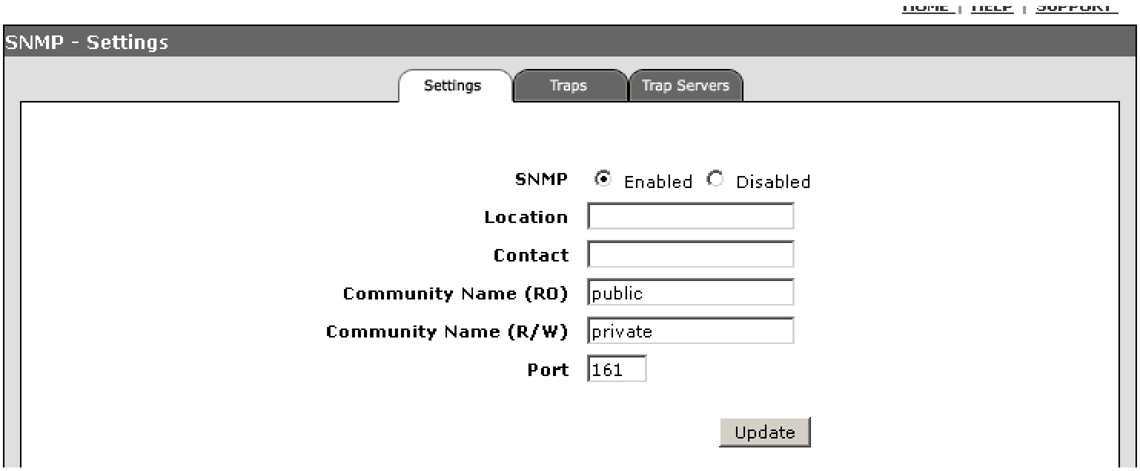
The access point supports the following Management Information Bases (MIBs): HP proprietary MIB, SNMPv2 MIB, 802.11 MIB and MIB II.

Web: Setting Basic SNMP Parameters

The SNMP window on the Management tab controls management access to the access point from management stations using SNMP.

The Web interface enables you to modify these parameters:

- **SNMP:** Enables or disables SNMP management access and also enables the access point to send SNMP traps (notifications). (Default is Enabled)
- **Location:** Text string defining the physical location of the access point. Range 0-255 characters. (Default is not set)
- **Contact:** Text string defining the name of the administrator of the access point. Range 0-255 characters. (Default is Network Administrator)
- **Community Name (RO):** Defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects. Range 0-32 characters, (Default is public)
- **Community Name (RW):** Defines the SNMP community access string that has read/write access. Authorized management stations are able to both retrieve and modify MIB objects. Range 0-32 characters. (Default is private)
- **Port:** Defines the number specifying the port to which the SNMP server will listen.(Default is 161)
- **[Update]:** Updates the SNMP settings.



SNMP ● Enabled ○ Disabled
Location
Contact
Community Name (RO) public
Community Name (R/W) private
Port 161

Figure 5-4. The SNMP Settings Tab

To Enable SNMP and Set Parameters:

1. Select Management > SNMP > Settings tab.
2. To activate the SNMP feature on the access point, select **Enabled.**
3. Enter a **location** and **contact** into their respective text fields**.**

4. To establish a public read-only SNMP community, type a **name** text string to replace the default community name (public) in the Community Name (RO) text field.
5. To establish a private read-write SNMP community, type a **name** text string to replace the default community name (private) in the Community Name (R/W) text field.
6. Enter a **port value** in the port text field.
7. Click **[Update]** to activate the new SNMP community name.

CLI: Setting Basic SNMP Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] snmp-server community <*comm*> **restricted | unrestricted**	9-36
snmp-server contact <*contact*>	9-37
snmp-server port <*port*>	9-39
[no] snmp-server host <host>|<comm>	9-38
snmp-server location <*location*>	9-39
show snmp-server	9-40

SNMP management on the access point defaults the community settings to “restricted” and “public”. To disable SNMP communities, type the following commands.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#no snmp-server community
public restricted
ProCurve Access Point 530(config)#no snmp-server community
system unrestricted

ProCurve Access Point 530(config)#
```

The following example shows how to configure the SNMP community strings, the community name (using the server host command), and the following parameters (contact, port, and location). The default port number is 161.

NOTE

Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#snmp-server community
alpha unrestricted
ProCurve Access Point 530(config)#snmp-server community beta
restricted
ProCurve Access Point 530(config)#snmp-server host
10.10.1.10 alpha
ProCurve Access Point 530(config)#snmp-server contact Jim
ProCurve Access Point 530(config)#snmp-server location 2F
R19
ProCurve Access Point 530(config)#snmp-server port 161
ProCurve Access Point 530(config)#
```

To display the current SNMP settings, use the **show snmp-server** command, as shown in the following example.

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#show snmp-server
SNMP Server Settings
-------------------------------------------------
SNMP Status      Enabled
SNMP Port        161
Community (ro)   beta
Community (rw)   alpha
Location         2FR19
Contact          Jim

Trap Destinations
Host            Community
-----------------------
1               192.168.1.15
2               192.168.1.19
192.168.1.10    alpha

hpWlanAdHocNetworkDetected        Enabled   hpWlanApDetectionUpdate    Enabled
hpWlanRadioAntennaUpdate          Enabled   hpWlanButtonUpdate         Enabled
hpWlanClientAssociation           Enabled   hpWlanApInterfaceUpdate    Enabled
hpWlanClientDeAuthentication      Enabled   hpWlanClientAuthentication Enabled
hpWlanClientRequestFailure        Enabled   hpWlanClientReAssociation  Enabled
hpWlanDot1XAuthNotInitiated       Enabled   hpWlanDot1XAuthFailure     Enabled
hpWlanLocalMacAuthClientFailure   Enabled   hpWlanDot1XAuthSuccess     Enabled
hpWlanLocalMacAuthClientSuccess   Enabled   hpWlanMgmtAccessUpdate     Enabled
hpWlanPossibleNeighborApDetected  Enabled   hpWlanMgmtVlanIdUpdate     Enabled
hpWlanRadiusAccountingUpdate      Enabled   hpWlanRadiusServerFailover Enabled
hpWlanRemoteMacAddrAuthFailure    Enabled   hpWlanSystemUp             Enabled
hpWlanRemoteMacAddrAuthSuccess    Enabled   hpWlanSystemDown           Enabled
hpWlanSystemFWUpgradeStatus       Enabled   hpWlanVlanUntaggedUpdate   Enabled
hpWlanSystemConfigFileTransfer    Enabled
ProCurve Access Point 530(config)#
```

Web: Configuring SNMP v1 and v2c Trap Destinations

The SNMP Trap and SNMP Trap Server tabs provide configuration for SNMP v1 and v2c trap notifications that can be sent to specified management stations.

The Traps tab allows enabling of specific SNMP notifications to be sent:

- **System Traps:** pertaining to the system.
  - **hpWlanSystemUp** – This notification is sent when the access point is fully up and running.
  - **hpWlanSystemDown** – This notification is sent before the access point is about to reboot.
  - **hpWlanMgmtAccessUpdate** – This notification is sent when system management access is set to Enable/Disable.
  - **hpWlanButtonUpdate** – This notification is sent when the RESET and CLEAR button functions buttons are set to Enable/Disable.
  - **hpWlanSystemFWUpgradeStatus** – This trap contains information about the current status of firmware upgrade. The IP address is the file server's IP address..
  - **hpWlanSystemConfigFileTransfer** – This trap contains information about the file name, server address and direction of configuration file. The IP address is the file server's IP address.
- **AP Traps:** pertaining to the access point.
  - **hpWlanApInterfaceUpdate** - This notification is sent out when the Ethernet or 802.11 wireless (radio) interface is enabled or disabled.
  - **hpWlanApSSIDUpdate** – This notification is sent out when an SSID is enabled or disabled.
  - **hpWlanClientAssociation**– This notification is sent when a station successfully associates with the access point. The notification value includes the MAC address of the associated station.
  - **hpWlanClientReAssociation** – This notification is sent when a station successfully re-associates with the access point. The notification value includes the MAC address of the re-associated station.
  - **hpWlanClientAuthentication** – This notification is sent when a station successfully authenticates with the access point. The notification value includes the MAC address of the authenticated station.
  - **hpWlanClientDeauthentication** – This notification is sent when a station successfully authenticates with the access point. The notification value includes the MAC address of the authenticated station.

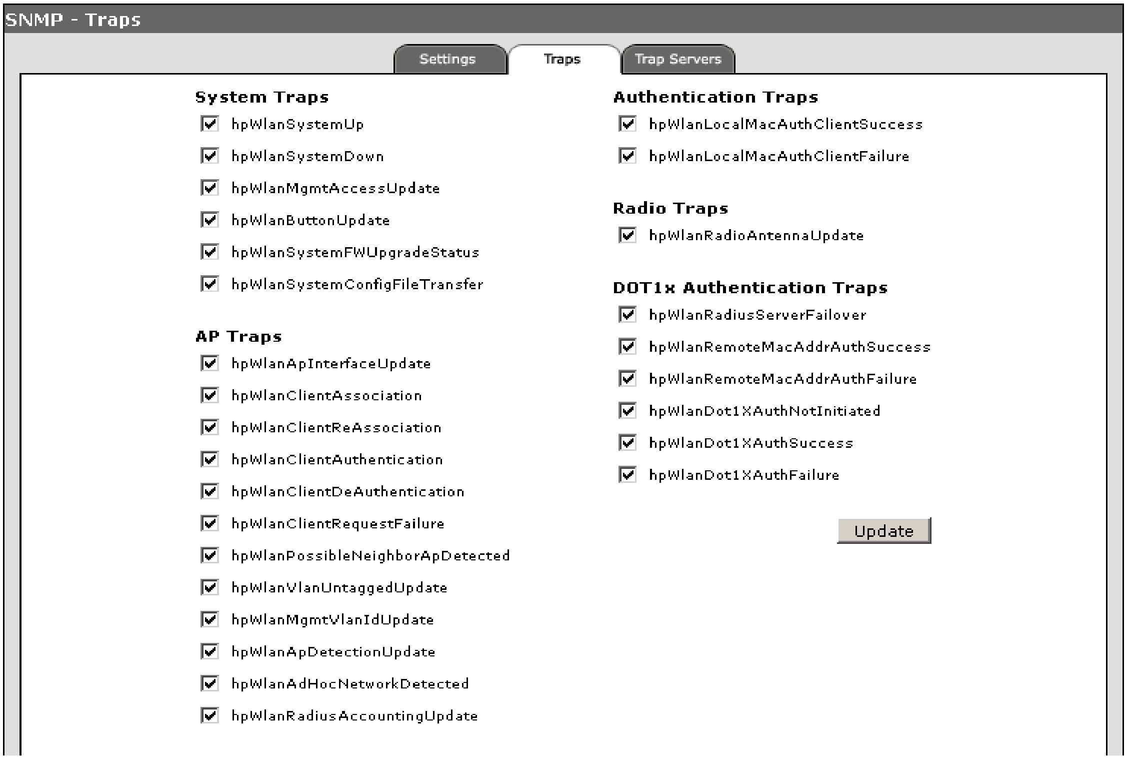
  - **hpWlanClientRequestFailure** – The station request failure is sent when a station fails to associate / re-associate / authenticate with the access point. The notification includes the station MAC address and the reason code for the failure.
  - **hpWlanPossibleNeighborApDetected** – This notification is sent when any access point is detected.
  - **hpWlanVlanUntaggedUpdate** – This notification is sent when the VLAN Id is set to untagged.
  - **hpWlanMgmtVlanIdUpdate** – This notification is sent if the management VLAN ID is changed.
  - **hpWlanApDetectionUpdate** – This notification is sent when AP detection scan is set to Enable/Disable.
  - **hpWlanAdHocNetworkDetected**– This notification is sent when adHoc is detected with BSSID.
  - **hpWlanRadiusAccountingUpdate** –This notification is sent when Radius Accounting is set to Enable/Disable.

- **Authentication Traps:** pertaining to local authentication.
  - **hpWlanLocalMacAuthstationsuccess** – This notification is sent when a station successfully authenticates the MAC address with the database stored locally within the access point. The notification value includes the MAC address of the authenticated station.
  - **hpWlanLocalMacAuthClientFail** – This notification is sent when a station fails to authenticate the MAC address with the database stored locally within the access point. The notification value includes the MAC address of the authenticated station.
- **Radio Traps:** pertaining to maintaining the access point radio.
  - **hpWlanRadioAntennaUpdate** – This notification is sent when the antenna configuration is changed.
- **DOT1X Authentication Traps:** pertaining to Dot1X authentication.
  - **hpWlanRadiusServerFailover**–This notification is sent when the RADIUS server changes from Primary to Secondary and vice versa.
  - **hpWlanRemoteMacAuthstationsuccess** – This notification is sent when a station successfully authenticates the MAC address with the RADIUS server. The notification value includes the MAC address of the authenticated station.
  - **hpWlanRemoteMacAuthClientFail** –This notification is sent when a station fails to authenticate the MAC address with the RADIUS server. The notification value includes the MAC address of the station that failed to authenticate.

- **hpWlanDot1XAuthNotInitiated**– This notification is sent when a station did not initiate 802.1X authentication with the RADIUS server. The notification value includes the MAC address of the station that did not initiate 802.1X authentication.
- **hpWlanDot1XAuthSuccess** – This notification is sent when a station successfully authenticates with the RADIUS server. The notification value includes the MAC address of the authenticated station.
- **hpWlanDot1XAuthFailure** –This notification is sent when a station fails to authenticate with the RADIUS server. The notification value includes the MAC address of the station that failed to authenticate.

The Trap Servers tab allows configuration of the following SNMP trap parameters:

- **Trap Destination Host (1 to 3):** Enables/Disables recipients (up to three) of SNMP notifications. For each destination, enter the IP address or the host name, and the community name.
- **IP Address:** Specifies the IP address or the host name (from 1 to 20 characters) for the recipient of SNMP notifications.
- **Community Name:** The community string sent with the notification operation. (Maximum length: 32 characters)
- **[Update]:** Updates the Trap settings.



System Traps

☑ hpWlanSystemUp
☑ hpWlanSystemDown
☑ hpWlanMgmtAccessUpdate
☑ hpWlanButtonUpdate
☑ hpWlanSystemFWUpgradeStatus
☑ hpWlanSystemConfigFileTransfer

AP Traps

☑ hpWlanApInterfaceUpdate
☑ hpWlanClientAssociation
☑ hpWlanClientReAssociation
☑ hpWlanClientAuthentication
☑ hpWlanClientDeAuthentication
☑ hpWlanClientRequestFailure
☑ hpWlanPossibleNeighborApDetected
☑ hpWlanVlanUntaggedUpdate
☑ hpWlanMgmtVlanIdUpdate
☑ hpWlanApDetectionUpdate
☑ hpWlanAdHocNetworkDetected
☑ hpWlanRadiusAccountingUpdate

Authentication Traps

☑ hpWlanLocalMacAuthClientSuccess
☑ hpWlanLocalMacAuthClientFailure

Radio Traps

☑ hpWlanRadioAntennaUpdate

DOT1x Authentication Traps

☑ hpWlanRadiusServerFailover
☑ hpWlanRemoteMacAddrAuthSuccess
☑ hpWlanRemoteMacAddrAuthFailure
☑ hpWlanDot1XAuthNotInitiated
☑ hpWlanDot1XAuthSuccess
☑ hpWlanDot1XAuthFailure

To Enable SNMP Traps:

1. Select Management > SNMP > Traps tab.
2. Under the Trap Groups, select or clear the **required traps**.
3. Click **[Update]** to set specified traps.

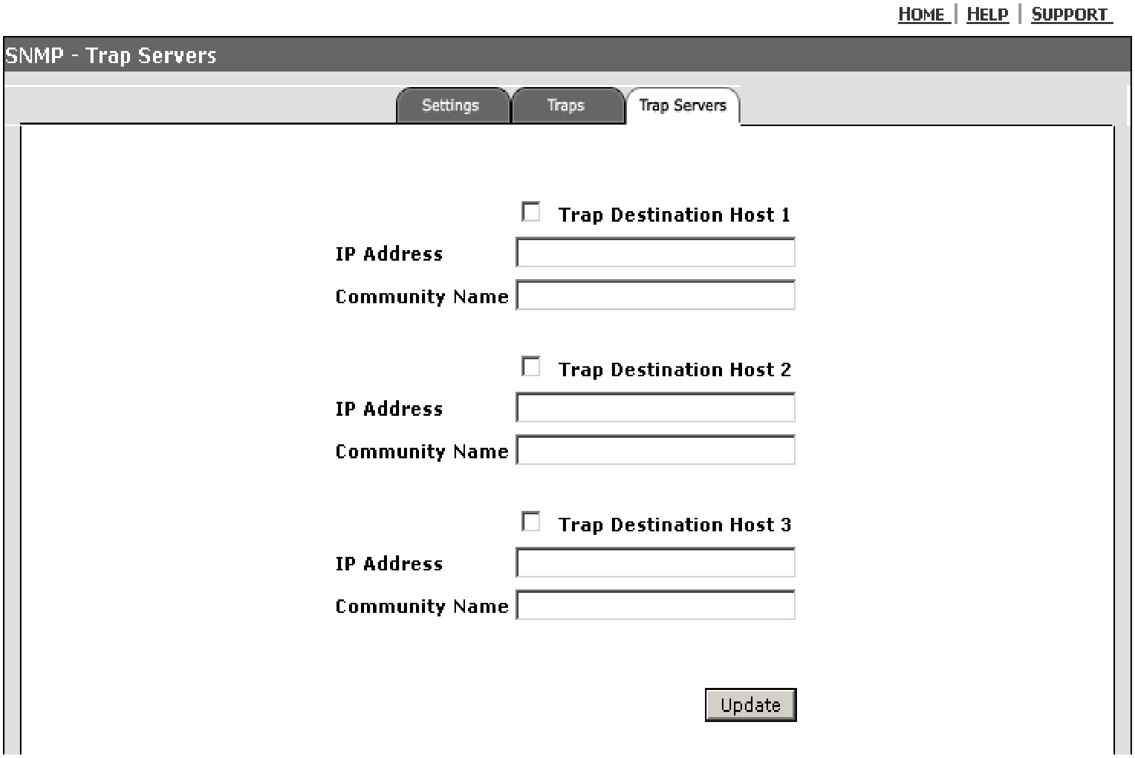


Figure 5-5. Configuring SNMP Trap Destinations

To Configure SNMP Trap Destinations:

1. Select Management > SNMP > Trap Servers tab.
2. To set trap destinations, select **Trap Destination Host 1, 2, or 3.**
3. Type the **IP address** in the Trap Destination IP Address text-field and specify one of the **configured community names** in the Community Name text-field.
4. Click **[Update]** to set SNMP Trap destinations.

CLI: Configuring SNMP v1 and v2c Trap Destinations

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] snmp-server host *<host_ip_address | host_name> <community-string>*	9-38
show snmp-server	9-40

To send SNMP v1 and v2c traps to a management station, specify the host IP address using the **snmp-server host** command and enable specific traps using the **snmp-server trap** command.

```
ProCurve Access Point 530(config)#snmp-server host 1 192.168
.1.15
ProCurve Access Point 530(config)#snmp-server host 2 192.168
.1.19
ProCurve Access Point 530#
```

To display the current SNMP settings from the Manager Exec level, use the **show snmp-server** command, as shown in the following example.

```
ProCurve Access Point 530(config)#show snmp-server
SNMP Server Settings
---------------------------------------------------------------------------
SNMP Status       Enabled
SNMP Port         161
Community (ro)    public
Community (rw)    private
Location          not set
Contact           not set

Trap Destinations
Host      Community
-----------------------
1         192.168.1.15
2         192.168.1.19

hpWlanAdHocNetworkDetected        Enabled   hpWlanApDetectionUpdate    Enabled
hpWlanRadioAntennaUpdate          Enabled   hpWlanButtonUpdate         Enabled
hpWlanClientAssociation           Enabled   hpWlanApInterfaceUpdate    Enabled
hpWlanClientDeAuthentication      Enabled   hpWlanClientAuthentication Enabled
hpWlanClientRequestFailure        Enabled   hpWlanClientReAssociation  Enabled
hpWlanDot1XAuthNotInitiated       Enabled   hpWlanDot1XAuthFailure     Enabled
hpWlanLocalMacAuthClientFailure   Enabled   hpWlanDot1XAuthSuccess     Enabled
hpWlanLocalMacAuthClientSuccess   Enabled   hpWlanMgmtAccessUpdate     Enabled
hpWlanPossibleNeighborApDetected  Enabled   hpWlanMgmtVlanIdUpdate     Enabled
hpWlanRadiusAccountingUpdate      Enabled   hpWlanRadiusServerFailover Enabled
hpWlanRemoteMacAddrAuthFailure    Enabled   hpWlanSystemUp             Enabled
hpWlanRemoteMacAddrAuthSuccess    Enabled   hpWlanSystemDown           Enabled
hpWlanSystemFWUpgradeStatus       Enabled   hpWlanVlanUntaggedUpdate   Enabled
hpWlanSystemConfigFileTransfer    Enabled

ProCurve Access Point 530(config)#
```

Enabling System Logging

The access point supports a logging process that can control error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating access point and network problems.

The following table lists the error message levels from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level.

Error Level	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

The access point error log can be viewed using the Web interface. The Web interface displays the last 128 messages logged in chronological order, from the newest to the oldest.

Log messages are only generated since the last reboot. Rebooting the access point erases all previous log messages. Consider configuring the access point to log messages to a Syslog server (see "CLI: Setting Logging Parameters" on page 5-37).

Web: Setting Logging Parameters

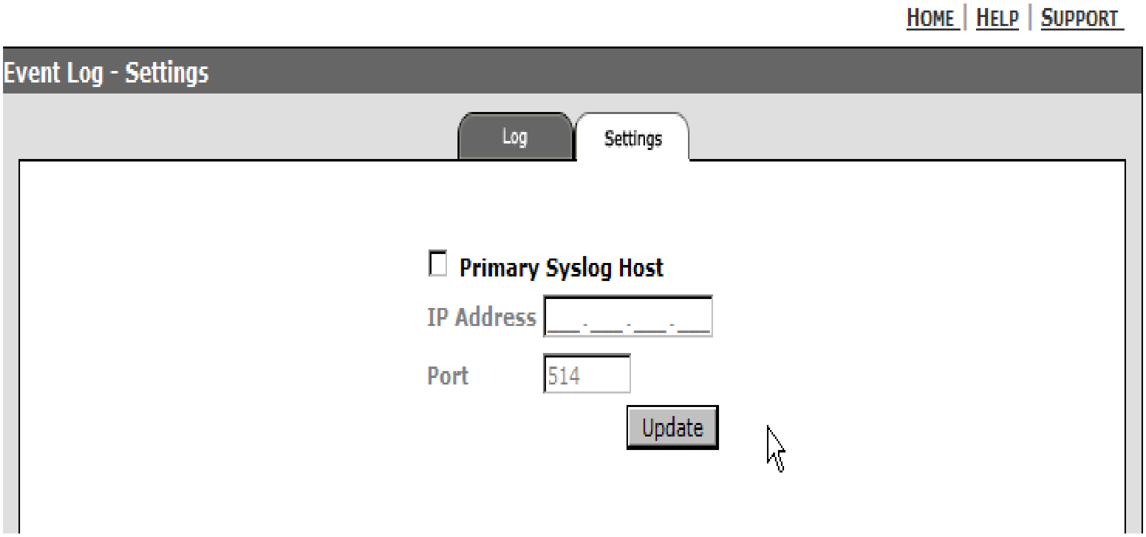
The Settings window from the Device Information tab enables system logs and Syslog server details to be configured for the access point.

The Web interface enables you to modify these parameters:

- **Primary Syslog Host:** Enables the logging of error messages.
- **IP Address:** The IP address of a Syslog server.
- **Port**: The UDP port used by a Syslog server. (Default is 514).
- **[Update]:** Updates the logging settings.

Note

To view log messages generated by the access point, select the Log tab on the Event Log page. See "Event Log" on page 4-26.



Event Log - Settings

☐ Primary Syslog Host

IP Address: ___.___.___.___

Port: 514

Figure 5-6. Setting Logging Parameters

To Enable Logging:

1. Select Device Information > Event Log > Settings tab.
2. Check **Primary Syslog Host** to enable the system log setup.
3. Enter the **IP address** of the Syslog server.
4. Set the **Relay port** used by the Syslog server.
5. Click **[Update]** to update logging settings on the access point.

CLI: Setting Logging Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
log	9-30
[no] logging <syslog_host >[syslog_port]	9-31
show debug	9-32
show logging	9-32

The following example shows how to set an IP address for the receiving syslog server using the **logging** command.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#logging 10.1.0.3

ProCurve Access Point 530(config)#
```

The following example shows the syslog settings.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#show debug
Debug Logging:
Syslog Relay    10.1.0.3 (port 514)

ProCurve Access Point 530(config)#
```

The following example shows the security level of entries.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#show logging
 Keys:   M=eMergency   C=Critical   W=Warning   I=Information
         A=Alert       E=Error      N=Notice    D=Debug
-----  Event Log Listing: Most Recent Events First  ----
I 01/10/00 20:39:09 login[12763]: root login  on `ttyp0'

I 01/08/00 06:22:55 login[12095]: root login  on `ttyp0'

I 01/07/00 05:00:43 login[11285]: root login  on `ttyp0'

I 01/05/00 19:17:45 login[9013]: root login  on `ttyp0'

I 01/05/00 05:35:48 syslog: wlan1: RADIUS Authentication server 127.0.0.1:1812
I 01/05/00 05:35:41 syslog: wlan1: RADIUS Authentication server 127.0.0.1:1812
I 01/05/00 05:34:04 syslog: wlan1: RADIUS Authentication server 127.0.0.1:1812
I 01/05/00 05:30:45 login[8495]: root login  on `ttyp0'

I 01/05/00 01:29:27 login[6498]: root login  on `ttyp0'

I 01/05/00 01:25:45 login[6491]: root login  on `ttyp0'

I 01/05/00 00:08:06 login[6389]: root login  on `ttyp0'

I 01/04/00 18:50:44 login[5855]: root login  on `ttyp0'

I 01/04/00 00:23:40 login[1969]: root login  on `ttyp0'

I 01/03/00 06:18:29 login[1767]: root login  on `ttyp0'

N 01/01/00 00:00:35 mini_httpd-ssl[577]: mini_httpd/1.17beta1 26may2002 startin
g on ProCurve-AP-530, port 80

ProCurve Access Point 530#
```

Configuring SNTP

Simple Network Time Protocol (SNTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an SNTP client in unicast mode, periodically sending time synchronization requests to specific time servers. The access point will attempt to poll each server in the configured sequence.

SNTP is **disabled** by default.

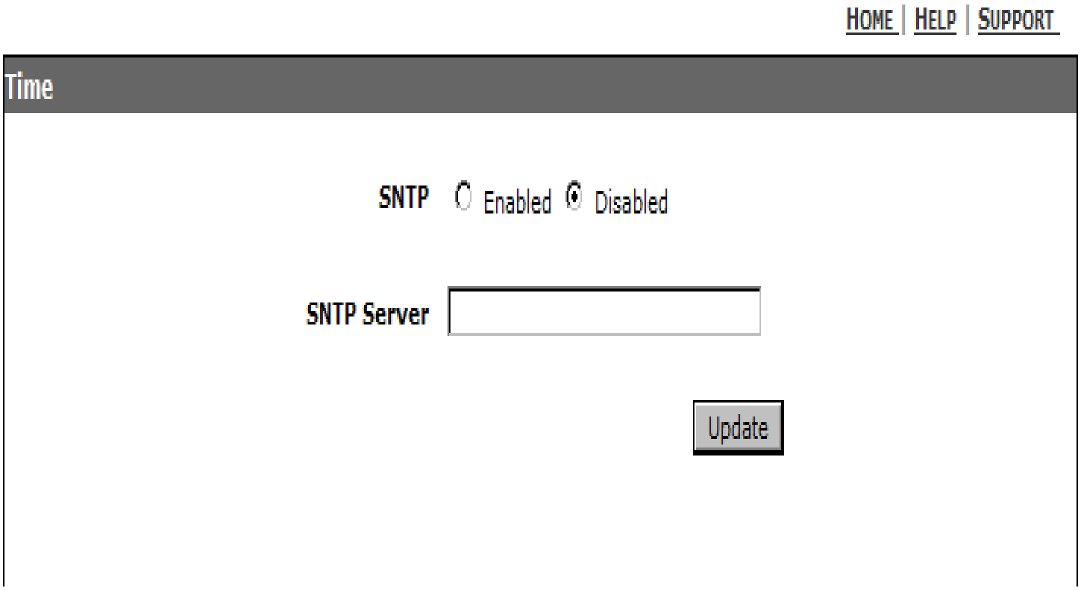
Universal Time. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude.

Web: Setting SNTP Parameters

The SNTP on the Special Features tab enables the SNTP server and time zone details to be configured for the access point.

The Web interface enables you to modify these parameters:

- **SNTP:** Enables/Disables the access point to operate as an SNTP unicast client. When enabled, at least one time server IP address or host name (recommended) must be specified. (Default is Disabled)
- **SNTP Server:** The IP address or hostname of an SNTP server that the access point attempts to poll for a time update.
- **[Update]:** Updates the SNTP settings on the access point.



SNTP ○ Enabled ● Disabled

SNTP Server

Figure 5-7. Configuring SNTP Settings

To Set SNTP Parameters:

1. Select Special Features > Time.
2. For **SNTP**, select **enabled**.
3. For the SNTP Server, type the **IP address** or the **hostname** in the **SNTP Server** text field.
4. Click **[Update]** to set the SNTP parameters.

CLI: Setting SNTP Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
sntp <*server*>	9-34
[no] sntp	9-34
show sntp	9-35

The following example shows how to enable SNTP and configure a server IP address by using the **sntp** <*server*> command.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#sntp 10.1.0.19

ProCurve Access Point 530(config)#
```

To display the current SNTP status, use the **show sntp** command, as shown in the following example.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#show sntp
---------------------------------------------------------
Status               : up
Server               : 10.1.0.19

ProCurve Access Point 530(config)#
```

Configuring RADIUS Accounting

Remote Authentication Dial-in User Service (RADIUS) Accounting is an extension to the RADIUS authentication protocol that uses a central server to log user activity on the network. A RADIUS Accounting server runs software that receives user-session information from the access point. The data collected by the server not only provides the information for billing and auditing, but also allows network administrators to monitor usage trends and plan for network growth.

NOTE

This configuration guide assumes that you have already configured the RADIUS Accounting server(s) to support the access point. The configuration of RADIUS Accounting software is beyond the scope of this guide, refer to the documentation provided with the RADIUS Accounting software.

The user-session information provided by the access point is sent to the server using standard RADIUS Accounting attributes (refer to RFC 2866). The following describes the RADIUS attributes supported by the access point.

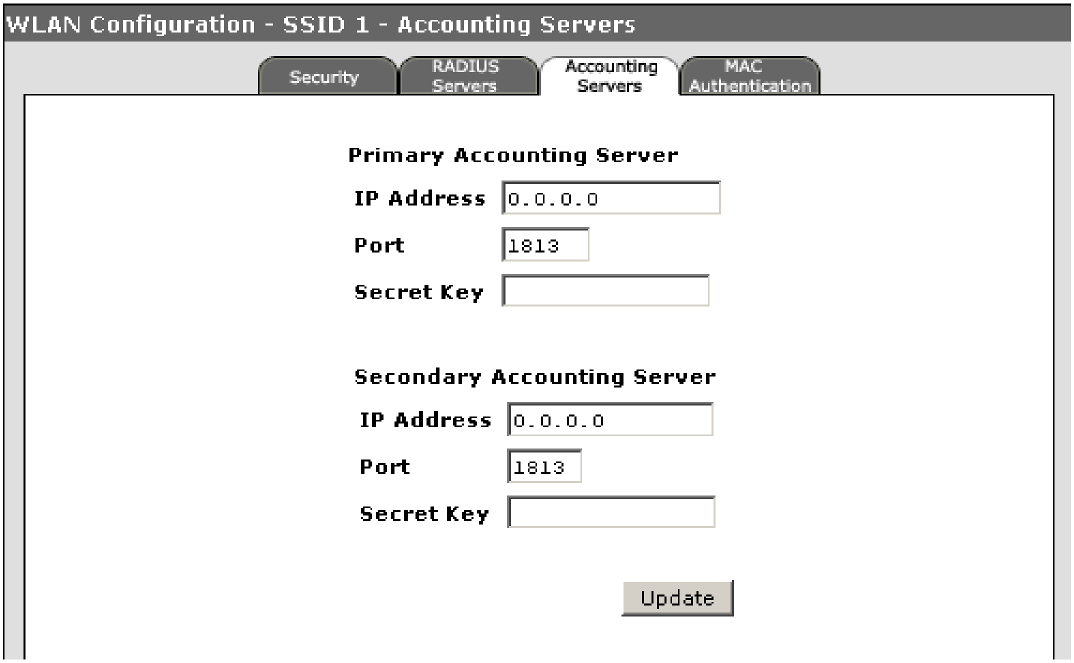
RADIUS Accounting Attribute	Description
Acct-Status-Type	Contains the RADIUS Accounting message type: • Start • Stop • Interim-Update • Accounting-On • Accounting-Off
Acct-Delay-Type	Contains the cumulative delay type for the session
Acct-Input-Octets	Contains the cumulative input byte count for the session
Acct-Output-Octets	Contains the cumulative output byte count for the session
Acct-Session-Id	Contains a unique Accounting ID for a given session
Acct-Authentic	Indicates how the user was authenticated
Acct-Session-Time	Contains the time in seconds that the user has received service
Acct-Input-Packets	Contains the cumulative input packet count for the session
Acct-Output-Packets	Contains the cumulative output packet count for the session
Acct-Terminate-Cause	Specifies how the session was terminated

Web: Setting RADIUS Accounting Server Parameters

The Accounting Servers tab provides setting of the primary and secondary server parameters on the RADIUS Accounting server. This configures the RADIUS Accounting servers to which the access point RADIUS server transmits user-session information. For the configuration of the RADIUS Servers, see "Web: Setting RADIUS Server Parameters" on page 7-28.

The Web interface allows modification of these parameters to use RADIUS Authentication on the access point:

- **Primary Accounting Server:** Enables configuration of a RADIUS Accounting server in the network for RADIUS authentication transmission from the access point.
  - **IP Address:** Specifies the IP address of the RADIUS Accounting server (Default is 0.0.0.0, which indicates disabled).
  - **Port:** The User Datagram Protocol (UDP) port number used by the RADIUS Accounting server for accounting messages. Setting the port number to zero disables RADIUS Accounting. (Default is 1813).
  - **Secret Key:** A shared text string used to encrypt messages between the access point and the RADIUS Accounting server. **Be sure that the same text string is specified on the RADIUS server.** Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Secondary Accounting Server:** Configure a secondary RADIUS Accounting server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role. (Default is Disabled)



WLAN Configuration - SSID 1 - Accounting Servers

Primary Accounting Server

IP Address 0.0.0.0

Port 1813

Secret Key

Secondary Accounting Server

IP Address 0.0.0.0

Port 1813

Secret Key

Figure 5-8. Configuring RADIUS Accounting Servers

To Set RADIUS Accounting Server Parameters:

1. Select Network Setup > WLANs > **[Edit]** button **>** Accounting Servers tab.
2. For the primary RADIUS Accounting server, type the **IP address** in the IP text field. (Default is 0.0.0.0, which indicates disabled).
3. In the Port text field, specify the UDP **port number** used by the RADIUS Accounting server. (Default is 1813)
4. In the Secret Key text field, specify the shared **text string** that is also used by the RADIUS server.
5. (Optional) If you need to configure a secondary RADIUS Accounting server in the network, specify its IP address and other parameters in the appropriate fields. Otherwise, leave the IP address as all zeros (0.0.0.0).
6. Click **[Update]** to set the RADIUS Accounting servers for RADIUS authentication.

CLI: Enabling RADIUS Accounting Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] radius-accounting <primary | secondary> <ip *<ip>* | port *<port>* | key *<key>*>	9-53

The following example shows how to enable RADIUS Accounting and set the ip address, port number, and the secret key on the access point.

Note

Enter radius commands, one per line.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radius-accounting primary
ip 192.168.1.52
ProCurve Access Point 530(config)#radius-accounting primary
port 161
ProCurve Access Point 530(config)#radius-accounting primary
key blue
ProCurve Access Point 530(config)#
```

Setting Up Filter Control

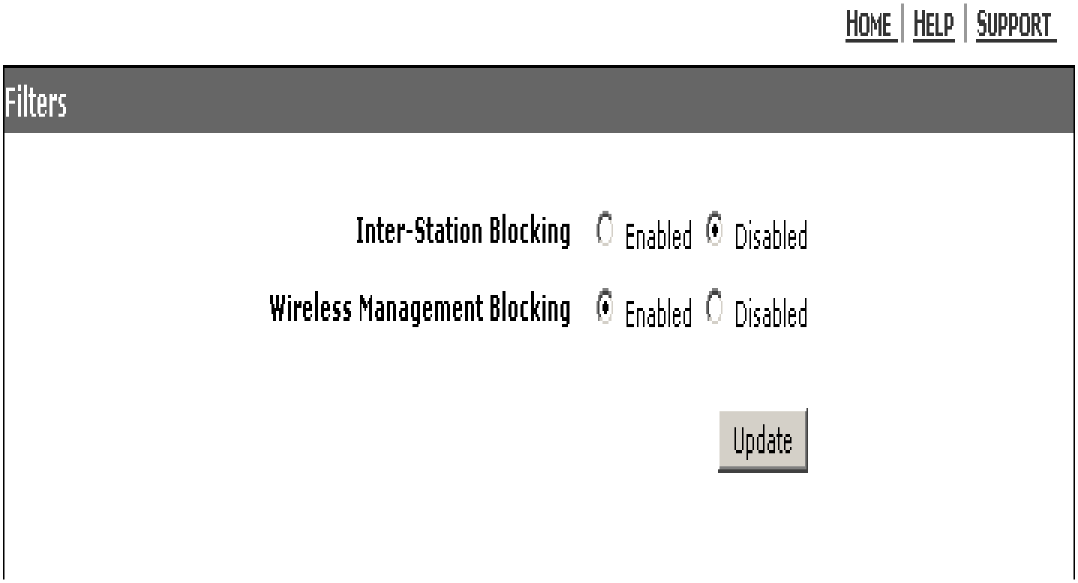
You can prevent communications between wireless stations associated to the access point, only allowing traffic between stations and the wired network. You can also prevent any wireless client from performing any access point configuration through any of its management interfaces, including Web, Telnet, or SNMP access.

Web: Setting Traffic Filters

The Filters on the Special Features tab enables the traffic filters to be set.

The Web interface enables you to modify these parameters:

- **Inter-Station Blocking:** Enables/Disables the blocking of communications between wireless stations. (Default is Disabled)
- **Wireless Management Blocking:** Enables/Disables the blocking of a wireless station's access to the access point.
- **[Update]:** Updates the SNTP settings on the access point.



Inter-Station Blocking ○ Enabled ● Disabled

Wireless Management Blocking ● Enabled ○ Disabled

Figure 5-9.   Configuring Traffic Filters

To Set Traffic Parameters:

1. Select Special Features > Filters tab.
2. For Inter-Station Blocking, select **enabled**.
3. For Wireless Management Blocking, select **enabled**.
4. Click **[Update]** to set the Traffic parameters.

CLI: Setting Traffic Filters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] inter-station-blocking	9-63
[no] wireless-mgmt-block	9-63
show filters	9-64

The following example shows how to block communications between wireless stations.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#inter-station-blocking
ProCurve Access Point 530(config)#
```

The following example shows how to block wireless stations from gaining management access to the access point.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#wireless-mgmt-block
ProCurve Access Point 530(config)#
```

The following example shows the enabled filters.

```
ProCurve Access Point 530#show filters
------------------------------------------------------------
Traffic/Security Filters:
Wireless Management Blocking   Enabled
Inter-Station Blocking         Disabled
ProCurve Access Point 530#
```

Configuring VLAN Support

A Virtual Local Area Network (VLAN) is a location independent broadcast domain. A VLAN is like the standard definition of a LAN without the physical constraints. These VLAN domains are a collection of workstations that are part of the same logical, working community but not likely part of the same physical community. The goal of VLANs is to allow for complete mobility and flexibility of workstation placement, yet keeping cross domain broadcast traffic to a minimum.

In large networks, VLANs are used to organize network nodes to reflect departmental (such as Marketing or R&D) or usage groups (such as guests). The VLANs are defined by software in switches and other devices across the enterprise network. VLANs help to simplify network management by allowing nodes to be moved to a new VLAN without having to change any physical connections.

VLANs confine broadcast traffic to the originating group, which helps prevent broadcast storms and provides a cleaner and more secure network environment. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

The access point can enable the support of VLAN-tagged traffic passing between wireless stations and the wired network. This VLAN tagging extends the wired network's VLANs to wireless stations. Associated stations are assigned to a VLAN and can only send and receive traffic within that VLAN. This enables the access point to provide secure support for different wireless users with various levels of network access and permissions.

VLAN assignments and SSID. The details on VLAN and SSID configuration are presented in a separate section, see"Managing Multiple WLAN (BSS/SSID) Interfaces" on page 6-26.

Client VLAN Assignment. The access point supports both "static" and "dynamic" VLAN assignment for wireless stations. Dynamic VLAN assignment is limited by the number of stations per radio (256). If the maximum number of wireless stations connected on each radio and each of those stations had a dynamic VLAN, there would be a limit of 512 dynamic VLANs (because of the limit on wireless stations). If stations are not assigned to a specific VLAN, they are assigned to the default VLAN of the associated SSID interface.

Management VLAN. A management VLAN can be configured for secure management access to the access point. The management VLAN is for managing the access point through remote management tools, such as the Web interface, SSH, Telnet, or SNMP. The access point only accepts management traffic that is tagged with the specified management VLAN ID.

Tagged and Untagged VLANs. VLAN support is always enabled on the access point and can not be disabled. Traffic passed to the wired network is tagged with the appropriate VLAN ID, either an assigned client VLAN ID, a default VLAN ID, or the management VLAN ID. By default, only one untagged VLAN ID is configured. Traffic passed to the wired network from the untagged VLAN does not include a VLAN tag.

Similarly, traffic received from the wired network must be tagged with a known VLAN ID, either an assigned client VLAN ID, a default VLAN ID, or the management VLAN ID. Received traffic that has no tag is passed to the access point's untagged VLAN, if configured, otherwise it is dropped. Received traffic that has an unknown VLAN ID or is tagged with the VLAN ID of the configured untagged VLAN is dropped.

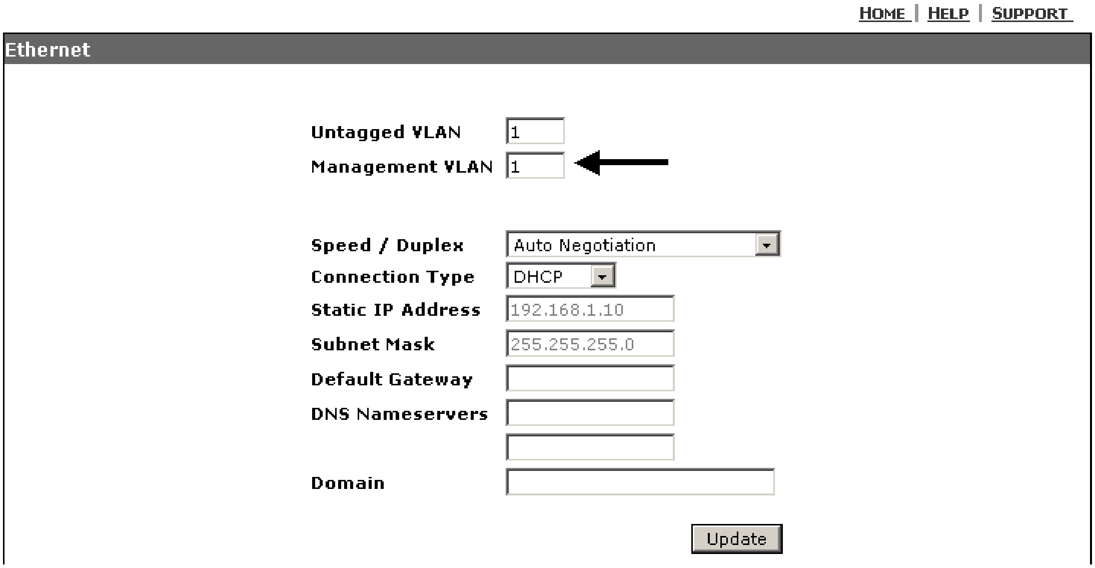
As part of ensuring appropriate VLAN support, configure the attached network switch port to support IEEE 802.1Q tagged VLAN frames from the access point's management VLAN ID, default VLAN IDs, and other client VLAN IDs.

Web: Setting A Management VLAN

Access the Ethernet window through the Network Setup tab to update a management VLAN ID.

The Web interface enables you to modify these parameters:

- **Management VLAN:** Indicates the VLAN that will be used to route all management traffic to and from the access point. (Default is 1)
- **[Update]:** Updates the Management VLAN.



Untagged VLAN 1
Management VLAN 1
Speed / Duplex Auto Negotiation
Connection Type DHCP
Static IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Gateway
DNS Nameservers
Domain

Figure 5-10. Setting A Management VLAN

To Set A Management VLAN:

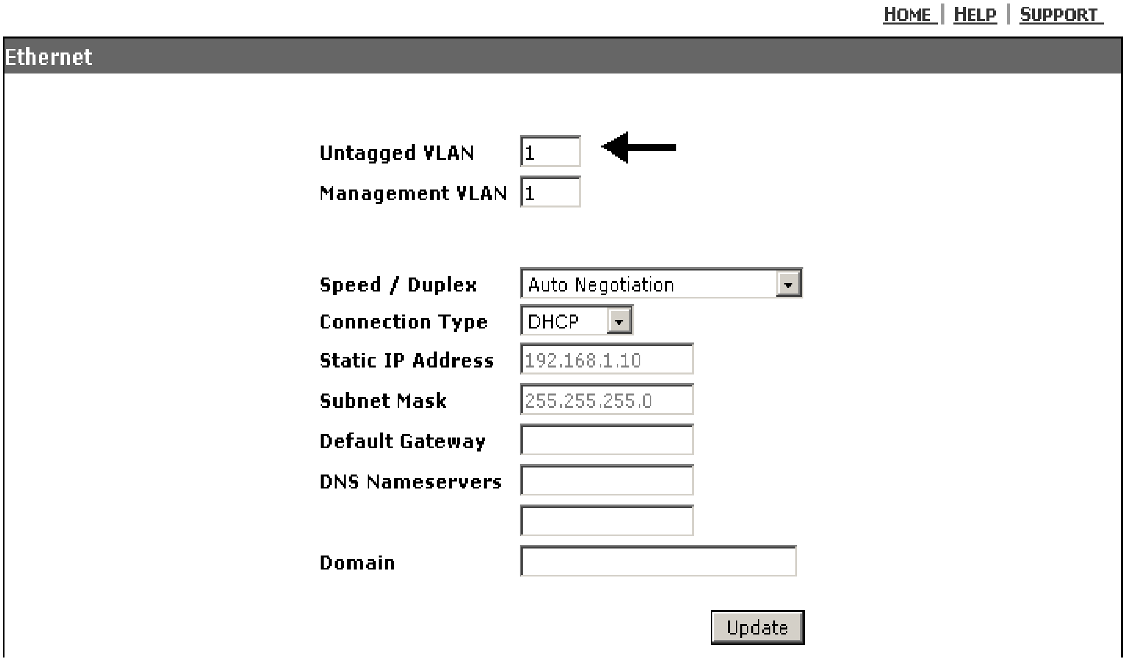
1. Select Network Setup> Ethernet tab.
2. To set the Management VLAN, type a **valid number** between 1 and 4094 in the Management VLAN ID text field.
3. Click **[Update]** to enable the management VLAN.

Web: Changing the Untagged VLAN ID

Access the Ethernet window through the Network Setup tab to change the untagged VLAN ID.

The Web interface enables you to modify these parameters:

- **Untagged VLAN:** Allows setting of a VLAN ID to which all untagged packets will be assumed to belong. The range is 1-4094. (Default is 1).
- **Connection Type:** Allows selection of a static or DHCP setting. See“Web: Configuring IP Settings Statically or via DHCP” on page 5-18.
- **[Update]:** Updates the VLAN settings.



Untagged VLAN 1

Management VLAN 1

Speed / Duplex Auto Negotiation

Connection Type DHCP

Static IP Address 192.168.1.10

Subnet Mask 255.255.255.0

Default Gateway

DNS Nameservers

Domain

Figure 5-11. Changing Untagged VLAN ID

To Set Untagged VLAN ID:

1. Select Network Setup > Ethernet.
2. To set the untagged VLAN, type a **valid number** between 1 and 4094 in the VLAN ID text field.
3. Click **[Update]** to enable the internal network as a VLAN.

CLI: Enabling VLAN Support

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
vlan	9-116
[no] untagged-vlan *<vid>*	9-117
management-vlan *<vid>*	9-117
show wlans	9-93

The following example shows how to establish a management VLAN ID.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface ethernet
ProCurve Access Point 530(ethernet)# management-vlan 9
ProCurve Access Point 530(ethernet)#
```

The following example shows how to set an untagged VLAN ID in the interface context.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface ethernet
ProCurve Access Point 530(ethernet)# untagged-vlan 9
ProCurve Access Point 530(ethernet)#
```

The following example shows how to set a tagged VLAN at the WLAN context.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#wlan 1
ProCurve Access Point 530(radio1-wlan1)#vlan 3
ProCurve Access Point 530(radio1-wlan1)#
```

The following example displays the management VLAN ID. The static or dynamic VLAN state is configured per WLAN and can be validated using the show wlans command.

```
ProCurve Access Point 530# show wlans
All WLANs on Radio 1:
#   WLAN                          BSSID              VLAN     Security Status
------------------------------------------------------------------------------
1   SSID 1                    00:14:C2:BE:05:50  9   (U)  None     Enabled
2   SSID 2                    not assigned yet   none(-)  None     Disabled
3   SSID 3                    not assigned yet   none(-)  None     Disabled
4   SSID 4                    not assigned yet   none(-)  None     Disabled
5   SSID 5                    not assigned yet   none(-)  None     Disabled
6   SSID 6                    not assigned yet   none(-)  None     Disabled
7   SSID 7                    not assigned yet   none(-)  None     Disabled
8   SSID 8                    not assigned yet   none(-)  None     Disabled
9   SSID 9                    not assigned yet   none(-)  None     Disabled
10  SSID 10                   not assigned yet   none(-)  None     Disabled
11  SSID 11                   not assigned yet   none(-)  None     Disabled
12  SSID 12                   not assigned yet   none(-)  None     Disabled
13  SSID 13                   not assigned yet   none(-)  None     Disabled
14  SSID 14                   not assigned yet   none(-)  None     Disabled
15  SSID 15                   not assigned yet   none(-)  None     Disabled
16  SSID 16                   not assigned yet   none(-)  None     Disabled
All WLANs on Radio 2:
#   WLAN                          BSSID              VLAN     Security Status
------------------------------------------------------------------------------
1   SSID 1                     00:14:C2:A5:22:F0  9   (U)  No Sec.  Enabled
2   SSID 2                     not assigned yet   none(-)  No Sec.  Disabled
3   SSID 3                     not assigned yet   none(-)  No Sec.  Disabled
4   SSID 4                     not assigned yet   none(-)  No Sec.  Disabled
5   SSID 5                     not assigned yet   none(-)  No Sec.  Disabled
6   SSID 6                     not assigned yet   none(-)  No Sec.  Disabled
7   SSID 7                     not assigned yet   none(-)  No Sec.  Disabled
8   SSID 8                     not assigned yet   none(-)  No Sec.  Disabled
9   SSID 9                     not assigned yet   none(-)  No Sec.  Disabled
10  SSID 10                    not assigned yet   none(-)  No Sec.  Disabled
11  SSID 11                    not assigned yet   none(-)  No Sec.  Disabled
12  SSID 12                    not assigned yet   none(-)  No Sec.  Disabled
13  SSID 13                    not assigned yet   none(-)  No Sec.  Disabled
14  SSID 14                    not assigned yet   none(-)  No Sec.  Disabled
15  SSID 15                    not assigned yet   none(-)  No Sec.  Disabled
16  SSID 16                    not assigned yet   none(-)  No Sec.  Disabled
ProCurve Access Point 530#
```

6

Wireless Interface Configuration

Contents

Overview

The Access Point 530 supports up to 16 Service Set IDentifier (SSID) interfaces. Most radio parameters apply globally to all configured SSID interfaces. For each SSID interface, different security settings, VLAN assignments, and other parameters can be applied.

This Chapter describes how to:

- Set the access point country code
- Configure the radio working mode
- Modify global radio parameters
- Configure SSID interfaces

Setting the Country Code

This section details setting the country code in both the Access Point 530 WW unit (J8987A), which has no preset country code and the Access Point 530 NA unit (J8986A), which has the country code preset to the "US". The country code is an identifier defined for a nation by ISO. For each nation, ISO Standard 3166 defines a unique two-character alphabetic code. Among many uses of these codes, the two-character codes are used as top-level domain names

A correct country code must be set for the country in which you operate the access point, so that it uses the correct authorized radio channels for wireless network devices. The country code can be set using the CLI.

The Country Code must be set before configuring other radio settings. This setting affects the radio channels that are available.

Note

The Country Code is preset to "US" in the Access Point 530 NA unit and can only be changed from the "US" to either Canada, Mexico, or Taiwan country codes. Once set to either Canada, Mexico, or Taiwan and you wish to reset to the "US", you must reset the unit back to factory defaults.

The radios are disabled if the Country Code is not set. Once the Country Code is set, the radios can be enabled.

When resetting to factory defaults, the Access Point 530 WW unit must have its Country Code set. The Access Point 530 NA will be set to "US".

CLI: Setting the Country Code

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
country <*country_code*>	9-17
write mem	9-17
show system-information	9-27

The following example uses the **country code** command to set the access point to United Kingdom (GB). For a list of available country codes, see "System Management Commands" on page 9-16.

Note

You do not need to perform a system reboot to set the Country Code! You should use the 'write mem' command to save the country code.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# country GB
ProCurve Access Point 530(config)# write mem
```

The following example shows how to use the **show system-information** command to return the access point's current values, including the Country Code.

```
ProCurve Access Point 530(config)# show system-information
-------------------------------------------------------------------
Serial Number         TW547VV007
System Name           ProCurve-AP-530
System Up Time        5 hours 18 mins 19 secs
System Location       not set
System Country Code   us
Software Version      WA.01.00
Ethernet MAC Address  00:14:C2:A5:08:CB
IP Address            192.168.15.100
Subnet Mask           255.255.255.0
Default Gateway       192.168.15.1
DHCP Client           Enabled
Management VLAN ID    1
Untagged-VLAN ID      1
Radio 1 MAC Address   00:14:C2:A5:22:E0
Radio 1 Status        Disabled (802.11g)
Radio 2 MAC Address   00:14:C2:A5:22:F0
Radio 2 Status        Disabled (802.11a)
HTTP Interface        Enabled
SSL Interface         Enabled
SSH Interface         Enabled
Telnet Interface      Enabled
Serial Interface      Enabled

ProCurve Access Point 530(config)#
ProCurve Access Point 530#
```

Configuring the Radio

Radio settings directly control the behavior of the radio device in the access point. The access point allows modification of various radio parameters, such as; enabling the radio, radio working mode, radio broadcasting channel, and transmit power level.

To enhance the access point's performance, the following table summarize key points to consider when configuring the radio parameters.

CAUTION

When access point configuration parameters are changed, wireless stations may be temporarily disconnected until the new configuration parameter is enabled. This includes any changes to a WLAN or radio parameter.

Table 6-1. Radio Configuration Summary Table

Summary Point	Parameters
There are three wireless LAN modes available for use on the 530 access point	802.11a, 802.11b, and 802.11g
There are two separate wireless LAN radios available for use on the 530 access point.	Radio 1 and Radio 2
Radio 1 configuration allows only two modes.	802.11b and 802.11g
Radio 2 configuration allows all three modes.	802.11a, 802.11b, and 802.11g
If Radio 1 and Radio 2 are both configured to 802.11 b/g mode, then Radio 2 must be connected to an external antenna.	802.11 b/g mode for both Radio 1 and 2. Requires external antenna configuration for Radio 2.
Each radio operates on one channel at a time.	
• This channel may be predetermined and fixed by the operator.	Channel-Policy = Static
• This channel can be automatically selected by the radio, depending on what channels are already being used by other access points.	Channel-Policy = Auto
The radio operates in the 2.4 GHz to 2.5 GHz spectrum, when set in these two modes.	802.11b and 802.11g mode
The radio operates in the 5 GHz to 6 GHz spectrum, if set in this mode.	802.11a

Summary Point	Parameters
Since they are in different parts of the spectrum, the channels within these modes do not interfere with one another.	802.11b and 802.11a channels. 802.11g and 802.11a channels.
Each radio that is used, no matter what the mode, must be set to a unique channel to avoid interference with other radios in the same area.	All modes (802.11a, 802.11b, and 802.11g).
There is much channel overlapping in these modes because they share the same 2.4 GHz spectrum and use the same channels. To avoid overlapping, there must be a separation of at least five channels between operating channels (e.g. channels 1,6,11) There is a maximum of three non-overlapping channels (e.g. channels 1,6,11 for US) (e.g. channels 1,7,13 for Europe).	Avoid channel interference between the 802.11b and 802.11g modes by separating the operating channels at least five channels apart.
In 802.11a mode, in the 5 GHz to 6 GHz spectrum, all channels are non-overlapping and will not interfere with each other.	No channel interference in 802.11a mode.
If your environment does not contain legacy 802.11b stations or legacy access points, you can obtain maximum throughput by configuring pure-G Mode (s). See "Web: Configuring Advanced Radio Settings" on page 6-13	- B + G stations to the access points only and protected mode enabled. - Wifi G stations only and protected mode enabled. -Pure-G stations only and protected mode disabled.
Dual 802.11b/g Configuration & External Antennas	
For dual 2.4 GHz (B/G) radio operation, it is best to operate on Channel 1 and Channel 11.	
For dual B-B mode operation, the external antenna must be placed 12 inches or more away from the center of the AP for no throughput degradation.	
For mixed-mode B-G or G-B operation, the external antenna must be placed 33 inches or more away from the center of the AP for no significant throughput degradation.	
For dual G-G mode operation, the external antenna must be placed 57 inches or more away from the center of the AP for no throughput degradation.	
Greater external antenna to AP separation is required to operate on Channel 6 and Channel 11.	
Greater external antenna to AP separation is required to operate on Channel 1 and Channel 6 .	
Greater external antenna to AP separation is required to operate on Channel 6 and Channel 11.	
*Please refer to the specific product antenna manuals for detailed specifications.	

Configuring the Radio Working Mode

As specified in the "Radio Configuration Summary Table" on page 6-5, the access point can operate in three standard radio modes, IEEE 802.11a, 802.11b, or a 802.11g mode.

Getting to know 802.11a. The IEEE 802.11a provides specifications for wireless ATM systems. 802.11a is also used in wireless hubs. Networks using 802.11a operate at radio frequencies between 5.725 GHz and 5.850 GHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. This standard supports data rates ranging from 6 to 54 Mbps.

Note

The 802.11a mode is only supported on the access point's second radio (Radio 2).

Getting to know 802.11g and 802.11b. The IEEE 802.11b is a WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference.

The IEEE 802.11g offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

To simultaneously support both 80211g and 802.11b stations, the access point utilizes a special "protected mode" operation as required for compliance with the IEEE 802.11g standard. This mechanism has the effect of reducing the maximum throughput for 802.11g stations in the network. Whenever 802.11b stations are detected within range of the access point, the access point will experience reduced throughput (even if the 802.11b stations are not active in the network).

To achieve a higher throughput, you can configure the access point to completely ignore the presence of 802.11b stations by changing the Advanced radio settings. See "Web: Configuring Advanced Radio Settings" on page 6-13.

Note

The 802.11g standard is backward-compatible with 802.11b. This backward-compatibility allows it to use OFDM or CCK modulation.

To support both 802.11g and 802.11b stations, the access point has to first communicate with all stations using CCK and only switch to OFDM for data transfers between 802.11g-compatible stations. This mechanism has the effect of reducing the maximum throughput for 802.11g stations in the network.

Working in its mixed “b/g” mode, the access point will experience reduced data throughput, even if there are no 802.11b stations active in the network. To achieve a higher throughput, you can set the access point to operate in 802.11g mode, which ignores all 802.11b stations in the service area.

Note

If both Radio 1 and Radio 2 are set to the IEEE 802.11b/g mode, Radio 2 must be configured to an external antenna. See “Modifying Antenna Settings” on page 6-21.

Note

Both the IEEE 802.11g and 802.11b standards operate within the 2.4 GHz band. In a wireless LAN environment there can often be interference from other 2.4 GHz devices, such as cordless phones. If you experience poor wireless LAN performance, try to limit any possible sources of radio interference within the service area.

Web: Setting the Radio Working Mode

The Radio window provides the setting for the access point’s radio working mode.

Note

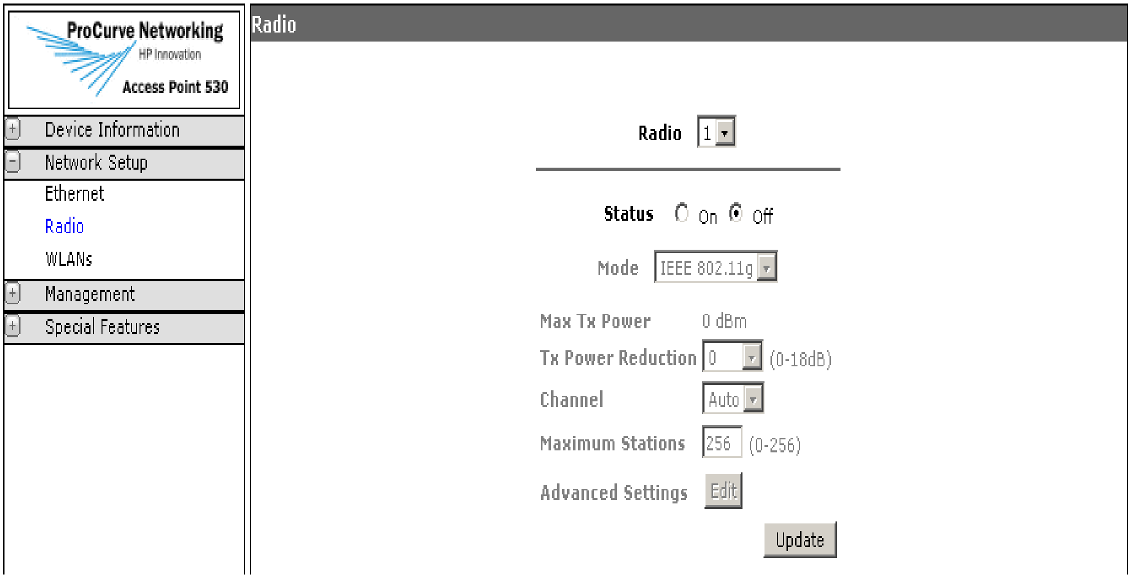
If you are using the worldwide product (J8987A) before you can configure the radio settings, the Country Setting must be set using the CLI. See “Setting the Country Code” on page 6-3. Employ the ‘write mem’ command to save the setting.

The Web interface enables you to modify these parameters:

- **Radio:** Allows toggling to either Radio 1 or 2 parameter sets. (Default is Radio 1)
- **Status:** Allows enabling/disabling of the respective radio. If enabled, the following fields become available for modification. (Default is Disabled)
- **Mode:** Selects a standard operating mode for the access point. If both Radio 1 and Radio 2 are set to the IEEE 802.11b/g mode, Radio 2 must be configured to an external antenna. See “Modifying Antenna Settings” on page 6-21.
  - **IEEE 802.11b:** stations communicate in a data transfer range between 1 to 11 Mbps. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates.

- **IEEE 802.11g:** stations communicate at a higher data transfer range between 1 to 54 Mbps, than the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). Backward compatible with IEEE 802.11b. (Radio 1 default).
- **IEEE 802.11a:** stations communicate in a data transfer range between 6 to 54 Mbps. This standard operates in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). (Radio 2 default).

■ **[Update]:** Updates the radio parameters.



Radio 1
Status ○ On ● Off
Mode IEEE 802.11g
Max Tx Power 0 dBm
Tx Power Reduction 0 (0-18dB)
Channel Auto
Maximum Stations 256 (0-256)
Advanced Settings Edit

Figure 6-1. Setting the Radio Working Mode

To Set the Radio Working Mode:

1. Select Network Setup> Radio tab.
2. To select the appropriate radio, choose **1 or 2** using the Radio drop-down.
3. To enable the radio, select **On** for the Status option.
4. Select the **radio mode**, using the Mode drop-down.
5. Click **[Update]** to save the settings.

CLI: Setting the Radio Working Mode

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
radio *<radio_name>*	9-77
mode*<mode>*	9-80
show radios <radio>* *use the parameter *<radio>* to display detailed information on the specified radio.	9-92

The following example shows how to enable the radio context level on a specific radio and set the working mode for the access point to 802.11g-only mode.

Note

Enter radio commands, one per line.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# mode g
ProCurve Access Point 530(radio1)#
```

The following example implements the **show radios** command to display current details on the dual radios configured on the access point.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# show radios
Radio   Status      Base MAC Address    Mode       Channel       TX-Power dBm
-----------------------------------------------------------------------------
1       Enabled     00:14:C2:BE:05:50   802.11g    1  - Auto   10. dBm
2       Enabled     00:14:C2:BE:05:60   802.11a    36 - Auto   5.5 dBm

ProCurve Access Point 530(config)#
```

Configuring the Radio Channel and Other Basic Settings

The access point uses the configured radio channel to communicate with wireless stations. As indicated in the "Radio Configuration Summary Table" on page 6-5, the access point's channel settings and radio mode have a configuration relationship to enhance the performance of the access point.

The channel spectrum is dependent upon the country of operation, the MHz or GHz bands desired, and specific country regulations. The country of operation might also enable specific features, for example, a European community or EFTA, requires a radar detection feature for use in a 5 GHz band. Once the country is configured, this feature is automatically enabled on the access point.

Note

If you are using the world wide product (J8987A), before you can configure the radio settings, the Country Setting must be set using the CLI. See "Setting the Country Code" on page 6-3. Employ the 'write mem' command to save the setting.

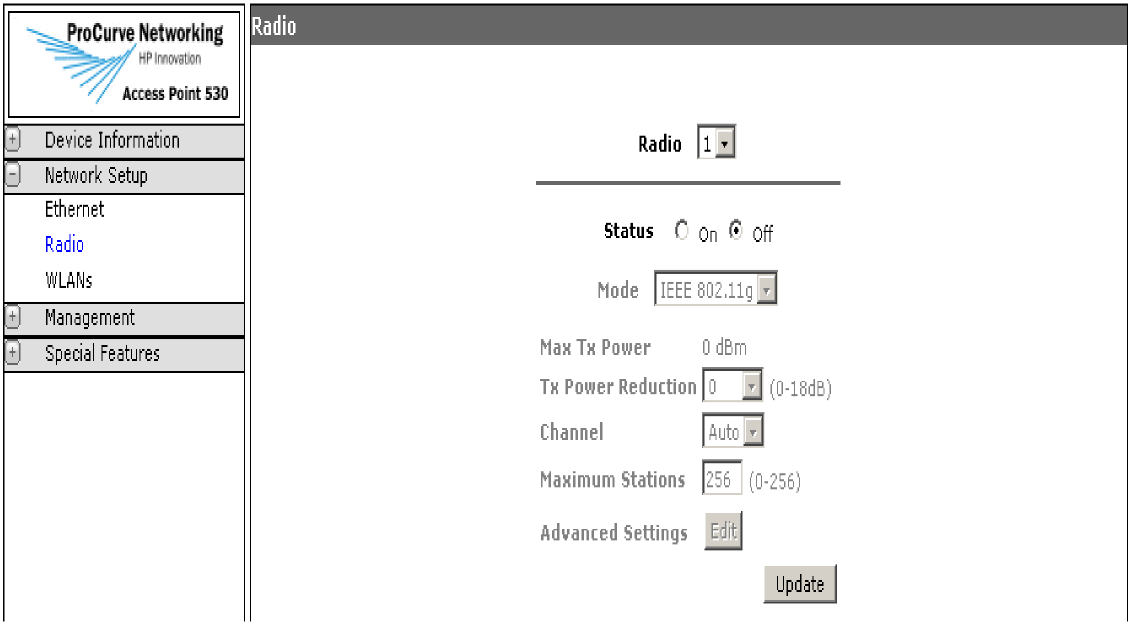
Web: Configuring Basic Radio Settings

The Radio tab provides the basic settings for the access point's radio operation. For the Advanced Settings, see "Web: Configuring Advanced Radio Settings" on page 6-13.

The Web interface enables you to modify these parameters:

- **Max Tx Power:** The maximum power in dBm that the current radio mode supports. (Default is 0)
- **Tx Power Reduction:** Adjusts the power of the radio signals transmitted from the access point. This value is in dBm. The radio operates at maximum power when this parameter is set to 0 dB. (Default is 0) For the configuration of Transmit Power, see "Web: Setting the Tx Power Reduction" on page 6-21.
- **Channel:** The radio channel that the access point uses to communicate with wireless stations. The range of channels and the default channel are determined by the radio mode and country of operation. Linked to auto channel select (ACS). When ACS is enabled, it displays channel settings. When ACS is disabled, it grays out the channel options and automatically sets the radio channel. (Default is variable, depending on the radio mode and access point model)
  Note: When the radio is configured for auto channel selection, any radio mode changes will result in a 5 to 10 second delay as the optimum radio channel is determined and selected.

- **Maximum Stations:** The maximum number of stations allowed to access the applicable radio at any one time. (Default is 256)
- **[Update]:** Updates the radio parameters.



Radio 1

Status ○ On ● Off

Mode IEEE 802.11g

Max Tx Power 0 dBm

Tx Power Reduction 0 (0-18dB)

Channel Auto

Maximum Stations 256 (0-256)

Advanced Settings

Figure 6-2. Configuring Basic Radio Settings

To Modify Basic Radio Settings:

1. Select Network Setup> Radio tab.
2. Select the **radio channel** using the drop-down. If you are deploying access points in the same area, reference the key points summarized in the overview.
3. To set the limit on stations accessing the access point, enter a **number** within the applicable range in the Maximum Stations text field.
4. Click **[Update]** to set these basic radio parameters.

Web: Configuring Advanced Radio Settings

The Advanced Settings pop-up window provides the advanced setting for the access point's radio operation.

The Web interface enables you to modify these parameters:

- **Broadcast/Multicast Rate Limiting:** Enables the rate limiting on the radio to transmit multicast and broadcast traffic. Enabling this parameter, enables the Rate Limit and Rate Limit Burst text fields. (Default is Disabled)
  - **Rate Limit:** The broadcast/multicast rate limit value in packets per second. Valid values are 0.0 through 999.9. (Default is 50)
  - **Rate Limit Burst:** The broadcast/multicast rate burst value in packets per second. This value specifies the length of time allowed for a packet burst. Valid values are 0.0 through 999.9. (Default is 75)
- **Antenna Type:** The type of radio antenna utilized by this access point. (Default is Internal) For the configuration details, see "Web: Setting the Antenna Type and Antenna Mode" on page 6-23.
- **Protected Mode:** Enables/disables the protection mode on the radio. (Default is Enabled)
- **Antenna Mode:** The mode of radio antenna utilized by this access point. (Default is Diversity) For the configuration details, see "Web: Setting the Antenna Type and Antenna Mode" on page 6-23.
- **Preamble**: Sets the length of the signal preamble used at the start of a data transmission. Using a short preamble can increase data throughput on the access point, but requires all associated stations be able to support a short preamble. (Default is Long)
  - Long: Sets the preamble to long. Using a long preamble ensures the access point can support all 802.11b and 802.11g stations.
  - Short: Sets the preamble according to the capability of stations that are currently associated. Uses a short preamble if all associated stations can support it, otherwise a long preamble is used.
- **RTS Threshold:** Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data. (Default is 2347)
- **Slot Time**: Sets the basic unit of time the access point uses for calculating waiting times before data is transmitted. (Default is Short)

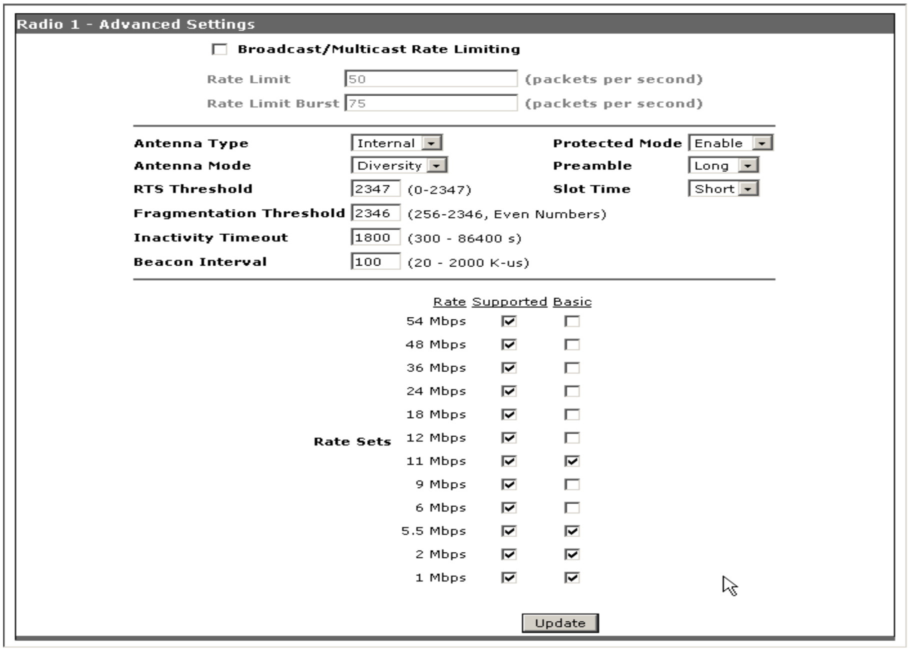
  - Short: Sets the slot time to short (9 microseconds). A short slot time can increase data throughput on the access point, but its use requires that all stations can support a short slot time (that is, 802.11g-compliant stations must support a short slot time).
  - Long: Sets the slot time to long (20 microseconds). A long slot time is required if the access point has to support 802.11b stations.
- **Fragmentation Threshold**: Configures the minimum packet size that can be fragmented when passing through the access point. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This speeds the retransmission of smaller frames. It is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. If set to 2346, this feature is disabled. Range: 256-2346, even numbers. (Default is 2346)
- **Inactivity Timeout:** Sets the length of time the wireless client is considered inactive if no traffic has been received from the station by this radio. Range: 300 - 86400 seconds.
- **Beacon Interval:** The rate at which beacon frames are transmitted from the access point. The beacon frames allow wireless stations to maintain contact with the access point. They may also carry power-management information. Range: 20-2000 K-us (Default is 100)
- **Rate Sets:** Rates are expressed in megabits per second.
  - **Supported Rate Sets:** Indicate rates that the access point supports. The AP automatically chooses the most efficient rate based on factors like error rates and distance of client stations from the AP.
  - **Basic Rate Sets:** Indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.
- **[Update]:** Updates the advanced radio parameters.

NOTE

To configure the access point to completely ignore 802.11b stations, the required settings are:

- Protected Mode: Disable
- Supported Rate Sets: Disable (1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps)

For the advanced Pure G Mode configuration details, see "To Configure Pure G Mode:" on page 6-18.



Radio 1 - Advanced Settings

□ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)
Rate Limit Burst 75 (packets per second)

Antenna Type Internal
Antenna Mode Diversity
RTS Threshold 2347 (0-2347)
Fragmentation Threshold 2346 (256-2346, Even Numbers)
Inactivity Timeout 1800 (300 - 86400 s)
Beacon Interval 100 (20 - 2000 K-us)

Protected Mode Enable
Preamble Long
Slot Time Short

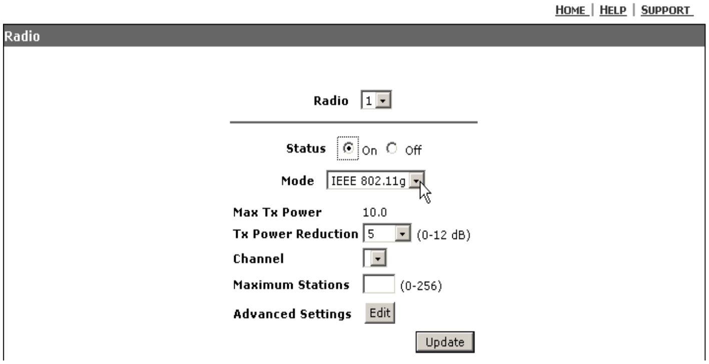
Rate Sets

Rate	Supported	Basic
54 Mbps	☑	□
48 Mbps	☑	□
36 Mbps	☑	□
24 Mbps	☑	□
18 Mbps	☑	□
12 Mbps	☑	□
11 Mbps	☑	☑
9 Mbps	☑	□
6 Mbps	☑	□
5.5 Mbps	☑	☑
2 Mbps	☑	☑
1 Mbps	☑	☑

Figure 6-3. Configuring Advanced Radio Settings

To Modify Advanced Radio Settings:

1. Select Network Setup> Radio tab >**[Edit]** button **>** Advanced Settings.
2. To enable the rate limiting, check **Broadcast/Multicast Rate Limiting**.
3. If you enabled Broadcast/Multicast Rate Limiting, enter the **rate limit** and the **rate limit burst** amounts.
4. Select **enable** for the Protected Mode, to set this radio parameter.
5. Select the **preamble and slot times**, using the drop-downs.
6. To configure the communication periods and packet size transmissions, enter a **value within the range amounts** for the RTS and Fragmentation text fields.
7. Enter the **length of time value** to establish inactivity timeout.
8. Select **rate set values** using the supported or basic check options.
9. Click **[Update]** to set the advanced radio parameters.



Radio

Radio 1

Status ● On ○ Off

Mode IEEE 802.11g

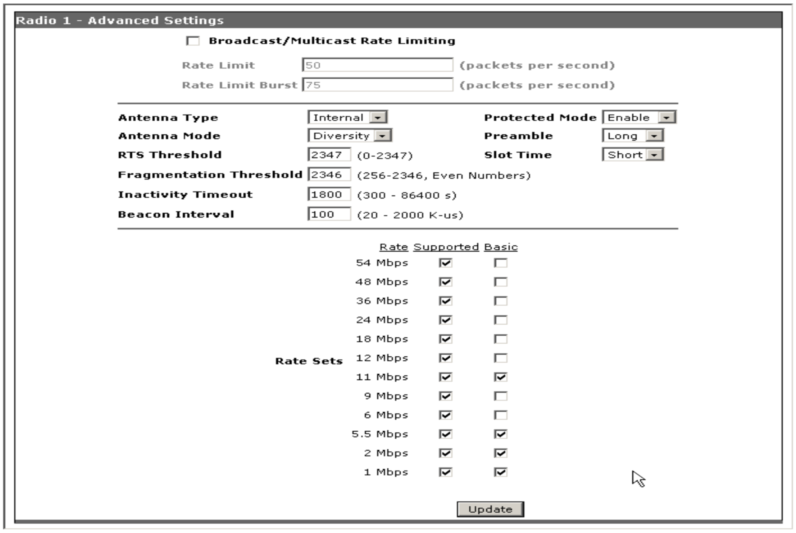
Max Tx Power 10.0

Tx Power Reduction 5 (0-12 dB)

Channel

Maximum Stations (0-256)

Advanced Settings



Radio 1 - Advanced Settings

□ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

Antenna Type Internal

Antenna Mode Diversity

RTS Threshold 2347 (0-2347)

Fragmentation Threshold 2346 (256-2346, Even Numbers)

Inactivity Timeout 1800 (300 - 86400 s)

Beacon Interval 100 (20 - 2000 K-us)

Protected Mode Enable

Preamble Long

Slot Time Short

Rate Sets

Rate	Supported	Basic
54 Mbps	☑	□
48 Mbps	☑	□
36 Mbps	☑	□
24 Mbps	☑	□
18 Mbps	☑	□
12 Mbps	☑	□
11 Mbps	☑	☑
9 Mbps	☑	□
6 Mbps	☑	□
5.5 Mbps	☑	☑
2 Mbps	☑	☑
1 Mbps	☑	☑

Figure 6-4. Configuring B + G Modes

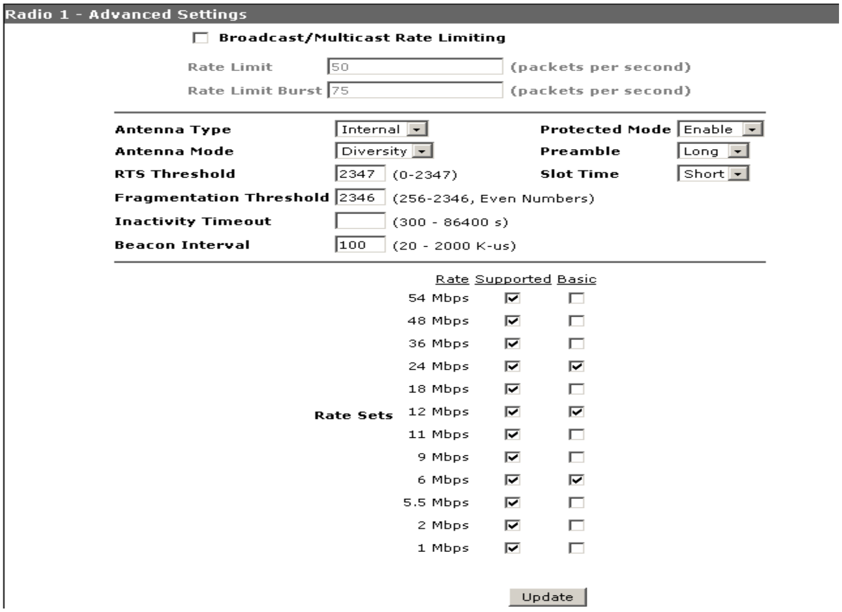
To Configure B + G Modes:

This setting allows both b-stations and g-stations to associate with the AP.

1. Select Network Setup> Radio tab >Select **IEEE 802.11g mode** >**[Edit]** button **>** Advanced Settings.

2. Select **enable** for the Protected Mode, to set this radio parameter.

3. Click **[Update]** to set the advanced radio parameters.



Radio 1 - Advanced Settings

☐ **Broadcast/Multicast Rate Limiting**

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

Antenna Type	Internal	**Protected Mode**	Enable
Antenna Mode	Diversity	**Preamble**	Long
RTS Threshold	2347 (0-2347)	**Slot Time**	Short
Fragmentation Threshold	2346 (256-2346, Even Numbers)		
Inactivity Timeout	(300 - 86400 s)		
Beacon Interval	100 (20 - 2000 K-us)		

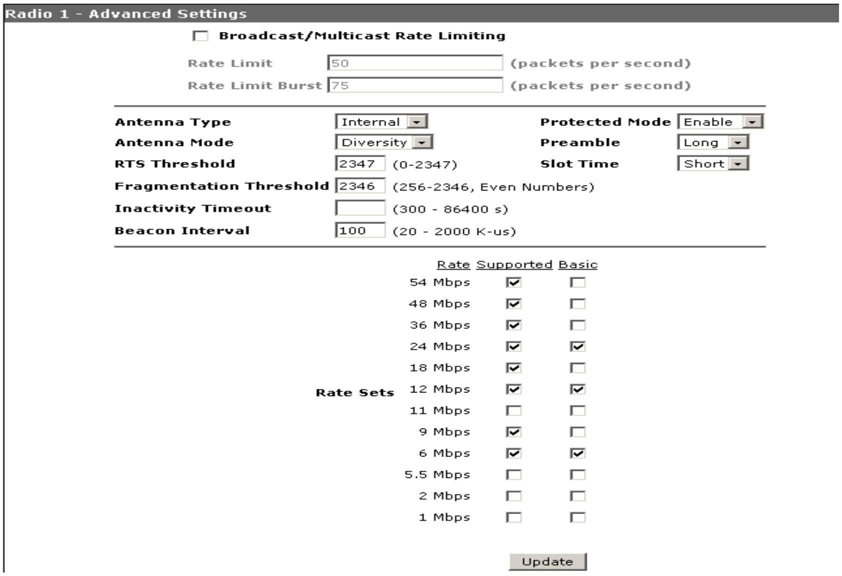
	Rate	Supported	Basic
Rate Sets	54 Mbps	☑	☐
	48 Mbps	☑	☐
	36 Mbps	☑	☐
	24 Mbps	☑	☑
	18 Mbps	☑	☐
	12 Mbps	☑	☑
	11 Mbps	☑	☐
	9 Mbps	☑	☐
	6 Mbps	☑	☑
	5.5 Mbps	☑	☐
	2 Mbps	☑	☐
	1 Mbps	☑	☐

Figure 6-5. Configuring Wifi G-Only Mode

To Configure Wifi G-Only Mode:

This setting allows only g-stations to associate with the AP. This is Wifi standard based g-only mode.

1. Select Network Setup> Radio tab >Select **IEEE 802.11g mode** >**[Edit]** button **>** Advanced Settings.
2. Select **enable** for the Protected Mode, to set this radio parameter.
3. Select **rate set values (24, 12, and 6)** using the basic check options.
4. Click **[Update]** to set the advanced radio parameters.



Radio 1 - Advanced Settings

□ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

Antenna Type Internal

Antenna Mode Diversity

RTS Threshold 2347 (0-2347)

Fragmentation Threshold 2346 (256-2346, Even Numbers)

Inactivity Timeout (300 - 86400 s)

Beacon Interval 100 (20 - 2000 K-us)

Protected Mode Enable

Preamble Long

Slot Time Short

	Rate	Supported	Basic
Rate Sets	54 Mbps	☑	□
	48 Mbps	☑	□
	36 Mbps	☑	□
	24 Mbps	☑	☑
	18 Mbps	☑	□
	12 Mbps	☑	☑
	11 Mbps	□	□
	9 Mbps	☑	□
	6 Mbps	☑	☑
	5.5 Mbps	□	□
	2 Mbps	□	□
	1 Mbps	□	□

Figure 6-6. Configuring Pure G Mode

To Configure Pure G Mode:

This setting allows only g-stations to associate with the access point, but should only be used if no legacy 802.11b clients or access points are within range of the 530 access point.

Caution

This mode is not a standard-based configuration mode. If this mode is used with legacy b-stations and b-access points, this mode will create a detrimental effect leading to low throughput, especially with the "Protected Mode" being disabled.

1. Select Network Setup> Radio tab >Select **IEEE 802.11g mode** >**[Edit]** button **>** Advanced Settings.
2. Select **disable** for the Protected Mode, to set this radio parameter.
3. Deselect **rate set values (11, 5.5, 2, and 1)** using the supported check options.
4. Deselect **rate set values (11, 5.5, 2, and 1)** and select **rate set values (24, 12, and 6)** using the basic check options.
5. Click **[Update]** to set the advanced radio parameters.

CLI: Configuring Radio Settings

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
description <*string*>	9-92
[no] basic-rate <*value*>	9-82
beacon-interval <*value*>	9-84
fragmentation-thresh <*value*>	9-87
rts-threshold <*value*>	9-89
show stations	9-98
show radio <*radio*>	9-92

Note

The Country Code must be set before radio settings can be configured. These basic settings affect the radio channels and values that are available for other parameters. See "Setting the Country Code" on page 6-3. Employ the 'write mem' command to save the setting.

Configuring One Radio. The following example details how to enable one radio and configure specific radio parameters on the access point.

Note

Enter radio commands one line at a time.

.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#description "Radio 1 -
802.11g"
ProCurve Access Point 530(radio1)#beacon-interval 102
ProCurve Access Point 530(radio1)#fragmentation-thresh 1024
ProCurve Access Point 530(radio1)#rts-threshold 2000
```

The following example uses the **show radio** <*radio*> command to display this access point's radio parameter details.

```
ProCurve Access Point 530# show radio 1
------------------------------------------------------------
Description     Radio 1-802.11g
Base MAC        00:14:C2:A5:22:E0       Status                 Disabled
Mode            802.11g                 Channel-Policy         Auto
Channel         1                       WLANs Supported        16
Preamble        long                    CTS Protection         Enabled
Slot-time       short                   Beacon-Interval(K-us)  102
TX-Power(dBm)   0                       Power Reduction(dB)    0
Antenna Mode    diversity               Antenna(s) In Use      internal
RTS-Threshold   2000                    Fragment-Threshold     1024
WMM QoS         Enabled                 Inactivity Timeout     1800
Max Stations    256

Rate-Limiting (Disabled)
Rate-Limit(packets/second)   50         Burst-Limit(packets/second)  75

AP-Detection (Disabled)
Periodic Scan Duration(ms)   30         Periodic Scan Interval(sec)   10
List Max Entries             255        List Expiration Time(sec)     3600
ProCurve Access Point 530#
```

The following example uses the **show stations** command to display connected stations to the access points.

.

```
ProCurve Access Point 530# show stations
Station On WLAN (radio index/WLAN index)  Auth. Assoc.  Fwd.
-------------------------------------------------------------
00:0b:cd:5c:3b:da  GJ SSID 1 (1/1)        Yes     -     n/a
00:0f:66:16:7a:77  GJ SSID 1 (2/1)        Yes    Yes    n/a
00:0b:cd:5a:47:64  GJ SSID 1 (2/1)        Yes    Yes    n/a
ProCurve Access Point 530#
```

Modifying Antenna Settings

When using an external antenna with the access point, you must configure the radio for the type of external antenna that is attached; either diversity or single. Also, the access point's transmit power must be limited to conform to local regulations.

When using the access point's included diversity antennas, the default antenna settings should be used. The default antenna mode is Diversity and the default transmit power reduction value is set to zero.

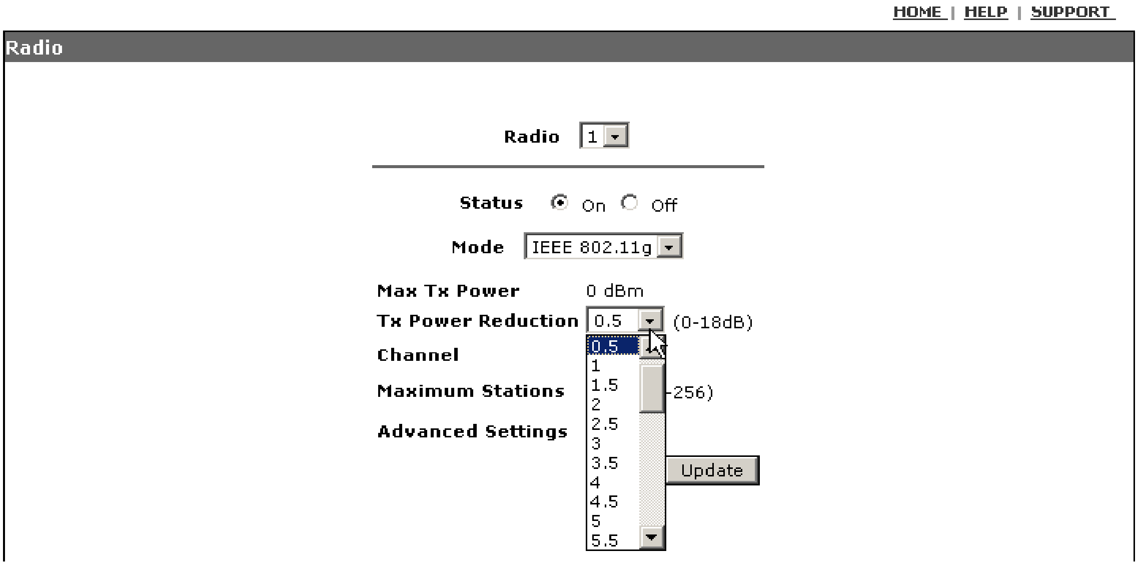
For more information on using an external antenna with the access point, refer to the *Installation and Getting Started Guide* and the specific product antenna manuals.

Web: Setting the Tx Power Reduction

The Radio window provides access to the configuration settings for adjusting the transmit power reduction values.

The Web interface enables you to modify or view these parameters:

- **Max Tx Power:** The maximum power that the current radio mode supports. (Default is maximum power)
- **Tx Power Reduction:** Adjusts the amount of attenuation applied to the selected radio. This value is in dBm. The radio operates at maximum power when this parameter is set to 0 dB. It may be necessary to apply Tx Power Reduction, if your antenna gain causes the radio power to exceed the regulatory domain limit. You may also want to apply Tx Power Reduction to avoid overlap with another access point coverage area (Default is 0)
- **[Update]:** Updates the transmit power parameter.



HOME | HELP | SUPPORT

Radio

Radio 1

Status ● On ○ Off

Mode IEEE 802.11g

Max Tx Power 0 dBm

Tx Power Reduction 0.5 (0-18dB)

Channel

Maximum Stations -256)

Advanced Settings

Figure 6-7. Setting Transmit Power Reduction

To Modify the Transmit Power Reduction:

1. Select Network Setup> Radio tab.
2. Use the Tx Power Reduction drop-down to select a **dBm value**.
3. Click **[Update]** to set the radio transmit power reduction.

Web: Setting the Antenna Type and Antenna Mode

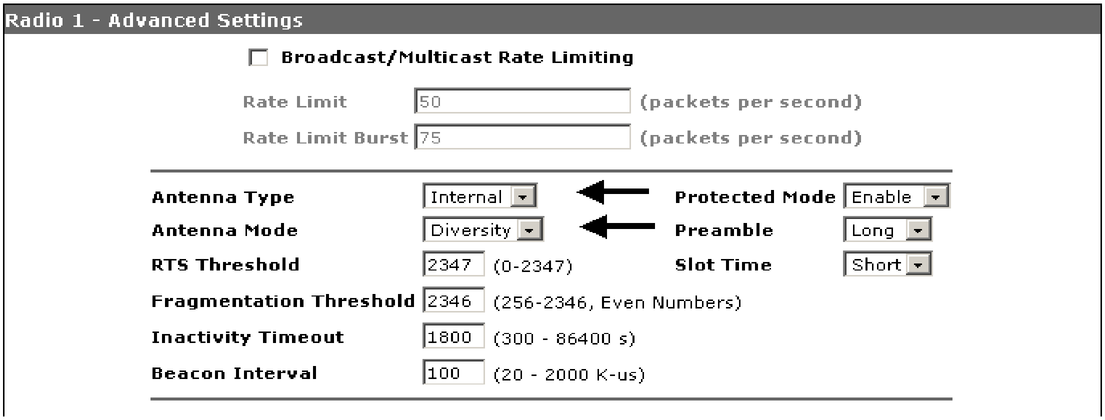
The Radio window provides access to the configuration settings for adjusting the transmit power limits.

The Web interface enables you to modify these parameters:

- **Antenna Type:** The type of radio antenna utilized by this access point. (Default is Internal).
- **Antenna Mode:** The mode of radio antenna utilized by this access point. (Default is Diversity).
- **[Update]:** Updates the antenna type and antenna mode parameters.

Note

Radio 2 must be configured to an external antenna if Radio 2 is configured to either the IEEE 802.11b or 802.11g mode, The Radio 2 internal antenna must be configured to the IEEE 802.11a mode. See "Radio Configuration Summary Table" on page 6-5.



Radio 1 - Advanced Settings

□ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)
Rate Limit Burst 75 (packets per second)

Antenna Type	Internal	Protected Mode	Enable
Antenna Mode	Diversity	Preamble	Long
RTS Threshold	2347 (0-2347)	Slot Time	Short
Fragmentation Threshold	2346 (256-2346, Even Numbers)		
Inactivity Timeout	1800 (300 - 86400 s)		
Beacon Interval	100 (20 - 2000 K-us)		

Figure 6-8. Setting Antenna Parameters

To Modify the Antenna Parameters:

1. Select Network Setup> Radio tab >**[Edit]** button **>** Advanced Settings.
2. To set the radio to use an internal or external antenna, select **Internal or External**, using the Antenna Type drop-down.
3. To set the radio to use a specific antenna mode, select **Diversity or Single**, using the Antenna Mode drop-down.
4. Click **[Update]** to set the antenna parameters.

CLI: Setting the Transmit Power Reduction and Antenna Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
tx-power-reduction <*value*>	9-90
antenna <external | internal>	9-81
antenna mode <diversity | single>	9-81
show radio	9-92

The following example shows how to set the transmit power reduction value, establish an external antenna, and set the mode to single on the access point. The default mode is set to 'diversity'.

```
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# tx-power-reduction 5
ProCurve Access Point 530(radio1)# antenna external
ProCurve Access Point 530(radio1)# antenna mode single
```

You can use the **show radio** command to display the current radio settings from the wireless interface configuration level.

```
ProCurve Access Point 530# show radio 1
------------------------------------------------------------
Description    Radio 1-802.11g
Base MAC       00:14:C2:A5:22:E0       Status                 Disabled
Mode           802.11g                 Channel-Policy         Auto
Channel        1                       WLANs Supported        16
Preamble       long                    CTS Protection         Enabled
Slot-time      short                   Beacon-Interval(K-us)  102
TX-Power(dBm)  0                       Power Reduction(dB)    5
Antenna Mode   single                  Antenna(s) In Use      external
RTS-Threshold  2000                    Fragment-Threshold     1024
WMM QoS        Enabled                 Inactivity Timeout     1800
Max Stations   256

Rate-Limiting (Disabled)
Rate-Limit(packets/second)   50        Burst-Limit(packets/second)  75

AP-Detection (Disabled)
Periodic Scan Duration(ms)   30        Periodic Scan Interval(sec)   10
List Max Entries             255       List Expiration Time(sec)     3600
ProCurve Access Point 530#
```

Managing Multiple WLAN (BSS/SSID) Interfaces

A Wireless Local-Area Network (WLAN) is a wireless LAN is a local area network (LAN) that users access through a wireless connection. The IEEE 802.11-1999 standards specify WLAN technologies. It uses high-frequency radio waves rather than wires to communicate between nodes. The access point's WLAN settings describe the BSSID unit that consists of an SSID, VLAN, security settings, MAC Authentication, and RADIUS servers. Each WLAN is in many ways similar to a standalone access point. The access point supports up to 16 fully configured WLANs.

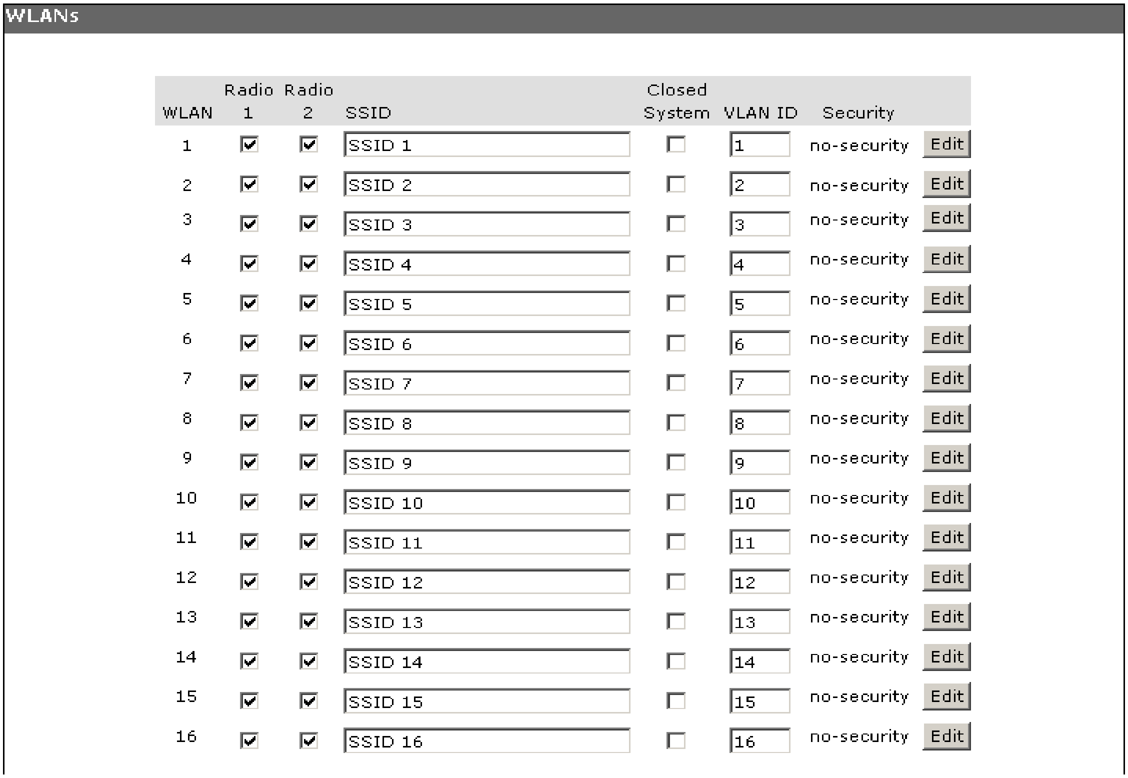
Understanding SSID. A Service Set Identifier (SSID) is a code (32 alphanumeric characters maximum) attached to all packets on a wireless network to identify each packet as part of that network. All wireless devices attempting to communicate with each other must share the same SSID. SSID also serves to uniquely identify a group of wireless network devices used in a given service set. Wireless stations that want to connect to a network through an access point must set their SSIDs to match that of the access point.

Multiple SSID interfaces enable wireless traffic to be separated for different user groups using a single access point that services one area. For each SSID interface, different security settings, VLAN assignments, and other parameters can be applied. Wireless stations within the service area to associate with what appears to be different access points. All the SSID interfaces are supported using a single radio channel, enabling efficient use of a limited number of available radio channels. The access point currently supports up to sixteen SSID interfaces.

Understanding VLAN assignments and SSID. The definitions and descriptions of VLAN (Management VLAN ID, dynamic, or static) are presented in a separate VLAN section, see "Configuring VLAN Support" on page 5-48.

This section provides details on VLAN and SSID configuration. It is important to establish a configuration plan to enhance the capabilities of the access point. The access point supports up to 16 fully configured WLANs or SSIDs on Radio 1, which will then copy over to Radio 2. The number of VLANs per radio match the amount of configured WLANs, which establishes a maximum of 16 total VLANs.

The following screen shot presents the configuration scenario to utilize when managing VLANs and SSID interfaces.



WLANs

WLAN	Radio 1	Radio 2	SSID	Closed System	VLAN ID	Security	
1	☑	☑	SSID 1	□	1	no-security	Edit
2	☑	☑	SSID 2	□	2	no-security	Edit
3	☑	☑	SSID 3	□	3	no-security	Edit
4	☑	☑	SSID 4	□	4	no-security	Edit
5	☑	☑	SSID 5	□	5	no-security	Edit
6	☑	☑	SSID 6	□	6	no-security	Edit
7	☑	☑	SSID 7	□	7	no-security	Edit
8	☑	☑	SSID 8	□	8	no-security	Edit
9	☑	☑	SSID 9	□	9	no-security	Edit
10	☑	☑	SSID 10	□	10	no-security	Edit
11	☑	☑	SSID 11	□	11	no-security	Edit
12	☑	☑	SSID 12	□	12	no-security	Edit
13	☑	☑	SSID 13	□	13	no-security	Edit
14	☑	☑	SSID 14	□	14	no-security	Edit
15	☑	☑	SSID 15	□	15	no-security	Edit
16	☑	☑	SSID 16	□	16	no-security	Edit

Figure 6-9. Configuring VLANs and SSID

Web: Configuring SSID Interfaces

The WLANs tab provides configuration access to SSIDs, VLANS, and closed system settings.

The Web interface enables you to modify these parameters:

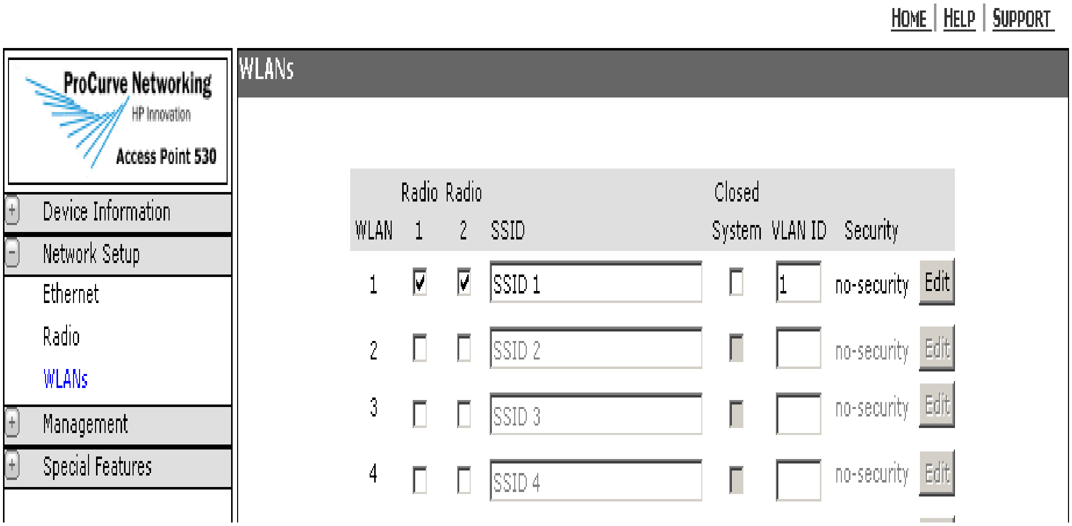
- **WLAN:** Displays the WLAN index number, 1 through 16.
- **Enabled:** Selects the applicable SSID interface to be enabled/disabled. WLAN 1 and the SSID 1 interface are automatically defaulted to enabled. Once a WLAN is enabled, the modifiable SSID interface name auto fills with the default text string (SSID 2, SSID 3, etc.) and the VLAN ID defaults.

- **Radio 1/2:** Enables/disables the WLAN for radio 1 or 2 on the specified WLAN index.
- **SSID**: Lists the access point's SSID interfaces with their basic settings. The **[Enabled]** option auto fills this text field. The SSID is an alphanumeric string of between 1 to 32 characters.

Note

Note: If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.

- **Closed-System**: Prohibits the broadcasting of the AP's SSID, if enabled. The network name will also not be displayed in the List of Available Networks on a client station. (Default is disabled, allowing SSID broadcasting)
- **VLAN ID**: Sets the VLAN associated for the specific SSID interface. Valid range is between 1 and 4094 for the Internal VLAN. (Default is 1 for WLAN 1, SSID 1)
- **Security**: Displays the Security Mode for this WLAN.
- **[Edit]**: Launches the Security window with the following tabs:
  - **Security tab:** Enables the Security Mode drop-down with the options for this WLAN (Default tab) For security mode configuration, see "Web: Setting Security Options" on page 7-14.
  - **RADIUS Servers tab:** Allows primary, secondary, and internal server configuration for RADIUS authentication. For RADIUS server settings, see "Web: Setting RADIUS Server Parameters" on page 7-28.
  - **Accounting Servers tab:** Allows primary and secondary server configuration for RADIUS Accounting. For RADIUS Accounting Server settings, see "Web: Setting RADIUS Server Parameters" on page 7-28.
  - **MAC Authentication tab:** Provides control to your wireless network by specifying a list of approved MAC addresses to 'access' your network. For MAC Authentication setting, see "Web: Configuring Access Control List" on page 7-38.



WLAN	Radio 1	Radio 2	SSID	Closed System	VLAN ID	Security	
1	☑	☑	SSID 1	□	1	no-security	Edit
2	□	□	SSID 2	□		no-security	Edit
3	□	□	SSID 3	□		no-security	Edit
4	□	□	SSID 4	□		no-security	Edit

Figure 6-10. Configuring WLAN (BSS/SSID) Interfaces

To Configure A WLAN (BSS/SSID) Interface:

1. Select Network Setup> WLANs tab.
2. Click the **Radio 1** option on the next available SSID interface.
3. Enter a **unique name** for the SSID interface. This name is automatically copied over to the compatible SSID interface for Radio 2.
4. To prohibit WLAN (BSS/SSID) interface broadcasting, check the **Closed-System** option.
5. To assign a VLAN ID per WlAN (BSS/SSSID), enter a **VLAN ID** in the VLAN text field.
6. To establish security, click **[Edit]** button and configure Security tab parameters.
7. To configure Radius servers for RADIUS authentication, click **[Edit]** button and configure RADIUS Server tab parameters.
8. To configure Accounting servers for RADIUS authentication, click **[Edit]** button and configure Accounting Servers tab parameters.
9. To configure MAC filtering, click **[Edit]** button and configure MAC Authentication tab parameters.
10. Click **[Update]** to set the SSID interface parameters.

CLI: Naming A SSID Interface

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
ssid <SSID>	9-78
show wlans [<name>] all	9-93

The following example shows how to name a SSID interface 'donna' within the 'wlan1' context.

The access point supports up to 16 fully configured WLANs or SSIDs on radio 1, which will then copy over to radio 2. WLAN context levels are different depending on the radio. The configure and enable/disable commands are available in the WLAN sub-contexts from radio 1, while only the enable/disable commands in the WLAN sub-contexts from radio 2.

Note

In order to configure an interface, you need to be in the radio configuration level. The name of the radio and WLAN (BSS/SSID) context are displayed in the parentheses. The WLAN index will have the format "wlan x", where "x" is a number from 1 to 16.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#ssid donna
```

To display a list of configured WLAN interface settings, use the **show wlan** *<x>* command, as shown in the following example.

```
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)# show wlan 1
------------------------------------------------------------
WLAN #1 on Radio 1
Description   Radio 1 - WLAN 1
Status        Enabled                SSID   donna
Max stations   2007                  BSSID  00:14:C2:BE:05:50
DTIM Period   2                      VLAN   1    - Untagged

Security Type   no-security                    Closed System   Disabled
MAC Auth Mode   local accept-list only         MAC Auth List   Bob
Authentication  open-system only               WEP Key Type    hex
WEP Key 1       not set                        WEP Key Size    128bit
WEP Key 2       not set                        Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
If Using WPA    don't allow non-WPA stations    WPA Cipher      TKIP only
WPA or WPA2     WPA and WPA2                   WPA Pre-auth.   Disabled
WPA shared key  not set

RADIUS
Failover To Local   Disabled                   Retransmit Num.  3
Primary Auth        local (built-in) server    Prim. Auth Port  n/a
Prim. Auth Key      n/a - using local (built-in) RADIUS server
Secondary Auth      not set                    Sec. Auth Port   1812
Sec. Auth Key       not set
Primary Acct        not set                    Prim. Acct Port  1813

Bytes Rx            0            Bytes Tx              918207
Packets Rx          0            Packets Tx            3579
Compressed Rx       0            Compressed Tx         0
Mcast packets Rx    0            Carrier errors Tx     0
Dropped Rx packets  0            Dropped Tx packets    0
FIFO overflows Rx   0            FIFO overflows Tx     0
Frame errors Rx     0            Packet collisions Tx  0
Total Rx errors     0            Total Tx errors       0

ProCurve Access Point 530(radio1-wlan1)#
```

CLI: Modifying WLAN (BSS/SSID) Interface Settings

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
ssid <SSID>	9-78
description <*description*>	9-78
disable | enable	9-78
vlan <*vid*>	9-78
closed-system	9-78
show wlan <*index* >	9-78

The following example shows how to modify WLAN interface settings.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#disable
ProCurve Access Point 530(radio1-wlan1)#description unsecure
ProCurve Access Point 530(radio1-wlan1)#vlan 9
ProCurve Access Point 530(radio1-wlan1)#closed-system
ProCurve Access Point 530(radio1-wlan1)
```

To display WLAN interface settings, use the **show wlan** command, as shown in the following example.

```
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 2
ProCurve Access Point 530(radio1-wlan2)# show wlan 2
------------------------------------------------------------
WLAN #2 on Radio 1
Description   Radio 1 - WLAN 2
Status        Enabled               SSID   donna
Max stations   2007                  BSSID  00:14:C2:BE:05:50
DTIM Period   2                     VLAN   1    - Untagged

Security Type   no-security                   Closed System   Disabled
MAC Auth Mode   local accept-list only        MAC Auth List   Bob
Authentication  open-system only              WEP Key Type    hex
WEP Key 1       not set                       WEP Key Size    128bit
WEP Key 2       not set                       Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
If Using WPA    don't allow non-WPA stations   WPA Cipher      TKIP only
WPA or WPA2     WPA and WPA2                  WPA Pre-auth.   Disabled
WPA shared key  not set

RADIUS
Failover To Local   Disabled                  Retransmit Num.  3
Primary Auth        local (built-in) server   Prim. Auth Port  n/a
Prim. Auth Key      n/a - using local (built-in) RADIUS server
Secondary Auth      not set                   Sec. Auth Port   1812
Sec. Auth Key       not set
Primary Acct        not set                   Prim. Acct Port  1813

Bytes Rx            0          Bytes Tx              918207
Packets Rx          0          Packets Tx            3579
Compressed Rx       0          Compressed Tx         0
Mcast packets Rx    0          Carrier errors Tx     0
Dropped Rx packets  0          Dropped Tx packets    0
FIFO overflows Rx   0          FIFO overflows Tx     0
Frame errors Rx     0          Packet collisions Tx  0
Total Rx errors     0          Total Tx errors       0

ProCurve Access Point 530(radio1-wlan1)#
```

— This page is intentionally unused. —

7

Wireless Security Configuration

Contents

Overview

This Chapter describes how to:

- Configure wireless security
- Configure MAC and 802.1X authentication
- Configure encryption
- Configure key management

Wireless Security Overview

The access point is configured by default as an "open system," with no security. This means the access point broadcasts a beacon frame advertising each configured WLAN. If a wireless client has a configured WLAN of "any," it can read the SSID from the beacon and use it to allow immediate connection to the access point. Client stations are permitted to connect with the access point without first verifying that users are authorized to access the network. In addition, user data is transmitted over the air without being encrypted, and is subject to being intercepted by client stations anywhere within range that want to eavesdrop on the wireless network.

Wireless network security requires attention to three main areas:

- **Authentication:** Verifying that stations attempting to connect to the network are authorized users before granting access to the network.
- **Encryption:** Encrypting data that passes between the access point and stations (to protect against interception and eavesdropping).
- **Key Management:** Assigning unique data encryption keys to each wireless station session, and periodically changing the encryption keys to minimize risk of their potential discovery.

Authentication

The two ways of authenticating users on the Access Point 530 are:

- **MAC Authentication:** Based on the user's wireless station MAC address.
- **802.1X Authentication:** Based on the user credentials, such as; username/password, digital certificates, etc.

MAC Authentication

MAC authentication of users can be done either using a remote authentication server like a RADIUS server or by creating a local database on the access point itself. MAC authentication is not as secured as 802.1X authentication, as it is easy to decipher and spoof for unauthorized network access.

NOTE

If Access Point 530s are deployed along with Access Point 520s, there can be a compatibility issue when MAC authentication is used. An Access Point 520 will sent a shared-secret string (for the authentication server) as the MAC authentication password. By default, the Access Point 530 will send the client station MAC address as the MAC authentication password. To avoid this compatibility issue, use the “radius” CLI command to configure the "mac-auth-password" for the Access Point 530 to be consistent with the Access Point 520 shared-secret password. For the CLI commands, refer to Section 9, page 9-55.

802.1X Authentication

User 802.1X authentication can be implemented either using a remote authentication server, such as a RADIUS server or by using the local built-in RADIUS server on the access point itself. The user's credentials are exchanged with the servers (both remote and local built-in) using a mechanism called “Extensible Authentication Protocol (EAP)”. EAP is a public-key encryption system to ensure that only authorized network users can access the network. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and sends back to the server to complete the authentication. Local built-in RADIUS server supports only one EAP type - PEAP-MSCHAPv2. For remote server authentication, the access point serves as an intermediate authenticator to transparently pass any EAP type to the remote server as specified in RFC3748.

The Access Point 530 supports all EAP type tested by the WiFi Alliance; TLS, TTLS, PEAP0/MSCHAPv2, PEAP1/GTC and SIM. EAP types which do not provide key management (like MD5) are not suitable for wireless networks. 802.1X authentication can be used with WEP, TKIP and CCMP/AES encryption ciphers.

It is possible to use a combination of both MAC authentication and 802.1X authentication simultaneously on the same WLAN.

Encryption

The Access Point 530 supports three types of encryption:

- Wired Equivalent Privacy (WEP): Key lengths of 64 bits and 128 bits are possible. WEP provides the least secure method of encryption (static WEP is not secure, as it can be easily compromised).
- Temporal Key Integrity Protocol (TKIP): Intermediate security between WEP and AES with key length of 256 bits. Provides a more-secure method of encryption than WEP (security is much better than WEP, but not as robust as CCMP).

- Counter mode/CBC-MAC Protocol (CCMP): Robust security with a key length of 128 bits. Provides the most secure method of encryption.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless stations and the access point.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, static WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For improved wireless security, the access point provides more robust data encryption methods like TKIP and AES.

Temporal Key Integrity Protocol (TKIP)

TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet.

TKIP provides further data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.

Counter Mode/CBC-MAC Protocol (CCMP)

CCMP is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES) combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks.

It is possible to use mixed cipher mode of TKIP and CCMP on an WLAN in the Access Point 530.

Key Management

Keys for encrypting the data can be managed either dynamically using 802.1X authentication or statically using pre-shared keys between the access point and station. Dynamic key management provides significantly better security when compared to using static keys.

Security Profiles

Based on Authentication, Encryption and Key Management, following is a list of security profiles in order of increasing robustness.

- No Security
- StaticWEP
- Dynamic WEP
- TKIP with PSK
- CCMP with PSK
- TKIP with 802.1X
- CCMP with 802.1X

No Security

This security mode transmits data over the wireless connection without any form of encryption for data privacy. This mode may be appropriate for systems that provide simple internet and printer access, as on a guest network. It may also be appropriate where additional security is provided by the use of encrypted VPN tunnels between the wireless client device and a network VPN server. If this mode is used, it may be desirable to prevent advertising availability of the network to other stations by configuring the WLAN for closed-system operation.

Caution

Use this mode on a sensitive internal network only for: initial setup, testing, or problem solving; or where VPN connections are mandated to provide end-to-end security for the otherwise insecure wireless connection.

Static Wired Equivalent Privacy (WEP)

Static WEP uses shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all stations hat want to use the network. WEP keys are indexed in different slots (up to four on each WLAN) and the client stations must have the same key indexed in the same slot to access data on the access point. Shared mode 802.11 authentication is not recommended, as it sends encryption keys viewable in plain text.

Dynamic Wired Equivalent Privacy (WEP)

Dynamic WEP uses WEP as the encryption cipher and 802.1X as the authentication mechanism. In this way, each client station is assigned a unique encryption key (for each session) from the authentication server. The length of the cipher can be 64 bits or 128 bits, and the encryption keys can automatically and periodically changed to further reduce the possibility of their discovery.

TKIP with Pre-shared Key

This security profile uses TKIP as the encryption cipher and pre-shared key between the access point and station as the master key and authentication mechanism. The encryption keys used between access point and stations are derived from the same master key.

CCMP with Pre-shared Key

This security profile uses AES as the encryption cipher and pre-shared key between the access point and station as the master key and authentication mechanism. The encryption keys used between access point and stations are derived from same master key.

TKIP with 802.1X

This security profile uses TKIP as the encryption cipher and 802.1X as the authentication mechanism. In this way, each station is going to utilize a unique master key to derive the encryption between the access point and station.

CCMP with 802.1X

This security profile uses AES as the encryption cipher and 802.1X as the authentication mechanism. In this way, each station is assigned a unique master key to derive the encryption between the access point and station, and the encryption keys can be automatically and periodically changed to further reduce the possibility of their discovery.

Other Security Features

In addition to these wireless security features, the Access Point 530 has a user-based security feature called "Identity Driven Management (IDM)".

For more details on IDM, please see "Identity Driven Management" on page 8-30.

Table 7-1. Summary of Wireless Security

Security Mechanism	Client Support	Implementation Considerations
No Security (NOT RECOMMENDED)	Built-in support on all 802.11a, 802.11b, and 802.11g devices	• No key management, data encryption, or user authentication is used
Static WEP Keys	Built-in support on all 802.11a, 802.11b, and 802.11g devices	• Provides only weak security • Requires manual key management
Dynamic WEP	Requires 802.1X client support in system or by add-in software (support provided in Windows 2000 SP3 or later and Windows XP)	• Provides dynamic key rotation for improved WEP security • Requires configured RADIUS server • 802.1X EAP type may require management of digital certificates for stations and server
WPA-PSK	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides dynamically generated keys that are periodically refreshed • Provides similar shared key user authentication • Provides robust security in small networks
WPA-PSK (WPA2 Only)	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides robust security in small networks • Requires manual management of pre-shared key • stations may require hardware upgrade to be WPA2 compliant
WPA-802.1X (RECOMMENDED MODE)	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides dynamically generated keys that are periodically refreshed • Requires configured RADIUS server • Provides backward compatibility to the original WPA
WPA-8021X (WPA2 only)	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides the strongest security in WPA2-only mode • Provides robust security in mixed mode for WPA and WPA2 stations • Offers fast roaming for time-sensitive station applications • Requires configured RADIUS server • 802.1X EAP type may require management of digital certificates for stations and server • Stations may require hardware upgrade to be WPA2 compliant

When you have decided which security mechanisms to implement in your network, refer to the following tables for a summary of the access point configuration procedures.

For more details on security configurations that are possible using the CLI, see "CLI: Configuring Security Settings" on page 7-20.

Table 7-2. Summary of Wireless Security Configuration

Configuring Encryption in the ProCurve Wireless Access Point 530			
Encryption Methods and Process	**WLAN Interface Level Commands**	**Additional Requirements**	**Notes**
No Security	**security** <no security>		
Static WEP Keys: 1. Enable WEP Security 2. Set the Key Index, Length, and Type 3. Configure the Keys 4. Set the Authentication	**security** <static-wep> **wep-default-key** <1| 2| 3| 4> [no] **wep-key ascii** **wep-key-length** <64|128> **wep-key** <1| 2| 3| 4> *<string>* [no] **open-system-authentication** [no] **shared-key authentication**	WEP supported station required.	Requires manual key management. Encryption index, length and type configured in the access point must match those configured in the stations.
Dynamic WEP: 1. Enable Dynamic WEP Security 2. Set the Authentication Server & Protocol 3. Set RADIUS Key	**security** <dynamic-wep> **radius-accounting** <**primary** | **secondary**> <**ip** *<ip>* | **port** *<port>* | **key** *<key>*> **radius**<**primary** | **secondary**> *The radius-key value is used with an external RADIUS server only and is ignored for the internal radius server. It should be set to the shared secret key that is configured on the external RADIUS server.	RADIUS server required. 802.1X supplicant required. WEP supported station required.	The built-in authentication server can be used on the access point or an external RADIUS server. To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server and turn RADIUS accounting off (because it is not supported by the built-in server)
WPA-PSK 1. Enable WPA Security 2. Enable WPA &/or WPA2 3. Set Authentication Protocol(s) - TKIP,CCMP (AES), or both 4. Set the key	**security** <wpa-psk> **wpa-allowed** [no]**wpa2-allowed** [no] **wpa-cipher-tkip** [no] **wpa-cipher-aes** **wpa-pre-shared-key** *<key>*	WPA supported station required. If a mix of stations, some support WPA2 and others support the original WPA, configure for both (set both wpa/wpa2 allowed).	When both TKIP and CCMP authentication methods are set, both TKIP and AES stations can associate with the access point. WPA stations must have either a valid TKIP or AES Key to communicate.

Configuring Encryption in the ProCurve Wireless Access Point 530

Encryption Methods and Process	WLAN Interface Level Commands	Additional Requirements	Notes
WPA-802.1X 1. Enable WPA Security 2. Enable WPA &/or WPA2 3. Enable Pre-Authentication 4. Set the Authentication Server & protocols - TKIP,CCMP (AES), or both 5. Set the Radius Key 6. Allow Non-WPA stations	**security** <wpa-802.1X> **wpa-allowed** [no] **wpa2-allowed** [no] **rsn-preauthentication** [no] **wpa-cipher-tkip** [no] **wpa-cipher-aes** **radius-accounting** <**primary** | **secondary**> <**ip** <*ip*> | **port** <*port*> | **key** <*key*>> **radius**<**primary** | **secondary**>	WPA supported station required. If there is a mix of stations, some support WPA2 and others support the original WPA, configure for both (set both wpa/wpa2 allowed).	• When both TKIP and CCMP authentication methods are set, both TKIP and AES stations can associate with the access point. WPA stations must have either a valid TKIP or AES Key to communicate. • For WPA2 wireless stations to send pre-authentication packets, enable pre-authentication.

The AP 530 supports the following Extensible Authentication Protocol (EAP) methods: TLS, TTLS, MD5, and PEAP (MS-CHAP v2) when configured to use an external RADIUS server for authentication. It supports only PEAP (MS-CHAP v2) when configured to use the built-in (local) RADIUS server.

To start, the access point is in the factory default configuration.
Conventions used:
Vertical bars separate alternative, mutually exclusive elements (|).
Braces enclose required elements (< >).
Italics indicate variables for which the user must supply a value when executing the command.

Table 7-3. Summary of MAC Authentication Configuration

Configuring MAC Authentication in the HP ProCurve Wireless Access Point 420							
MAC Authentication Mode	**MAC Authentication**	**Local MAC Authentication**	**MAC Authentication Table**			**RADIUS**	**Comments**
			MAC Address	**Permission**			
		MAC Table Permission		**Active**	**Inactive**		
Local MAC authentication	Local MAC	Deny	xx:xx:xx:xx:xx:xx	*		Not needed	All MAC addresses **allowed except for entries set to active** in the MAC Authentication Table. Can be combined with other methods for improved security.
Local MAC authentication	Local MAC	Allow	xx:xx:xx:xx:xx:xx	*		Not needed	All MAC addresses **denied except for entries set to active** in MAC Authentication Table. Can be combined with other methods for improved security.
Remote MAC authentication	Radius MAC	MAC address permission policy based on RADIUS server configuration.	RADIUS Server Use PAP authentication and enter MAC address as specified by the Radius MAC Address Format. User and password on the RADIUS server must be the same.			MUST	Works with static and dynamic WEP keys. Does not work with WPA with 802.1X or WPA-PSK.

Establishing Security

The security options are available from the WLANs tab and provide wireless security configuration for the WLAN.

Basic parameters required for a security option configuration are provided in the window, all other access point settings are made automatically. Some options require a RADIUS server to be configured. A link to the RADIUS Servers tab is provided where RADIUS server parameters can be configured.

The security option for WLAN 1 should be given special consideration if one or more Wireless Distribution System (WDS) links are to be configured on the Access Point 530. The security option configured for WLAN 1 also establishes the security option that is used with WDS links (1-6). WDS security options (and thus the WLAN 1 configuration) are limited to one of the choices listed in Table 7-4. The following are presented from least secure to most secure.

Table 7-4. WLAN 1 and WDS Security Configuration

Security Mode on WLAN 1	Security Mode for WDS links (1-6)
No Security	No Security (not recommended)
Static/Dynamic WEP	Static WEP
WPA-PSK/802.1X, WPA-only, TKIP cipher	WPA-PSK, TKIP cipher
WPA-PSK/802.1X, WPA2-only, CCMP (AES) cipher	WPA-PSK, AES cipher (recommended)

NOTE

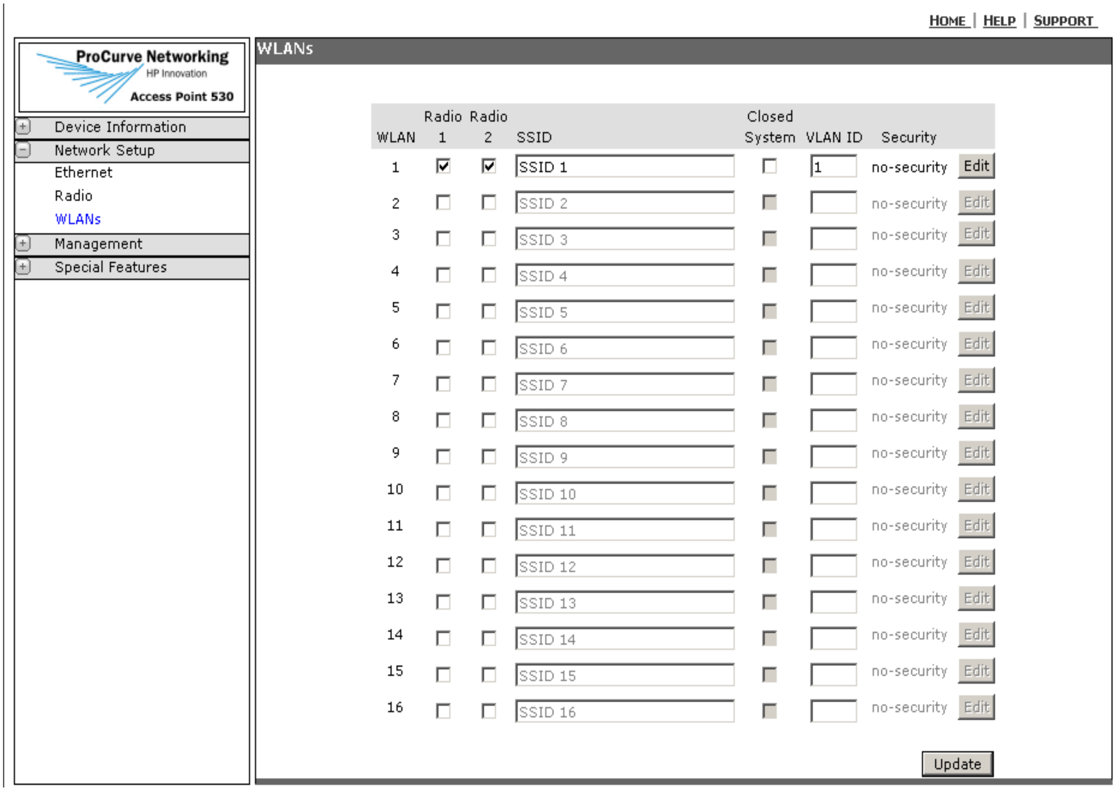
You must configure WDS data encryption keys separately, as the WEP or WPA/ WPA2 encryption key configured for WLAN 1 is not used for WDS links. See "Web: Configuring WDS Parameters" on page 8-14.

CAUTION

When access point configuration parameters are changed, wireless stations may be temporarily disconnected until the new configuration parameter is enabled. This includes any changes to a WLAN or radio parameter.

The recommended security option for WDS operation is WPA2 using the CCMP(AES) cipher, as this setting will provide the maximum security for data sent over the WDS link.

The 'No Security' option for WDS link can be used for initial setup, testing or problem-solving for a WDS link, but this setting is not recommended for normal operation. With No Security, all wireless data received by the access point (for all WLAN's) will be decrypted by the access point on receipt and then sent over the WDS link with no data encryption



	Radio	Radio		Closed			
WLAN	1	2	SSID	System	VLAN ID	Security	
1	☑	☑	SSID 1	□	1	no-security	Edit
2	□	□	SSID 2	□		no-security	Edit
3	□	□	SSID 3	□		no-security	Edit
4	□	□	SSID 4	□		no-security	Edit
5	□	□	SSID 5	□		no-security	Edit
6	□	□	SSID 6	□		no-security	Edit
7	□	□	SSID 7	□		no-security	Edit
8	□	□	SSID 8	□		no-security	Edit
9	□	□	SSID 9	□		no-security	Edit
10	□	□	SSID 10	□		no-security	Edit
11	□	□	SSID 11	□		no-security	Edit
12	□	□	SSID 12	□		no-security	Edit
13	□	□	SSID 13	□		no-security	Edit
14	□	□	SSID 14	□		no-security	Edit
15	□	□	SSID 15	□		no-security	Edit
16	□	□	SSID 16	□		no-security	Edit

Figure 7-1. Security Access via the WLANs Window

Web: Setting Security Options

The Security tab provides these options:

- **1. No Security:** The access point is configured as an open system with no user authentication or data encryption. This is the default setting.
- **2. Static WEP:** Use static IEEE 802.11 Wired Equivalent Privacy (WEP) shared keys for user authentication and data encryption. Four keys can be defined for each WLAN interface that uses static WEP. But only one of these WEP keys is transferred for active use by the SSID interface at any given time. Note that the same WEP shared key must be used by each station associated to the SSID interface. Thus static WEP is not recommended for a high-level of security.
  - **Authentication:** Select Open-System to allow association of wireless stations without requiring authentication. Select Shared Key to establish a rudimentary form of user authentication. (Default is Open-System). Select both modes if Shared Key authentication is to be supported, but not required.

Caution

Shared Key mode is seriously flawed, in that it utilizes the static WEP encryption key (transmitted openly) for station authentication. This allows the WEP encryption key to be easily discovered by anyone who might eavesdrop on the wireless network. If static WEP is configured, it is recommended to select Open System authentication.

  - **Transfer Key Index:** Select the key number (1-4) to use for encryption of transmitted data. The selected index must not be already allocated to another SSID interface. (Default is 1)
  - **Key Length:** Select 64 Bit or 128 Bit. Note that the same size of encryption key must be supported on all wireless stations. (Default is 128 bits)
  - **Key Type:** Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys:
    - **ASCII:** Enter keys as 5 alphanumeric characters for 64 bit keys or 13 alphanumeric characters for 128 bit keys.
    - **Hex:** Enter keys as 10 hexidecimal digits for 64 bit keys or 26 hexidecimal digits for 128 bit keys. (Default is Hex)
  - **WEP Keys:** Enter up to four strings of character keys. If you selected "ASCII", enter any combination ASCII characters. If you selected "Hex", enter hexadecimal digits (any combination of 0-9 and a-f or A-F). The number of characters required updates automatically based on how you set Key Length and Key Type.
  - **[Update]:** Updates the security parameters.

Note

WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA) for improved data encryption and user authentication.

3. Dynamic WEP: Establishes the Extensible Authentication Protocol (EAP) to pass user credentials from the station to the RADIUS server. Authentication is then verified on the RADIUS server before the access point grants station access to the network. For the configuration of the RADIUS Servers, see "Web: Setting RADIUS Server Parameters" on page 7-28.

- **RADIUS Servers:** Launches the RADIUS configuration window.

■ **4. WPA-PSK:** Employs a pre-shared key (instead of using IEEE 802.1x and EAP as is used in the WPA-802.1x security mode). The PSK is used for an initial check of credentials only. WPA supported station required. If a mix of stations, some support WPA2 and others support the original WPA, configure for both (set both wpa/wpa2 allowed).

- **WPA Versions**: Specifies support for WPA/WPA2 stations.
  - **WPA**: stations using WPA only are supported.
  - **WPA2**: stations using WPA2 only are supported.
  - **Both**: stations using both WPA and WPA2 are supported. (Default)
- **Enable pre-authentication**: Enables pre-authentication packets to be transmitted from the access point the station is currently using to the target access point. It speeds up authentication for roaming stations connecting to multiple access points. Only enabled if WPA2 or Both were selected with the WPA Support drop-down. WPA does not support this feature.
- **Cipher Suites**: Specifies encryption support:
  - **TKIP**: TKIP uses a 128-bit "temporal key", which combines the station's MAC address and a 16-octet initialization vector to produce the encryption key. This ensures unique key encryption. TKIP uses RC4 to perform the encryption and changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. (Default)
  - **CCMP (AES)**: CCMP is an IEEE802.1x encryption method that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.
  - **Both:** If you select both TKIP and CCMP(AES), Pairwise cipher is AES and Groupwise cipher is TKIP. Pairwise cipher is used for unicast traffic and Groupwise cipher is used for multicast/ broad-

cast traffic. Both TKIP and AES stations can associate with the access point. if WPA stations have either a valid TKIP or CCMP (AES) key to associate with the access point.

Note Stations not configured to use a WPA-PSK will not be able to associate with an access point.

- **Pre-Shared Key**: The Pre-shared Key is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters
- **[Update]:** Updates the security parameters.

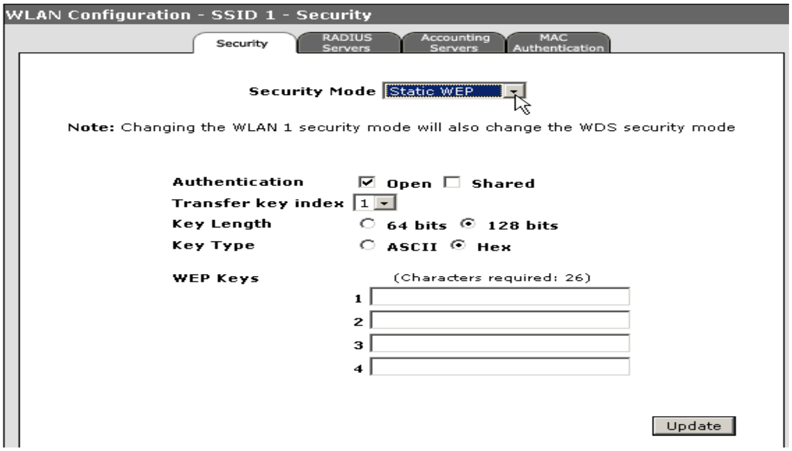
■ **5. WPA-802.1X:** This IEEE 802.11i-2004 (Specifies security enhancements in encryption, authentication, and key management. IEEE 802.1X is used in its authentication enhancement. Support for roaming is also provided) standard includes AES, CCMP, and TKIP mechanisms. This method requires the use of a RADIUS server to authenticate users, and configuration of user accounts. This security mode is backwards-compatible with wireless stations that support the original WPA.

- **WPA Versions**: Specifies support for WPA/WPA2 stations.
  - **WPA**: stations using WPA only are supported.
  - **WPA2**: stations using WPA2 only are supported.
  - **Both**: stations using both WPA and WPA2 are supported. (Default)
- **Enable pre-authentication**: Enables pre-authentication packets to be transmitted from the access point the station is currently using to the target access point. It speeds up authentication for roaming stations connecting to multiple access points. Only enabled if WPA2 or Both were selected with the WPA Support drop-down. WPA does not support this feature.
- **Cipher Suites**: Specifies encryption support:
  - **TKIP**: TKIP uses a 128-bit "temporal key", which combines the client's MAC address and a 16-octet initialization vector to produce the encryption key. This ensures unique key encryption. TKIP uses RC4 to perform the encryption and changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. (Default)
  - **CCMP (AES)**: CCMP is an IEEE802.1x encryption method that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

- **Both:** If you select both TKIP and CCMP(AES), Pairwise cipher is AES and Groupwise cipher is TKIP. Pairwise cipher is used for unicast traffic and Groupwise cipher is used for multicast/ broadcast traffic. Both TKIP and AES stations can associate with the access point. if WPA stations have either a valid TKIP or CCMP (AES) key to associate with the access point.

- **RADIUS Servers:** Launches the RADIUS configuration window.
- **[Update]:** Updates the security parameters.

.



WLAN Configuration - SSID 1 - Security

Security Mode: Static WEP

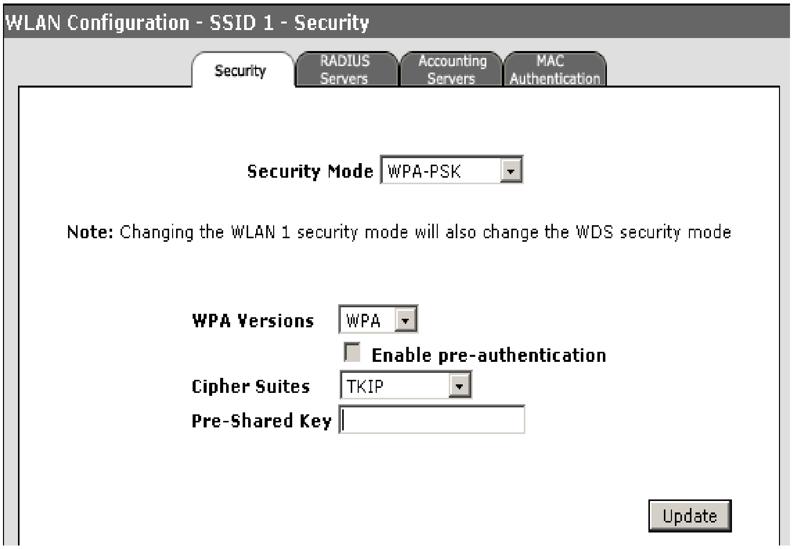
Note: Changing the WLAN 1 security mode will also change the WDS security mode

Authentication ☑ Open ☐ Shared
Transfer key index 1
Key Length ○ 64 bits ● 128 bits
Key Type ○ ASCII ● Hex
WEP Keys (Characters required: 26)
1
2
3
4

Figure 7-2. Configuring Static WEP

To Configure Static WEP Shared Keys:

1. Select Network Setup> WLANs tab >WLAN (BSS/SSID) interface > **[Edit]** button > Security Tab.
2. Select **Static WEP** from the Security Mode drop-down.
3. To allow system authentication, select **Shared-Key** from the Authentication option.
4. Select a **key index** from the Transfer Key Index to be used for encryption for the WLAN interface.
5. Select the **key length** to be used by all stations, 64 or 128 bit.
6. Select the **Hex** or **Ascii** for the Key Type.
7. Enter the **key value** conforming to the length and type already selected.
8. Click **[Update]** to set Static WEP security parameters.



WLAN Configuration - SSID 1 - Security

Security Mode WPA-PSK

Note: Changing the WLAN 1 security mode will also change the WDS security mode

WPA Versions WPA

□ **Enable pre-authentication**

Cipher Suites TKIP

Pre-Shared Key

Figure 7-3. Configuring WPA-PSK

To Configure WPA-PSK:

1. Select Network Setup> WLANs tab >WLAN (BSS/SSID) interface > **[Edit]** button > Security Tab.

2. Select **WPA-PSK** from the Security Mode drop-down.

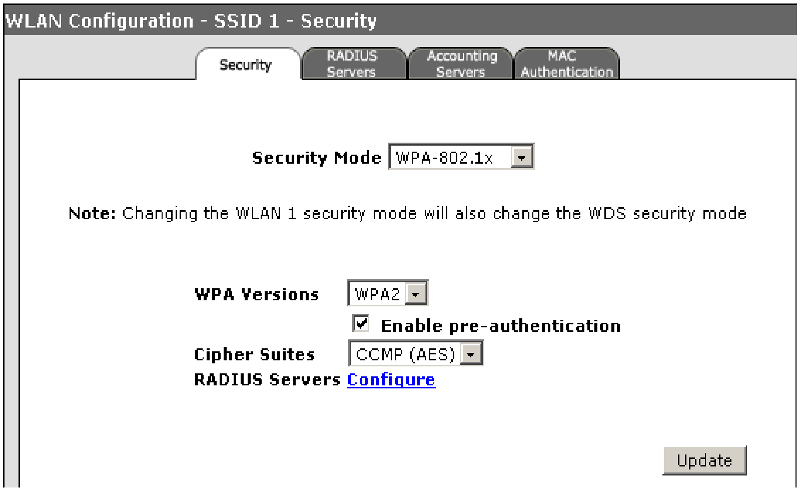
3. Select **WPA**, **WPA2**, or **Both** for WPA support, as required.

4. Enable **pre-authentication**, if you selected WPA2 or Both for the WPA Version.

5. Select **TPIK (recommended), CCMP (AES)**, or **Both** to enable the type of CIPHER encryption.

6. For the **key,** enter between 8 and 63 alphanumeric characters. (Be sure that all wireless stations use the same key.)

7. Click **[Update]** to set the WPA-PSK security parameters.



WLAN Configuration - SSID 1 - Security

Security Mode WPA-802.1x

Note: Changing the WLAN 1 security mode will also change the WDS security mode

WPA Versions WPA2

☑ Enable pre-authentication

Cipher Suites CCMP (AES)

RADIUS Servers Configure

Figure 7-4. Configuring WPA-802.1X

To Configure WPA-802.1X:

1. Select Network Setup> WLANs tab >WLAN (BSS/SSID) interface > **[Edit]** button > Security Tab.
2. Select **WPA-802.1X** from the Security Mode drop-down.
3. Select **WPA**, **WPA2**, or **Both** for WPA support, as required.
4. Enable **pre-authentication**, if you selected WPA2 or Both for the WPA Version.
5. Select **TPIK , CCMP (AES) (recommended if selected WPA2)**, or **Both** to enable the type of CIPHER encryption.
6. Select **Remote Servers** to configure the RADIUS Server to enhance security.
7. Click **[Update]** to set the WPA-802.1X security parameters.

Manual Configuration Using the CLI

The following sections show examples of how to use the CLI to view and configure security settings access point.

NOTE: Security settings using the CLI can only be made for WLANs in the context of Radio 1. Security settings for each different WLAN are automatically copied over from Radio 1 to Radio 2. The only setting that can be made specifically in the context of Radio 2 is to enable or disable the entire WLAN on Radio 2.

CLI: Configuring Security Settings

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
security <no-security|static-wep|dynamic-wep|wpa-psk|wpa-802.1x>	9-101
wep-default-key <1| 2| 3| 4>	9-103
[no] **wep-key ascii**	9-104
wep-key-length <64|128>	9-105
wep-key-<1| 2| 3| 4> *<string>*	9-105
[no] **open-system-authentication**	9-106
[no] **shared-key authentication**	9-107
radius-accounting <primary | secondary> <ip *<ip>* **| port** *<port>* **| key** *<key>*	9-53
radius <primary | secondary>	9-55
[no] **wpa-allowed**	9-107
[no] **wpa2-allowed**	9-107
wpa-pre-shared-key *<key>*	9-108
wpa-cipher-tkip	9-109
wpa-cipher-aes	9-109
rsn-preauthentication	9-110

Using the CLI to Configure No Security. The following example shows how to configure an WLAN interface to have no security set.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security no-security
ProCurve Access Point 530(radio1-wlan1)#
```

Using the CLI to View the Current WLAN (BSS/SSID) Configuration. The following example shows how to view the current configuration settings.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)# show wlan 1
------------------------------------------------------------------------------
WLAN #1 on Radio 1
Description   Radio 1 - WLAN 1
Status        Enabled                SSID   Radio 1 - SSID 1
Max stations   2007                  BSSID  00:14:C2:BE:05:50
DTIM Period   2                      VLAN   1    - Untagged
Security Type   no-security                    Closed System   Disabled
MAC Auth Mode   local accept-list only         MAC Auth List   Bob
Authentication  open-system only               WEP Key Type    hex
WEP Key 1       not set                        WEP Key Size    128bit
WEP Key 2       not set                        Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
If Using WPA    don't allow non-WPA stations    WPA Cipher      TKIP only
WPA or WPA2     WPA and WPA2                   WPA Pre-auth.   Disabled
WPA shared key  not set
RADIUS
Failover To Local   Disabled                   Retransmit Num.  3
Primary Auth        local (built-in) server    Prim. Auth Port  n/a
Prim. Auth Key      n/a - using local (built-in) RADIUS server
Secondary Auth      not set                    Sec. Auth Port   1812
Sec. Auth Key       not set
Primary Acct        not set                    Prim. Acct Port  1813
Bytes Rx            0            Bytes Tx             918207
Packets Rx          0            Packets Tx           3579
Compressed Rx       0            Compressed Tx        0
Mcast packets Rx    0            Carrier errors Tx    0
Dropped Rx packets  0            Dropped Tx packets   0
FIFO overflows Rx   0            FIFO overflows Tx    0
Frame errors Rx     0            Packet collisions Tx  0
Total Rx errors     0            Total Tx errors      0
ProCurve Access Point 530(radio1-wlan1)#
```

Using the CLI to Configure Static WEP Shared Keys. The following example shows how to configure an SSID interface to use static WEP keys for authentication and encryption.

These commands enable security and establish the transfer key index (set to 4).

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security static-wep
ProCurve Access Point 530(radio1-wlan1)#wep-default-key 4
ProCurve Access Point 530(radio1-wlan1)#
```

The following commands set the wep key to an ascii type and sets the key length .

Note

Using the [no] version of the wep-key-ascii command sets the key type to Hex. You can set the wep-key-length to 64 or 128.

```
ProCurve Access Point 530(radio1-wlan1)#wep-key-ascii
ProCurve Access Point 530(radio1-wlan1)#wep-key-length 64
ProCurve Access Point 530(radio1-wlan1)#wep-key-4 pqrst
ProCurve Access Point 530(radio1-wlan1)#
```

The following commands set the actual key values for the wep keys.

Note

The number of characters required for each WEP key depends on the Key Length and Key Type settings:

- If Key Length is 64 bits and the Key Type is "ASCII", then each WEP key must be five (5) characters long.
- If Key Length is 40 bits and Key Type is "Hex", then each WEP key must be 10 characters long.
- If Key Length is 128 bits and Key Type is "ASCII", then each WEP Key must be 13 characters long.
- If Key Length is 128 bits and Key Type is "Hex", then each WEP Key must be 26 characters long.

```
ProCurve Access Point 530(radio1-wlan1)#wep-key-1 abcde
ProCurve Access Point 530(radio1-wlan1)#wep-key-2 fghi
ProCurve Access Point 530(radio1-wlan1)#wep-key-3 klmn
ProCurve Access Point 530(radio1-wlan1)#wep-key-4 pqrs
ProCurve Access Point 530(radio1-wlan)#
```

The following commands set the security to a shared-key authentication protocol.

Note

Supported authentications are: open system, shared key, or both.

Caution

Shared Key mode is seriously flawed, in that it utilizes the static WEP encryption key (transmitted openly) for station authentication. This allows the WEP encryption key to be easily discovered by anyone who might eavesdrop on the wireless network. If static WEP is configured, it is recommended to select Open System authentication.

```
ProCurve Access Point 530(radio1-wlan1)#shared-key-auth
ProCurve Access Point 530(radio1-wlan1)#no open-system-auth
ProCurve Access Point 530(radio1-wlan1)#
```

Using the CLI to Configure Dynamic WEP. The following example shows how to configure a WLAN (BSS/SSID) interface to use Dynamic WEP as the security method, configure an external authentication server and set the RADIUS key (the radius key is automatically provided if using the built-in authentication server).

Note

Supported authentication servers are: built-in authentication server on the access point or an external RADIUS server. The radius-key value is used with an external RADIUS server only and is ignored for the internal radius server. It should be set to the shared secret key that is configured on the external RADIUS server.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security dynamic-wep
ProCurve Access Point 530(radio1-wlan1)#radius primary ip
192.168.1.52
ProCurve Access Point 530(radio1-wlan1)#radius primary
port 161
ProCurve Access Point 530(radio1-wlan1)#radius primary key
secret
ProCurve Access Point 530(radio1-wlan1)#
ProCurve Access Point 530(radio1-wlan1)#
```

Using the CLI to Configure WPA-PSK. The following commands configure the access point to use the WPA-PSK security mode and to accept both the WPA and WPA2 stations.

Note

If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security wpa-psk
ProCurve Access Point 530(radio1-wlan1)#wpa-allowed
ProCurve Access Point 530(radio1-wlan1)#wpa2-allowed
ProCurve Access Point 530(radio1-wlan1)#
```

The following commands set the authentication to accept both the TPIK and CCMP (AES) protocols.

Note

On the default access point, cipher authentication is the TPIK protocol. When both TKIP and CCMP authentication methods are set, both TKIP and AES stations can associate with the access point. WPA stations must have either a valid TKIP or AES Key to communicate.

```
ProCurve Access Point 530(radio1-wlan1)#wpa-cipher-tkip
ProCurve Access Point 530(radio1-wlan1)#wpa-cipher-aes
ProCurve Access Point 530(radio1-wlan1)#
```

The following example shows how to set to set the security key value using the **wpa-pre-shared-key** command.

Note

Supported stations must be WPA-enabled and configured with the same personal key.

The personal-key must be a string of at least 8 characters to a maximum of 63 characters.

Shared secret keys can include spaces and special characters if the key is placed inside quotation marks (“goodsecret !”). If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary.

```
ProCurve Access Point 530(radio1-wlan1)#wpa-pre-shared-
key goodsecret
```

Using the CLI to Configure WPA-802.1X. The following commands configure the access point to use the WPA-802.1X security mode, to accept both the WPA and WPA2 stations, and to allow pre-authentication.

Note

WPA-802.1x is the recommended security mode. The incorporation of the RADIUS server makes it superior to the WPA-PSK security mode.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security wpa-802.1x
ProCurve Access Point 530(radio1-wlan1)#wpa-allowed
ProCurve Access Point 530(radio1-wlan1)#wpa2-allowed
ProCurve Access Point 530(radio1-wlan1)#rsn-preauthentication
ProCurve Access Point 530(radio1-wlan1)#
```

The following commands configure the built-in authentication server and authentications to the best security combination using the WPA Enterprise mode and the CCMP (AES) protocol.

Note

Supported authentication servers are: built-in authentication server on the access point or an external RADIUS server. Use of the built-in server automatically establishes the RADIUS key.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius primary ip
192.168.1.52
ProCurve Access Point 530(radio1-wlan1)#radius primary port
161
ProCurve Access Point 530(radio1-wlan1)#radius primary key
secret
ProCurve Access Point 530(radio1-wlan1)#
```

Configuring RADIUS Client Authentication

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

A primary RADIUS server (either using the built-in authentication server or specifying an external server) must be specified for the access point to implement IEEE 802.1X (802.1X) network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible. For details on configuring RADIUS Accounting servers, see "Web: Setting RADIUS Accounting Server Parameters" on page 5-43.

A RADIUS server can also be configured to provide MAC address authentication of wireless stations. If required, the access point can support both MAC address and 802.1X authentication using a RADIUS server. For more information, see "CLI: Configuring MAC Address Authentication" on page 7-40.

Note

This configuration guide assumes that you have already configured the RADIUS server(s) to support the access point. The configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Dynamic VLAN Assignment. A VLAN ID (a number between 1 and 4094) can be assigned to each client after successful authentication using IEEE 802.1X and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the access point assigns the user to the default VLAN ID of the associated WLAN(BSS/SSID) interface. For more information on the access point's VLAN support, see "Configuring VLAN Support" on page 5-48.

Note

VLAN IDs on the RADIUS server can be entered as a hexadecimal number or an ASCII string. The Access Point 530 requires that VLAN IDs be configured as an ASCII string.

To use dynamic VLAN, the access point must be using a security configuration that enables 802.1X authentication and have a RADIUS server configured (see page 7-35). Wireless stations must also support 802.1X station software to be assigned to a specific VLAN.

Web: Setting RADIUS Server Parameters

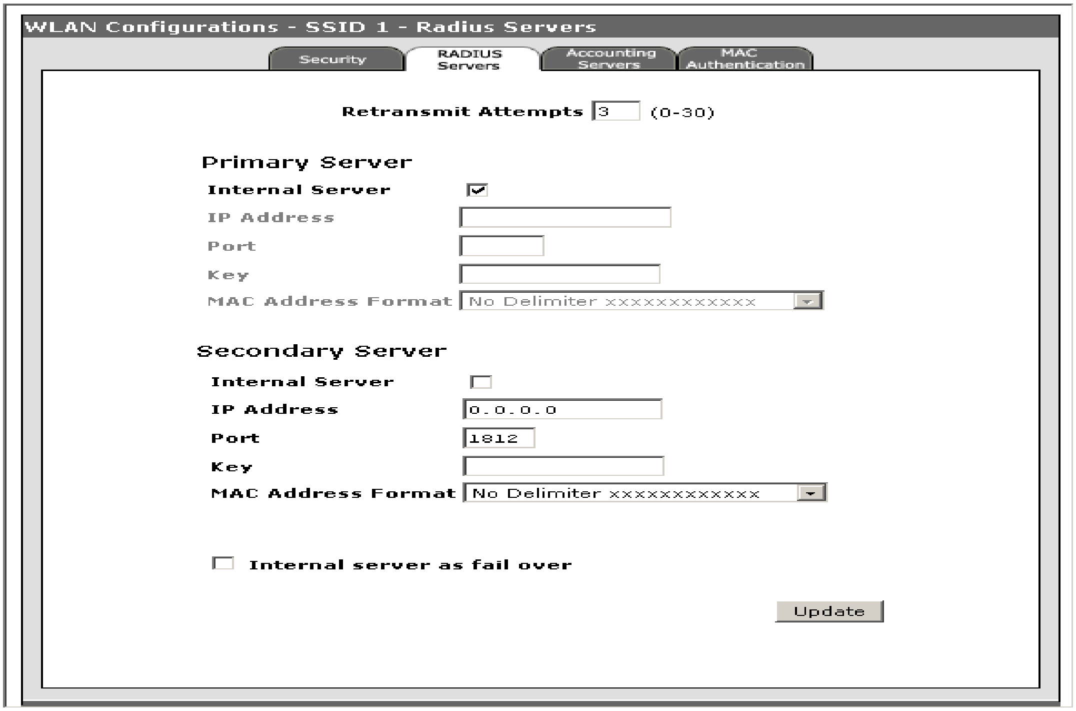
The RADIUS Servers tab provides setting of the primary and secondary server parameters on the access point. This establishes the RADIUS servers on the access point used to send user-session information to a configured RADIUS Accounting server. For details on configuring RADIUS Accounting servers, see "Web: Setting RADIUS Accounting Server Parameters" on page 5-43.

The Web interface allows modification of these parameters in order to use RADIUS Authentication on the access point:

- **Retransmit Attempts:** Sets the maximum transmission attempts to a RADIUS Accounting server. Range is 3 -30. (Default is 3)
- **Primary Server:** Configure the following settings to send user-session information from the access point to a RADIUS Accounting server.
  - **Internal Server:** Enables the access point to use the internal server for authentication. (Default is Enable)
  - **IP Address:** Specifies the IP address of the RADIUS server (Default is 0.0.0.0, which indicates Disabled).
  - **Port:** The User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication. (Default is 1812).
  - **Key:** A shared text string used to encrypt messages between the access point and the RADIUS server. **Be sure that the same text string is specified on the RADIUS Accounting server.** Do not use blank spaces in the string. (Maximum length: 20 characters)
  - **MAC Address Format:** Establishes the MAC Address format as either:
    - **No Delimiter** - MAC addresses are in the form xxxxxxxxxxxx. (default)
    - **Single Dash** - MAC addresses are in the form xxxxxx-xxxxxx.
    - **Multi Dash** - MAC addresses are in the form xx-xx-xx-xx-xx-xx.
    - **Multi Colon** - MAC addresses are in the form xx:xx:xx:xx:xx:xx.
- **Secondary Server Setup:** Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodi-

cally attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role. (Default is Disable)

- **Internal Server as Failover:** Enables the internal server to begin authenticating in the event that the primary server is disconnected. (Default is Disabled)



WLAN Configurations - SSID 1 - Radius Servers

Retransmit Attempts 3 (0-30)

Primary Server

Internal Server ☑

IP Address

Port

Key

MAC Address Format No Delimiter xxxxxxxxxxxx

Secondary Server

Internal Server ☐

IP Address 0.0.0.0

Port 1812

Key

MAC Address Format No Delimiter xxxxxxxxxxxx

☐ Internal server as fail over

Figure 7-5. Configuring RADIUS Servers on the Access Point

To Set RADIUS Server Parameters:

1. Select Network Setup> WLANs tab >WLAN (BSS/SSID) interface > **[Edit]** button > RADIUS Servers Tab.

2. Enter **the maximum number of retransmission attempts** to be made in the Retransmit Attempts text field.

3. Select **Internal Server** to establish the internal server parameters as the RADIUS server. If selected, proceed to step 8. If not selected, continue to steps 4 -8.

4. For the primary RADIUS server, type the **IP address** in the Radius IP text field.
5. In the Port text field, specify the UDP **port number** used by the RADIUS server.
6. In the Key text field, specify the shared **text string** that is also used by the RADIUS server.
7. (Optional) If you need to configure a secondary RADIUS server in the network, specify its IP address and other parameters in the appropriate fields. Otherwise, leave the IP address as all zeros (0.0.0.0).
8. Select **Internal Server as failover** to ensure RADIUS authentication remains uninterrupted should the primary server disconnect.
9. Click **[Update]** to set the RADIUS servers for RADIUS authentication.

CLI: Setting RADIUS Server Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] radius failover-to-local | retransmit	9-54
[no] radius <primary | secondary>	9-55

The following example shows how to configure RADIUS authentication failover and the RADIUS retransmit retry parameter for this WLAN.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius failover-to-
local
ProCurve Access Point 530(radio1-wlan1)#radius retransmit 30
```

The following example shows how to configure RADIUS primary or secondary parameters for this WLAN.

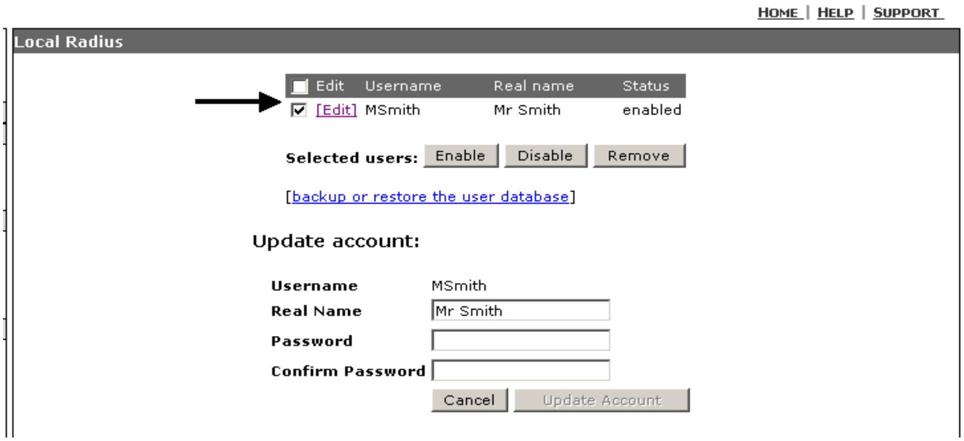
Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius primary key
open
ProCurve Access Point 530(radio1-wlan1)#radius primary ip
192.168.1.53
ProCurve Access Point 530(radio1-wlan1)#radius primary mac-
format mutli-colon
ProCurve Access Point 530(radio1-wlan1)#
```

Web: Establishing Local RADIUS Accounts

The Local Radius tab displays the existing local RADIUS accounts configured on the access point:

- **Username:** Displays the user name assigned to the account.
- **Real Name:** Displays the real name assigned to the account.
- **Status:** Displays the status of the account (Enabled or Disabled).
- **[Enable]:** Allows enabling of a disabled account.
- **[Disable]:** Allows disabling of an enabled account.
- **[Remove]:** Allows system removal of an account.



□ Edit	Username	Real name	Status
☑ [Edit]	MSmith	Mr Smith	enabled

Selected users: Enable Disable Remove

[backup or restore the user database]

Update account:

Username	MSmith
Real Name	Mr Smith
Password	
Confirm Password	

Figure 7-6. Configuring An Existing Account

To Modify an Existing Local RADIUS Account:

1. Select Special Features > Local Radius tab.
2. Select the account to modify.
3. To enable the account, click **[Enable]**.
4. To disable the account, click **[Disable]**.
5. To remove the account from the system, click **[Remove]**.

The Local Radius tab allows you to modify these RADIUS account details to use RADIUS authentication on the access point:

- **Add User Account:** Configure the following account details. The access point limits the local radius account users to 100.
  - **Username:** Provides an alphanumeric text string of up to 50 characters. Do not use special characters or spaces.
  - **Real Name:** Provides a text string of up to 50 characters.
  - **Password:** Provides a string with a minimum of 1 character and a maximum of 32 characters. Do not use special characters or spaces.
  - **Confirm Password:** Repeats the same string with a minimum of 1 character and a maximum of 32 characters.
  - **[Cancel]**: Cancels the add user account operation.
  - **[Add User]:** Updates the access point with the new user account information.

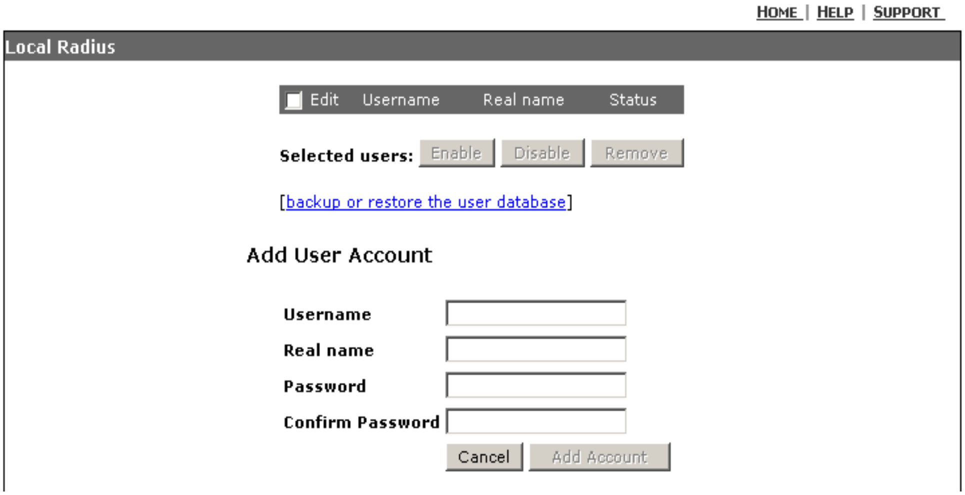


Figure 7-7. Configuring A Local Radius User

To Add Local RADIUS User Accounts:

1. Select Special Features > Local Radius > Users tab.
2. In the User Name text field, specify the **User Name** used by the RADIUS server for authentication.
3. In the Real Name text field, specify the **full name of the user** that is only used by the RADIUS server for informational purposes.
4. In the Password text field, specify the **password** to be associated with the User Name, the RADIUS server utilizes for authentication.
5. In the Confirm Password text field, enter the **password** a second time for confirmation (the two password entries must match exactly to be accepted).
6. Click **[Add Account]** to set the user account.

The User Database tab allows you to create a backup file. Once you have created User Accounts for use with Local RADIUS, you can save the account information to a "backup" file, which can then be used to "restore" the Local RADIUS User Accounts if needed.

- **[Backup User Database]**: Backs up the user database.
- **Restore User Database /[Browse]:** Allows browsing for a restore file (.ubk). The selected file displays in the Restore User Database field.
- **[Restore]:** Restores selected file.
- **Return to Local Radius /[Return]:** Returns to the Local Radius window.

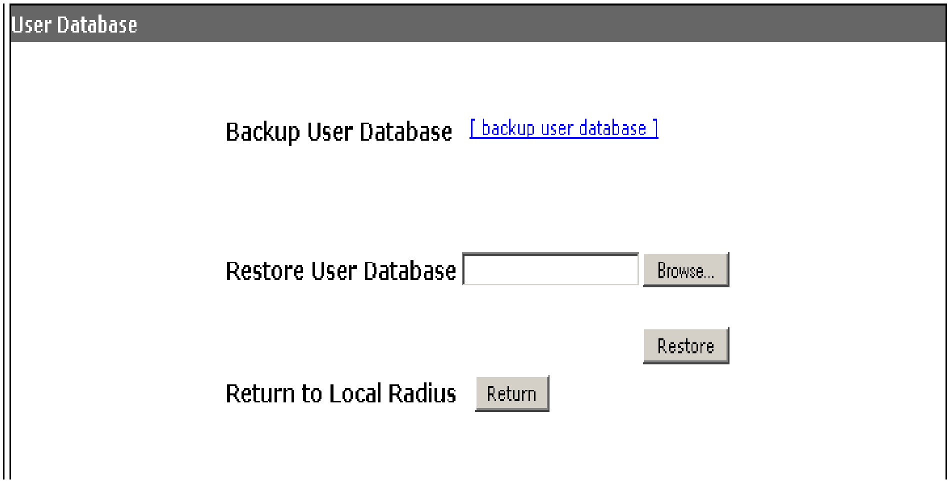


Figure 7-8. Backing Up A User Database

To Make A Backup File of Local RADIUS User Accounts Information:

1. Select Special Features > Local Radius to display the Local RADIUS window and user account information.
2. Click **[backup or restore user database]** link to display the User Database window.
3. Click **[backup user database]**.
4. A confirmation pop-up displays, click **Save** to continue (or Cancel to exit).
5. In the "Save As" dialogue window, select the **location (folder)** where the file will be saved.
   The default file name is wirelessUsers.ubk. You can edit the filename but do not change the file extension (.ubk)
6. Click **Save** to complete the process. The backup file will be placed in the specified folder.

To Restore the Local RADIUS User Accounts from a user database backup: 7.

1. Select Special Features > Local Radius to display the Local RADIUS window and user account information.
2. Click **[backup or restore user database]** link to display the User Database window.
3. Use **[Browse..]** to select the user database file (.ubk file) you want to restore.
   The selected file (pathname/filename.ubk) displays in the Restore User Database field.
4. Click **[Restore]** to complete the process.
5. Click **[Return]** to close the User Database window and return to the Local Radius window.

CLI: Setting Local RADIUS Server Parameters

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
[no] radius-local <*username*> **[Disabled]** **[password**<*password*>**]** **[realname**<*realname*>**]**	9-57
vlan<*id*>	9-116
show radius-local	9-58

The following example shows how to configure local RADIUS server parameters, including adding a new user, disabling existing user, removal of the user from the local database.

Note

Supported authentication servers are: local (built-in) RADIUS server on the access point or an external RADIUS server. The local (built-in) RADIUS server does not support assignment of VLAN IDs based on user authentication. An external RADIUS server is required to support assignment of VLAN IDs based on authentication of an individual user. If using the local (built-in) RADIUS server, the RADIUS accounting feature must be disabled and or set to us an external RADIUS accounting server.

.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radius-local newuser
ProCurve Access Point 530(config)# radius-local existinguser
Disabled
ProCurve Access Point 530(config)# no radius-local
existinguser
ProCurve Access Point 530(config)#
```

The following example first sets the radius-local username to "chris" and subsequently sets the password for the chris user account to "chrisopen".

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radius-local chris
realname csmith
ProCurve Access Point 530(config)# radius-local chris
password chrisopen

ProCurve Access Point 530(config)#
```

To display the current local RADIUS servers from the Manager Exec level, use the **show radius-local** command, as shown in the following example.

Example

```
ProCurve Access Point 530# config
ProCurve Access Point 530(config)# show radius-local
Local-Radius User Accounts (wireless client authentication:
Username   Real Name  Status
---------- ---------- ----------
chris      csmith     Enabled

ProCurve Access Point 530(config)#
```

Configuring MAC Address Authentication

The access point can be configured to authenticate client MAC addresses against a database stored locally on the access point or remotely on a RADIUS server. Station MAC addresses in the local database can be specified as allowed or denied access to the network. This enables the access point to control which devices can associate with the access point.

Note

If a RADIUS authentication server is used for MAC authentication, the server must first be configured in the RADIUS servers window. For details on configuring RADIUS servers, see "Web: Setting RADIUS Server Parameters" on page 7-28.

Client station MAC authentication occurs prior to any IEEE 802.1X authentication configured for the access point. However, a client's MAC address provides relatively weak user authentication, since MAC addresses can be easily captured and used by another station to break into the network. Using 802.1X provides more robust user authentication using user names and passwords or digital certificates. So, although you can configure the access point to use MAC address and 802.1X authentication together, it is better to choose one or the other, as appropriate. Consider the following guidelines:

- Use MAC address authentication for a small network with a limited number of users. MAC addresses can be manually configured on the access point itself without the need to set up a RADIUS server. The access point supports up to **200** MAC addresses in its filtering table, but managing a large number of MAC addresses across more than one access point quickly becomes very cumbersome.
- Use IEEE 802.1X authentication for networks with a larger number of users and where security is the most important issue. A RADIUS server is required in the wired network to control the user credentials (digital certificates, smart cards, passwords, or other) of wireless stations. The 802.1X authentication approach provides a standards-based, flexible, and scalable solution that can be centrally managed.

Note

On dual-radios, MAC filtering settings apply to both radios.

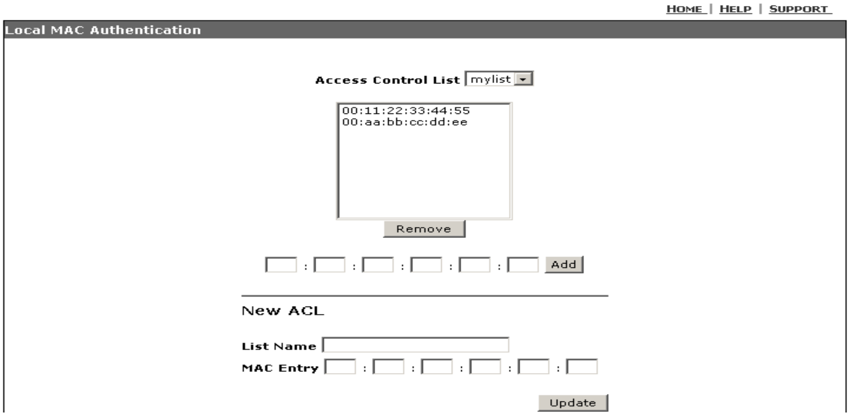
If you choose to configure RADIUS MAC authentication and 802.1X together, the RADIUS MAC address authentication occurs before 802.1X authentication. If the RADIUS MAC authentication is successful, 802.1X authentication is performed. When RADIUS MAC authentication fails, 802.1X authentication is not performed.

Web: Configuring Access Control List

The Local MAC Authentication tab allows creation and maintenance of ACLs which can be directly applied to each WLAN for access control.

The Web interface enables you to modify these parameters:

- **Access Control List** Allows selection of pre-configured ACL Lists.
- **[Remove]**: Updates the WLAN (BSS/SSID) interface by removing (prohibiting) the selected MAC configuration.
- **Field Entry/[Add]**: Adds the entered MAC address to the selected ACL list.
- **List Name:** Allows specification of new list name.
- **MAC Entry:** Allows entry of MAC Address for list.
- **[Remove]**: Updates the WLAN (BSS/SSID) interface by removing (prohibiting) the selected MAC configuration.



Access Control List: mylist

00:11:22:33:44:55
00:aa:bb:cc:dd:ee

List Name
MAC Entry

Figure 7-9. Configuring an Access Control List

To Configure Access Control List:

1. Select Management> Local MAC Authentication tab.
2. Enter the **ACL name** in the List Name text field.
3. Enter the **MAC address** in the MAC Entry text field.

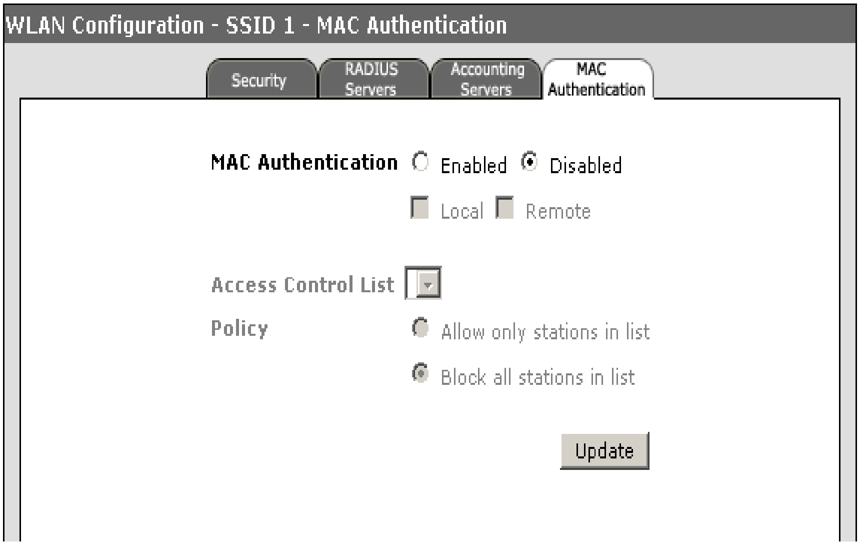
4. Click **[Update]** and the new list appears in the **ACL List** drop-down.

Web: Configuring MAC Address Authentication

The MAC Authentication tab enables the WLAN (BSS/SSID) interface to be configured to use with MAC Authentication.

The Web interface enables you to modify these parameters:

- **MAC Authentication:** Provides configuration of either the local or remote MAC authentication on this access point. Selecting the enable option allows selection of the Local or Remote parameters.
- **Access Control List** Allows selection of pre-configured ACL Lists.
- **Policy:** Allows or prohibits specified station addresses.
- **[Update]**: Updates the WLAN (BSS/SSID) interface with the selected MAC configuration



WLAN Configuration - SSID 1 - MAC Authentication

MAC Authentication ○ Enabled ● Disabled

□ Local □ Remote

Access Control List

Policy ○ Allow only stations in list

● Block all stations in list

Figure 7-10. Configuring Built-In MAC Authentication

To Configure Built-In MAC Authentication:

1. Select Network Setup> WLANs tab >WLAN (BSS/SSID) interface > **[Edit]** button > Mac Authentication Tab.

If you have already created a new ACL list, proceed to step 2. If you have not created the ACL list, see "To Configure Access Control List:" on page 7-38.

2. To enable local or remote MAC authentication, select **enable** and choose **local** or **remote**.
3. To apply a configured authentication list, select **list** from the ACL drop-down.
4. To prohibit specific MAC addresses from gaining access to the network, select **Block all stations in list** policy option.
5. To allow only known MAC addresses access to the network, select **Allow only stations in list** policy option.
6. Click **[Update]** to set MAC Authentication on the access point.

CLI: Configuring MAC Address Authentication

CLI Commands Used in This Section

Command Syntax	CLI Reference Page
mac-auth-local <*listname*> **<**accept listl deny list**>**	9-60
mac-auth-local <*listname*> **mac<***mac_address***>**	9-60
show mac-auth-local	9-62

Configuring Local MAC Authentication Lists. The following example shows how to create a list of MAC addresses for authentication.

NOTE

The address format is a 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by periods, for example FE:DC:BA:09:87:65.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#mac-auth-local mylist mac
00:11:22:33:44:55
ProCurve Access Point 530(config)# mac-auth-local mylist mac
00:aa:bb:cc:dd:ee
ProCurve Access Point 530(config)#
```

Creating a MAC accept list. The following example shows how to configure a MAC address to the accept list.

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#wlan 1
ProCurve Access Point 530(radio-wlan1)#mac-auth-local mylist
accept-list
ProCurve Access Point 530(radio-wlan1)#
```

Displaying MAC Authentication Settings. The following example shows how to display the current authentication configuration on the access point from the Manager Exec level.

```
ProCurve Access Point 530#show mac-auth-local mylist
MAC address authentication control list “mylist”:

MAC Addresses
---------------------------------------------------------------------------
00:11:22:33:44:55
00:aa:bb:cc:dd:ee

ProCurve Access Point 530#
```

Validating the list was set on the WLAN. The following example shows how to view the newly created list using the show wlan command.

```
ProCurve Access Point 530(radio1-wlan1)# show wlan 1
WLAN #1 on Radio 1
Description   Radio 1 - WLAN 1
Status        Enabled                SSID   SSID 1
VLAN          1    - Untagged        BSSID  00:14:C2:A5:22:E0
DTIM Period   2

Security Type   no-security (No Sec.)          Closed System   Disabled
MAC Auth Mode   local accept-list only         MAC Auth List   mylist
Authentication  open-system only               WEP Key Type    hex
WEP Key 1       not set                        WEP Key Size    128bit
WEP Key 2       not set                        Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
WPA or WPA2     WPA and WPA2                   WPA Cipher      TKIP only
WPA Pre-auth.   Disabled
WPA Shared Key  not set

RADIUS
Failover To Local   Disabled                   Retransmit Num.  3
Primary Auth        not set                    Prim. Auth Port  1812
Prim. Auth Key      not set
Secondary Auth      not set                    Sec. Auth Port   1812
Sec. Auth Key       not set
Primary Acct        not set                    Prim. Acct Port  1813
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

Special Features

Contents

Overview

The Access Point 530 provides the Web interface and CLI methods to configuring special features such as; QoS, upgrading software, WDS, AP Detection, and STP.

This Chapter describes how to:

- Configure QoS parameters
- Maintain Configuration and Upgrade Files
- Modify WDS parameters
- Enable AP Detection
- Configure STP via CLI

QoS Commands

QoS describes a range of technologies for controlling traffic on shared network connections. The IEEE 802.11e - 2005 standard defines a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion, limiting jitter, latency, and packet loss; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

QoS on WLAN can be achieved by two ways: by prioritized access to the channel, and by "parameterized" access to the channel. The prioritized access to the channel implementation is called Wireless Multimedia (WMM) and parameterized access to the channel is called WSM.

802.11e ratified specification for wireless QoS enhancements, includes packet prioritization, scheduled access, and call admission control. Eager to spur interoperability among multi-vendor wireless gear, the Wi-Fi Alliance created a certification process on a subset of 802.11e called Wi-Fi Multi-media (WMM). WMM provides four categories of relative QoS - voice, video, best-effort and background. Wi-Fi Alliance based certification, including WMM, is supported by many leading wireless vendors including ProCurve.

Both access points and wireless stations (laptops, consumer electronics products) should be WMM-enabled in order to utilize this QoS feature.

CAUTION

The default WMM parameters settings are usually adequate for WMM operation. Incorrect WMM settings can adversely affect network performance. Changes to WMM parameters should be reserved for someone with an advanced knowledge of how WMM operates. For more on WMM, see the IEEE 802.11e standard.

Web: Configuring QoS Parameters

The QoS window provides initial enabling of the QoS parameters.

The Web interface enables you to modify these parameters:

- **WiFi Multimedia (WMM):** Enables/Disables QoS prioritization and coordination of wireless medium access. The QoS settings on the Access Point 530 control downstream traffic flowing from the access point to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the access point (station EDCA parameters). Disabling

WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point, however, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters). (Default is enabled).

- **[Advanced Settings]:** Launches the window to configure specific queue QoS parameters.
- **[Update]:** Updates the access point with the QoS details.

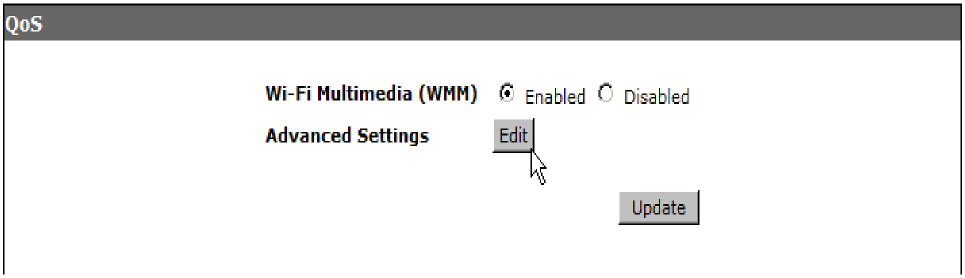
The Advanced Settings Parameter window provides configuration for specific queue QoS parameters.

The Web interface enables you to modify these parameters:

- **AP Enhanced Distributed Channel Access (EDCA) Parameters:** Affect traffic flowing from the access point to the client station.
  - **Queue:** Specifies which of the prioritization queues (defined for each type of data transmitted from AP-to-Station) to configure.
    - **Data 0 (Voice):** High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
    - **Data 1(Video):** High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
    - **Data 2 (Best effort):** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
    - **Data 3 (Background):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
  - **AIFs:** Arbitration Inter-Frame Spacing (AIFS) specifies a wait time in milliseconds for data frames. Valid values are: 1-255. (Default per queue: 1, 1, 3. 7).
  - **cwMin:** Specifies the Minimum Contention Window QoS parameter. The value specified is the lower limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmin" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmin" must be lower than the value for "cwmax". (Default per queue: 3, 7, 15, 15).
  - **cwMax*:*** Specifies the Maximum Contention Window QoS parameter. The value specified is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". (Default per queue: 7, 15, 63, 1023).

  - **Burst:** Specifies the Maximum Burst Length QoS parameter. This value specifies the length of time allowed for a packet burst (collection of transmitted multiple frames w/out header information) on a wireless network.Valid values for maximum burst length are 0.0 through 999.9. (Default per queue: 1.5, 3, 0, 0)

- **Station Enhanced Distributed Channel Access (EDCA) Parameters:** Affect traffic flowing from the client station to the access flow.
  - **Queue:** Specifies which of the prioritization queues (defined for each type of data transmitted from AP-to-Station) to configure.
    - **Data 0 (Voice):** High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
    - **Data 1(Video):** High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
    - **Data 2 (best effort):** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
    - **Data 3 (Background):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
  - **AIFs:** Arbitration Inter-Frame Spacing (AIFS) specifies a wait time in milliseconds for data frames. Valid values are: 1-255. (Default per queue: 2, 2, 3. 7).
  - **cwMin:** Specifies the Minimum Contention Window QoS parameter. The value specified is the lower limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmin" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmin" must be lower than the value for "cwmax". (Default per queue: 3, 7, 15, 15).
  - **cwMax***:* Specifies the Maximum Contention Window QoS parameter. The value specified is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". (Default per queue: 7, 15, 1023, 1023).
  - **TXOP Limit:** Specifies the Transmission Opportunity QoS parameter. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network. Valid values are 0.0 through 999.9. (Default per queue: 47, 94, 0, 0)

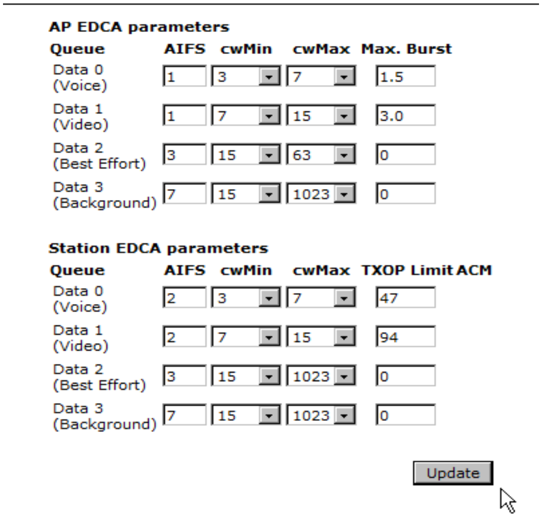


QoS

Wi-Fi Multimedia (WMM) ● Enabled ○ Disabled

Advanced Settings

Figure 8-1. Initial QoS Window



AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit	ACM
Data 0 (Voice)	2	3	7	47	
Data 1 (Video)	2	7	15	94	
Data 2 (Best Effort)	3	15	1023	0	
Data 3 (Background)	7	15	1023	0	

Figure 8-2. QoS Advanced Settings Window

To Modify QoS Parameters:

1. Select Special Features > QoS.
2. To set the prioritization of QoS, select **Enable** for the WMM option.
3. Select **Advanced Settings** to set queue QoS parameters on the Advanced window.
4. To affect the flow from the access point to the client station (downstream), update **AP EDCA** parameter options.
5. To affect the flow from the client station to the client station (upstream), update **Station EDCA** parameter options.
6. Click **[Update]** to save the settings.

CLI: Configuring QoS Parameters

CLI Commands Used in This Section

Command	CLI Reference Page
qos ap-params <voice|video|best-effort|background> {<[**aifs** *<aifs>*] [**cwmin** *<swmin>*] [**cwmax** *<cwmax>]* [**burst** *<burst>*]}}	9-120
qos sta-params <voice|video|best-effort|background> {<[**aifs** *<aifs>*] [**cwmin** *<swmin>*] [**cwmax** *<cwmax>]* [**burst** *<burst>*]}	9-122
[no] **qos wmm**	9-124
show qos	9-125

Using the CLI to Configure QoS queues. This example sets the quality of service AIFS wait time parameter to 10 seconds on the AP EDCA medium priortiy queue.

```
ProCurve Access Point 530(radio1)#qos ap-params voice aifs
10
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service CWIM minimum and CMAX maximum contention window parameters on the AP EDCA medium priority queue. .

```
ProCurve Access Point 530(radio1)#qos ap-params video cwmin
1
ProCurve Access Point 530(radio1)#qos ap-params video cwmax
7
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service BURST parameter on the AP EDCA medium priority queue. .

```
ProCurve Access Point 530(radio1)#qos ap-params background
burst 1
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service AIFS wait time parameter to 10 seconds on the Station EDCA high priortiy queue.

```
ProCurve Access Point 530(radio1)#qos sta-params voice aifs
10
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service CWIM minimum and CMAX maximum contention window parameters on the Standard EDCA high priority queue. .

```
ProCurve Access Point 530(radio1)#qos sta-params video cwmin
1
ProCurve Access Point 530(radio1)#qos sta-params video cwmax
15
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service TXOP-LIMIT (transmission opportunity limit) parameter on the Standard EDCA high priority queue. .

```
ProCurve Access Point 530(radio1)#qos sta-params background
txop-limit 1
ProCurve Access Point 530(radio1)#
```

Using the CLI to Enable WME. This example enables using Wireless Multimedia Extensions as the preferred priority method, .

```
ProCurve Access Point 530(radio1-ssid1)#qos wmm
ProCurve Access Point 530(radio1-ssid1)#
```

This example uses the “show qos” commands to display qos details on the access point.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# show qos ap-params
------------------------------------------------------------
Transmission Queue QoS Settings for the Access Point:

Radio 1      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0

Radio 2      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0


ProCurve Access Point 530(radio1)# show qos sta-params
Transmission queue QoS settings for wireless stations:
Radio 1      Adaptive Inter-   Contention    Contention    Transmission
Queue        Frame Space       Min. Window   Max. Window   Opportunity Limit
------------------------------------------------------------------------------
Voice         2                 3             7             47
Video         2                 7             15            94
Best-Effort   3                 15            1023          0
Background    7                 15            1023          0

Radio 2      Adaptive Inter-   Contention    Contention    Transmission
Queue        Frame Space       Min. Window   Max. Window   Opportunity Limit
------------------------------------------------------------------------------
Voice         2                 3             7             47
Video         2                 7             15            94
Best-Effort   3                 15            1023          0
Background    7                 15            1023          0

ProCurve Access Point 530(radio1)#
```

Wireless Distribution System (WDS) and Spanning Tree Protocol (STP)

The Access Point 530 includes Wireless Distribution System (WDS) support allowing wireless connectivity between access points, instead of using a wired Ethernet connection. An Access Point 530 can be located where there is no available Ethernet connection and still provide wireless network connectivity to stations using a wireless uplink to another Access Point 530. A pair of Access Point 530 units can also be used to implement a point-to-point "wireless bridge", connecting two physically separated Ethernet subnets together without a cable connection between them.

When implementing a WDS link, the recommended practice is to dedicate one of the two radios in the Access Point 530 to servicing the WDS link. It is not recommended that the same WDS radio be configured to support wireless stations, although it is possible to do so. When a radio is configured to support both WDS and wireless stations, the data-handling capacity of the radio has to be split between these two separate activities. Thus any wireless station activity on the WDS radio will reduce the data-handling capacity of the WDS link for passing traffic from wireless stations associated to the radio.

It is also recommended practice to enable Spanning Tree Protocol (STP) whenever one or more WDS links are configured into a wireless network. STP is supported with WDS to manage loops that might be formed in the network through configuration of multiple WDS links. Without STP, loops can seriously degrade network operation. STP automatically identifies any potential network loops and dynamically manages network traffic to prevent loops from impacting network operation. The most common way of forming a loop is when both access points are connected with an Ethernet switch (for management purposes) and then a WDS link is established.

It is recommended you enable STP whenever WDS links are configured, unless you are assured that loops cannot occur in your network configuration. On the Access Point 530, STP is automatically enabled. As STP operation is applied at the WDS interfaces and Ethernet port, in order for proper STP operation, the switch to which the access point is connected needs to have STP enabled.

At least one Access Point 530 must be connected to the network using a wired Ethernet connection. This one Access Point 530 can then provide wireless WDS links for up to six other Access Point 530 units. In this configuration, the connected Access Point 530 (the one with the Ethernet connection) serves as a central access point to pass traffic to and from the other remote access points. This configuration is illustrated in Figure 8-3.

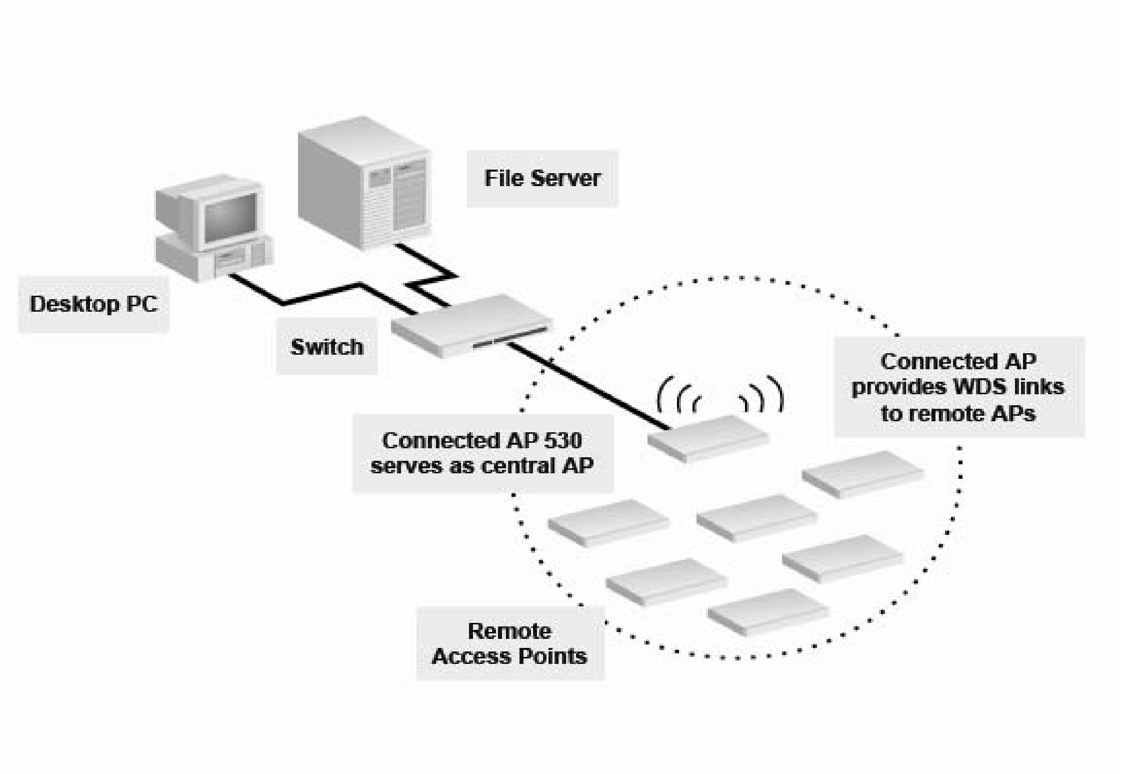

File Server
Desktop PC
Switch
Connected AP provides WDS links to remote APs
Connected AP 530 serves as central AP
Remote Access Points

Figure 8-3. Wired Access Point provides wireless WDS links to wireless access points

The Access Point 530 can be used as a wireless bridge to connect two different wired sub-networks together. For example, wired networks in two buildings across the street from one another can be interconnected by attaching an Access Point 530 to each separate network, and configuring with a WDS link between them. This is illustrated in Figure 8-4.

In this configuration, it is recommended that one radio on each access point be dedicated to the WDS link (to maximize WDS link throughput); the other radio can either be disabled, or used to service wireless stations.

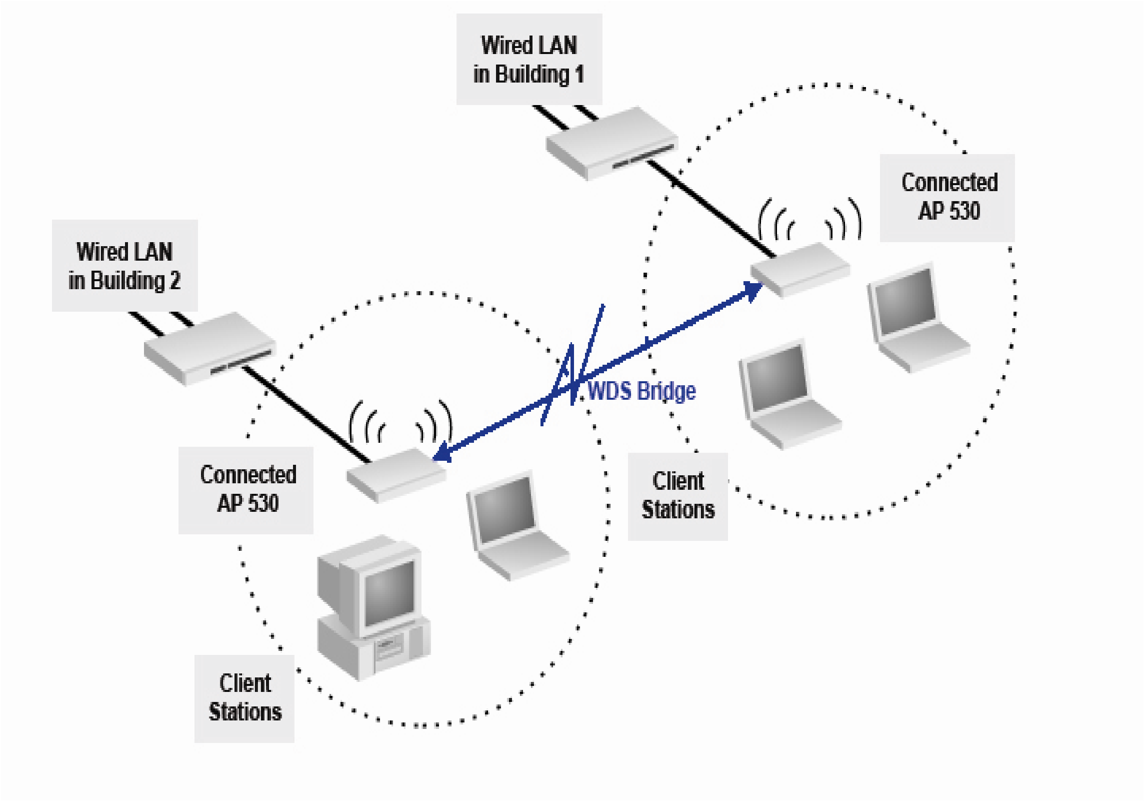


Figure 8-4. WDS Bridge between sub-networks

The Access Point 530 can also be configured to use WDS links in a multiple-hop configuration, as shown in Figure 8-5.

In this configuration, the intermediate access point serves as a "repeater", to bridge wireless traffic between an access point with an Ethernet connection and a more remote access point on the other side. All three access points in this configuration can support wireless stations in addition to bridging network traffic between one another.

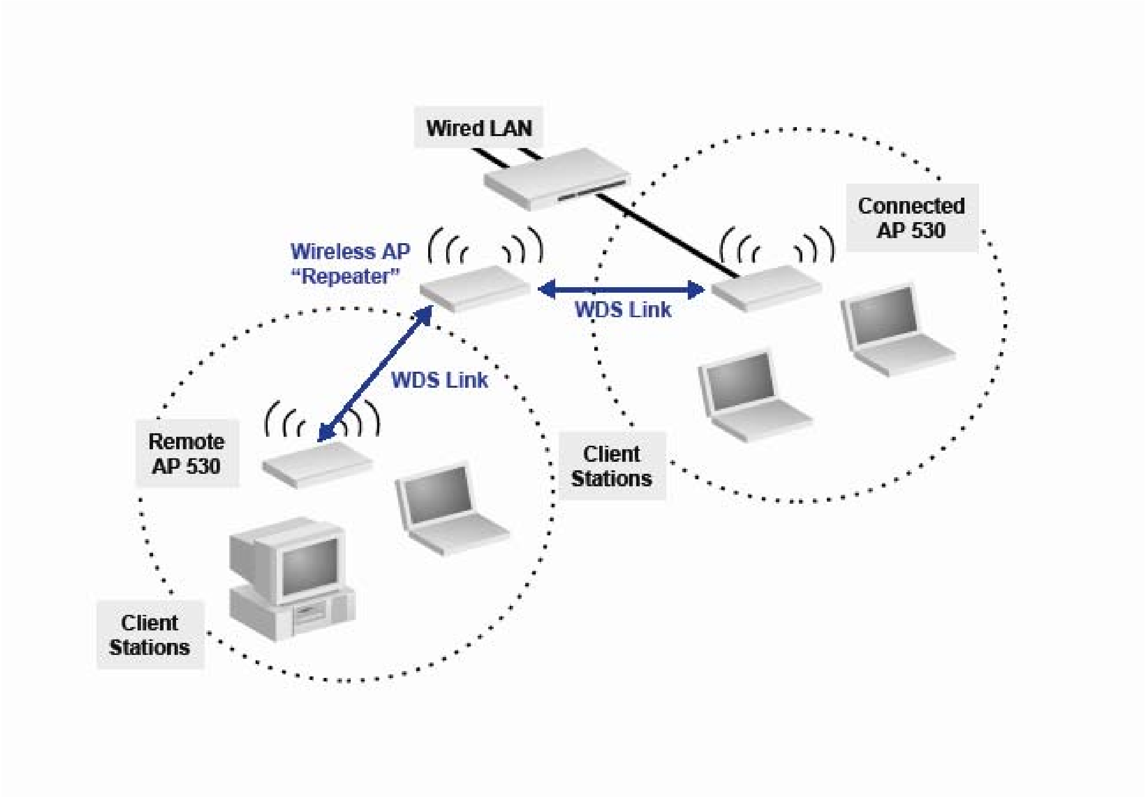


Figure 8-5. WDS Links with AP Repeater to Remote Access Point

Spanning Tree Protocol (STP) is supported with WDS to manage loops that might be formed in the network through configuration of multiple WDS links. Enabling STP is recommended whenever WDS links are configured, unless you are assured network loops cannot occur in your WDS configuration.

Note

When using WDS, be sure to configure WDS settings identical for both access points participating in a WDS link.

The security option for a WDS link is determined by the security option configured for WLAN 1 and is limited to a specific set of choices. See "Establishing Security" on page 7-12.

Important

Both access points participating in WDS link must be on the same Radio channel and use the same IEEE 802.11(802.11 a/b/g) mode.

Web: Configuring WDS Parameters

The WDS window provides configuration for wireless parameters.

The Web interface enables you to modify these parameters:

- **Spanning Tree Protocol Status:** Enables/Disables STP capabilities on the access point. (Default is Enabled)
- **Link (1-6):** Enables/Disables WDS link (1-6) capabilities on the access point. You can set up to six links on the access point. (Default is Disabled) If enabled is selected, the following parameters are enabled:
  - **Radio:** Selects radio for the WDS link. (Default is Radio 2)
  - **Local Address:** Populates local MAC address for the access point.
  - **Remote:** Enters remote MAC address or selects MAC address from pull-down menu (if AP detection is enabled).
  - **Security:** Displays pre-configured security based on the configured WLAN 1 security. See "WLAN 1 and WDS Security Configuration" on page 7-12.

    Depending on the type of WLAN Security selected, the following parameters are enabled:

    WDS WEP Security
    - **WEP:** Enables/Disables WEP security for the WDS link. If enabled, the key length, type, and characters are defaulted for the WDS window.
    - **Key Length:** Establishes length of the key as either 64 or 128 bits.
    - **Key Type:** Establishes type of the key as either ASCII or HEX.
    - **Characters Required:** Automatically populated based on the Key Length and Key Type.

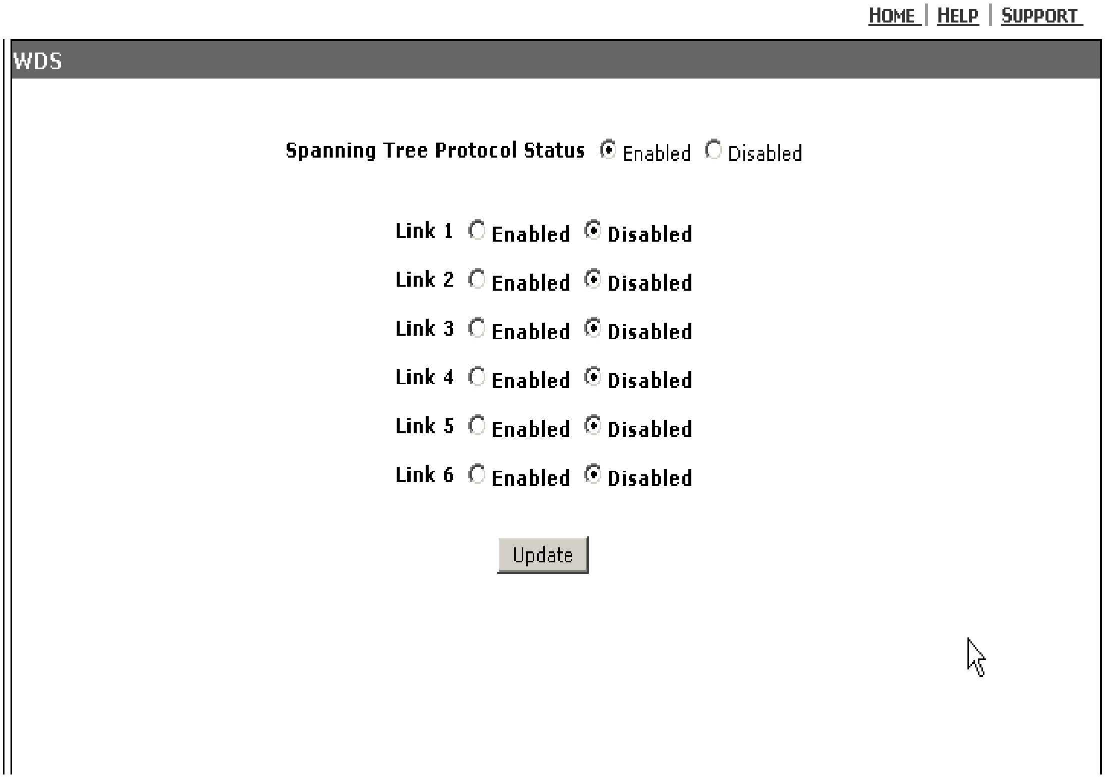
- **WEP Key:** Configures WEP key for security.

WDS WPA Security

- **SSID:** Establishes alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.

  Note: When using WPA over WDS, an SSID is required and must match the SSID on the WDS partner access point for successful operation.
- **Key:** Configures WPA key for security.

- **[Update]:** Updates the WDS link parameters.



Spanning Tree Protocol Status ● Enabled ○ Disabled

Link 1 ○ Enabled ● Disabled

Link 2 ○ Enabled ● Disabled

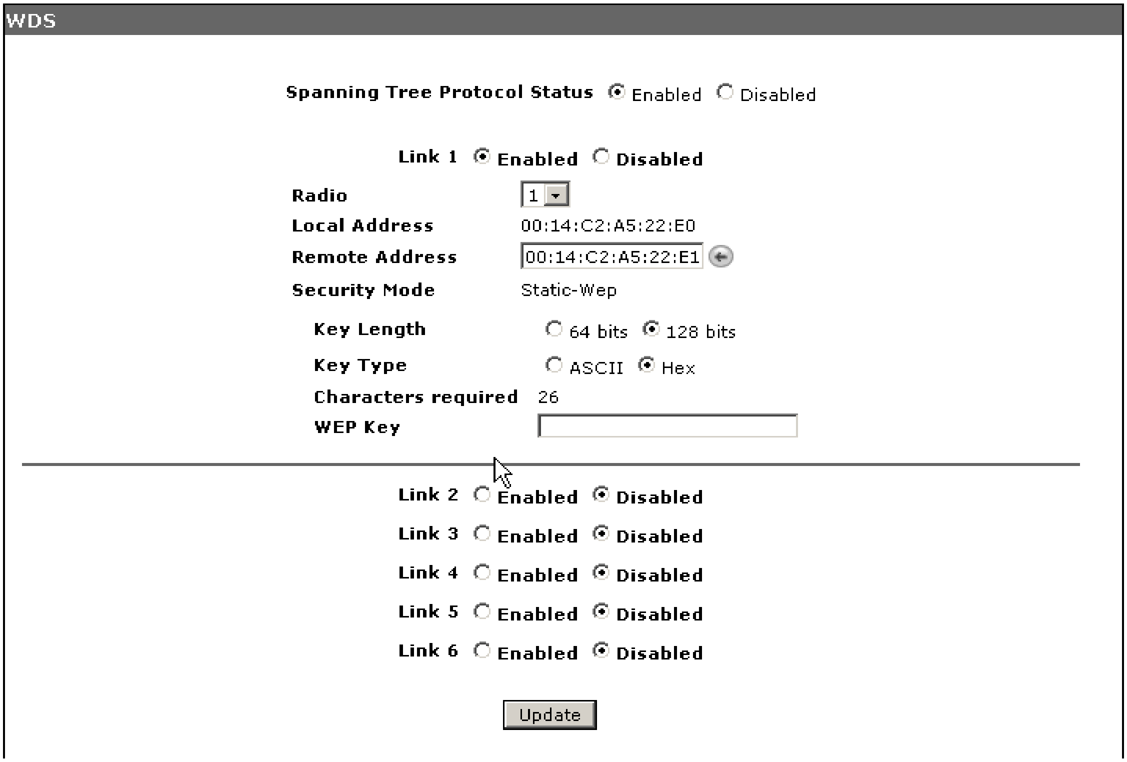
Link 3 ○ Enabled ● Disabled

Link 4 ○ Enabled ● Disabled

Link 5 ○ Enabled ● Disabled

Link 6 ○ Enabled ● Disabled

Figure 8-6. WDS Configuration Window



WDS

Spanning Tree Protocol Status ● Enabled ○ Disabled

Link 1 ● Enabled ○ Disabled

Radio 1

Local Address 00:14:C2:A5:22:E0

Remote Address 00:14:C2:A5:22:E1

Security Mode Static-Wep

Key Length ○ 64 bits ● 128 bits

Key Type ○ ASCII ● Hex

Characters required 26

WEP Key

Link 2 ○ Enabled ● Disabled

Link 3 ○ Enabled ● Disabled

Link 4 ○ Enabled ● Disabled

Link 5 ○ Enabled ● Disabled

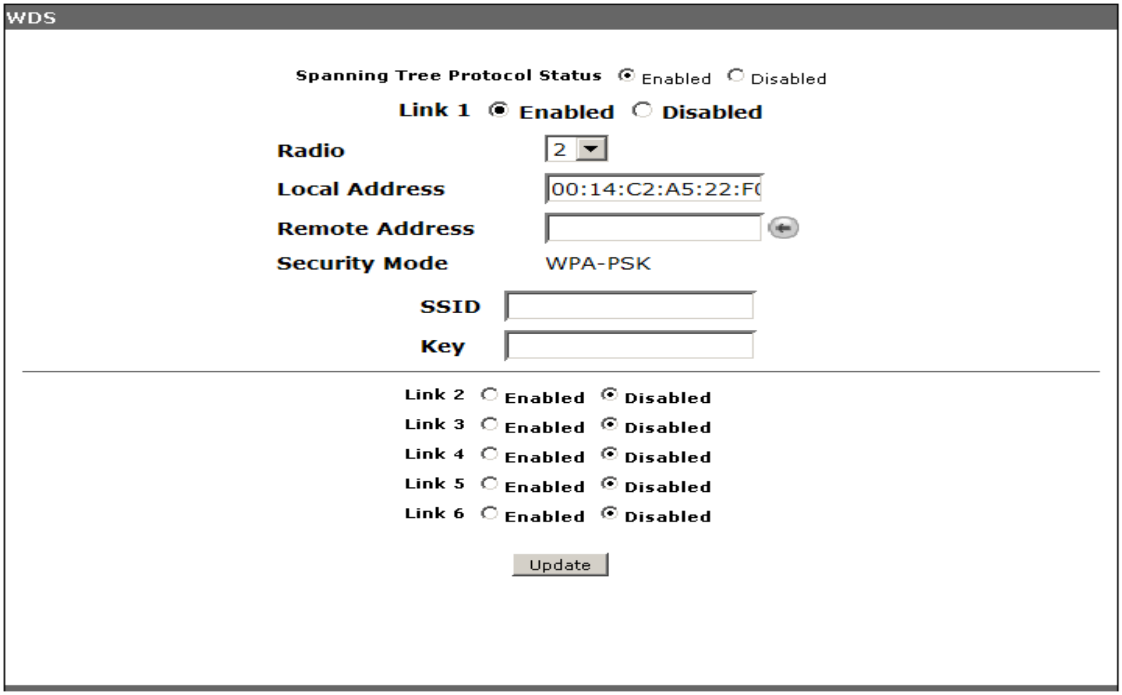
Link 6 ○ Enabled ● Disabled

Figure 8-7. Configuring WDS Link Parameters with WEP Security

To Configure WDS Link Parameters with WEP Security:

1. Select Special Features > WDS tab.
2. To enable a WDS link, choose **Enabled** for the specific link option.
3. To set the radio to establish the WDS link, use the **Radio** drop-down.
4. Enter the **remote MAC Address** or, if AP detection is enabled, select the **remote MAC Address** from the drop down menu of the access point to which you are trying to establish the WDS link.

   The Security Mode is pre-configured when the WLAN Security is configured. See "WLAN 1 and WDS Security Configuration" on page 7-12.
5. Modify defaulted **key length and key type**, if necessary.
6. Enter the **WEP Key,** adhering to previous set key parameters.
7. Click **[Update]** to save the settings.



WDS

Spanning Tree Protocol Status ● Enabled ○ Disabled

Link 1 ● Enabled ○ Disabled

Radio 2

Local Address 00:14:C2:A5:22:F(

Remote Address

Security Mode WPA-PSK

SSID

Key

Link 2 ○ Enabled ● Disabled

Link 3 ○ Enabled ● Disabled

Link 4 ○ Enabled ● Disabled

Link 5 ○ Enabled ● Disabled

Link 6 ○ Enabled ● Disabled

Figure 8-8. Configuring WDS Link Parameters with WPA Security

To Configure WDS Link Parameters with WPA Security:

1. Select Special Features > WDS tab.

2. To enable a WDS link, choose **Enabled** for the specific link option.

3. To set the radio to establish the WDS link, use the **Radio** drop-down.

4. Enter the **remote MAC Address** or, if AP detection is enabled, select the **remote MAC Address** from the drop down menu of the access point to which you are trying to establish the WDS link..

   The Security Mode is pre-configured to “WPA-PSK”, when WLAN 1 Security is configured with either WPA-802.1X security or WPA-PSK. See “WLAN 1 and WDS Security Configuration” on page 7-12.

5. Enter the **SSID** name for the WDS link.

6. Enter the **WPA preshared key.**

7. Click **[Update]** to save the settings.

CLI: Configuring WDS Links

CLI Commands Used in This Section.

Command	CLI Reference Page
enable	9-129
radio-used *<1 /2 >*	9-130
remote-mac *<mac>*	9-131
wds-ssid *<ssid> (required when using WPA over WDS)*	9-130
wep-key-ascii	9-133
wep-key *<key>*	9-132
wep-key-length *<64/128>*	9-133
wpa-pre-shared-key *<key>*	9-134
show wds & show wds*<wds_name>*	9-131

Using the CLI to Enable WDS. This example enables the WDS link.

```
ProCurve Access Point 530(config)# interface wds1
ProCurve Access Point 530(wds1)#enable
```

Using the CLI to Set the WDS SSID. This command sets the WDS SSID string for this WDS link and establishes a pre-shared key.

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#interface wds1
ProCurve Access Point 530(wds1)#wds-ssid marge
ProCurve Access Point 530(wds1)#wpa-pre-shared-key
goodsecret
ProCurve Access Point 530(wds1)#
```

Using the CLI to Create A Radio Link. This example sets the radio used with this WDS link.

```
ProCurve Access Point 530(wds1)#radio-used 1
```

Using the CLI to Set Remote MAC. This example sets the remote MAC address associated with this WDS link. Valid format is 00:00:00:00:00:00~FF:FF:FF:FF:FF:FF.

```
ProCurve Access Point 530(wds1)#remote-mac 00:0D:9D:C6:98:7E
```

This example sets the WDS WEP key type to ASCII when using static-wep security. The no version of the command sets the key type to hexadecimal.

.

```
ProCurve Access Point 530(wds1)# wep-key-ascii
ProCurve Access Point 530(wds1)#
```

This example sets the WDS WEP key length when using static-wep security. The options are 64 or 128.

```
ProCurve Access Point 530(wds1)# wep-key-length 64
ProCurve Access Point 530(wds1)#
```

This example defines the wep-key used for data encryption on an WDS interface.

```
ProCurve Access Point 530(wds1)# wep-key abcde
ProCurve Access Point 530(wds1)#
```

Using the CLI to View WDS Parameters. This example uses the show wds command to see the status of the WDS links.

```
ProCurve Access Point 530(wds1)#show wds

#Radio  Local MAC           Remote MAC          Status     Security
-----------------------------------------------------------------------------
1   2   00:14:C2:A4:14:BO   00:0D:9D:C6:98:7E   Enabled    no-security
2   2   00:14:C2:A4:14:AO   00:11:33:C6:88:EE   Disabled   no-security
3   2   not assigned yet    not set             Disabled   no-security
4   2   not assigned yet    not set             Disabled   no-security
5   2   not assigned yet    not set             Disabled   no-security
6   2   not assigned yet    not set             Disabled   no-security

ProCurve Access Point 530(wds1)#
```

```
ProCurve Access Point 530(wds1)#show wds 1
WDS #1
Description  WDSLINK
Status       Enabled            Use Radio   1
Local MAC    00:14:C2:A4:14:BO  Remote MAC 00:0D:9D:C6:98:7E
STP State    forwarding         WDS SSID    marge

Security Type  no-security (from WLAN 1)WEP Key Type  hex
WEP Key        not set                  WEP Key Size  128bit
WPA Key        goodsecret

Bytes Rx            3562         Bytes Tx              7234
Packets Rx          0            Packets Tx            0
Compressed Rx       0            Compressed Tx         0
Mcast packets Rx    0            Carrier errors Tx     0
Dropped Rx packets  0            Dropped Tx packets    0
FIFO overflows Rx   0            FIFO overflows Tx     0
Frame errors Rx     0            Packet collisions Tx  0
Total Rx errors     0            Total Tx errors       56

ProCurve Access Point 530(wds1)#
```

Web: Configuring STP Parameters

The WDS window in the Web browser interface provides global configuration for the Spanning Tree Protocol. To modify additional details specific to STP, see "CLI: Establishing STP Settings" on page 8-22" .

The Spanning Tree Protocol (STP) is an IEEE 802.11 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between network devices.

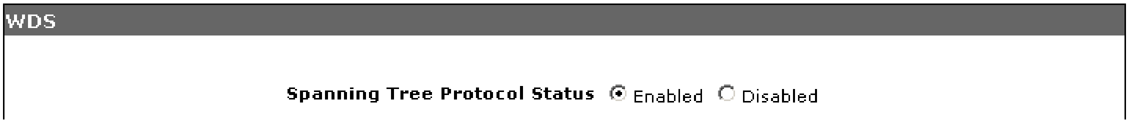
Loops occur when there are multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state. STP allows only one active path at a time between any two network devices (this prevents the loops), but establishes the redundant links as a backup if the initial link should fail.

If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm re-configures the spanning tree topology and reestablishes the link by activating the standby path. Without STP in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

Essentially, STP is used to avoid redundant loops in layer 2.

The Web interface enables you to modify this STP parameter:

- **Spanning Tree Protocol Status:** Enables/Disables STP capabilities on the access point. (Default is Enabled) For WDS parameter details, see "Web: Configuring WDS Parameters" on page 8-14



Spanning Tree Protocol Status ● Enabled ○ Disabled

Figure 8-9. Configuring STP Parameters

To Modify STP Parameters:

1. Select Special Features > WDS tab.
2. To enable STP, choose **Enabled** for the STP option.
3. Click **[Update]** to save the settings.

CLI: Establishing STP Settings

CLI Commands Used in This Section.

Command	CLI Reference Page
[no] **stp [hello-time** *<value>*] **[forward-delay** *<value>*] **[priority** <value>**]**	9-135
show interface ethernet	9-73

NOTE

This STP configuration is only available through the CLI and not through the Web browser interface.

Using the CLI to Establish STP Settings. This example configures Spanning Tree Protocol settings for the device. The no version of the command disables STP on the device.

The hello-time range is 1-10, the forward-delay range is 4-30, and the bridge priority range is 0-65535.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# stp hello-time 10
ProCurve Access Point 530(config)# stp forward-delay 10
ProCurve Access Point 530(config)# stp priority 255
ProCurve Access Point 530(config)#
```

Using the CLI to View WDS Parameters. This example uses the show interface ethernet command and the show wds x command to check the status of the STP state and configured parameters.

```
ProCurve Access Point 530#show interface ethernet
Ethernet interface:
------------------------------------------------------------
Description            Ethernet
MAC address            00:14:C2:A5:08:CB
Speed-duplex           auto
Administrative status  Enabled
Management VLAN ID     1    (U)
Untagged-VLAN ID       1
Spanning Tree (STP)    Enabled
STP Port State         forwarding
STP Hello Interval     10.0
STP Forward Delay      10
STP Bridge Priority    255

Bytes Rx             22911       Bytes Tx               46107
Packets Rx           240         Packets Tx             299
Compressed Rx        0           Compressed Tx          0
Mcast packets Rx     0           Carrier errors Tx      0
Dropped Rx packets   0           Dropped Tx packets     0
FIFO overflows Rx    0           FIFO overflows Tx      0
Frame errors Rx      0           Packet collisions Tx   0
Total Rx errors      0           Total Tx errors        56
ProCurve Access Point 530#
```

Note: Spanning Tree Protocol (STP) has detected a loop and the WDS 1 interface is being blocked by STP, as can be seen from the output below.

```
ProCurve Access Point 530(wds1)#show wds 1
WDS #1
Description Wireless Distribution System - Link 1
Status      Enabled            Use Radio   1
Local MAC   00:14:C2:A5:22:61  Remote MAC  00:14:C2:A4:14:A0
STP State   blocking           WDS SSID    WDS SSID 1

Security Type  no-security (from WLAN 1)WEP Key Type  hex
WEP Key        not set                  WEP Key Size  128bit
WPA Key        not set

Bytes Rx            7140        Bytes Tx               76
Packets Rx          66          Packets Tx             1
Compressed Rx       0           Compressed Tx          0
Mcast packets Rx    0           Carrier errors Tx      0
Dropped Rx packets  0           Dropped Tx packets     0
FIFO overflows Rx   0           FIFO overflows Tx      0
Frame errors Rx     0           Packet collisions Tx   0
Total Rx errors     0           Total Tx errors
ProCurve Access Point 530(wds1)#
```

AP Detection Commands

The access point can be configured to periodically scan all radio channels and find other access points within range. Alternatively, the access point can scan continuously in a dedicated mode with no stations supported. A database of nearby access points is maintained where detected access points can be identified.

Each radio can be independently configured to be a dedicated or background scanner. Dedicated scanning provides the best AP detection results. Background scanning allows the radio to service stations in addition to detecting neighboring access points.

Background scanning is designed to try to avoid wireless traffic interruptions, thus during heavy-traffic conditions, background scanning may delay a scan until it appears that a scan may be performed without losing wireless traffic.

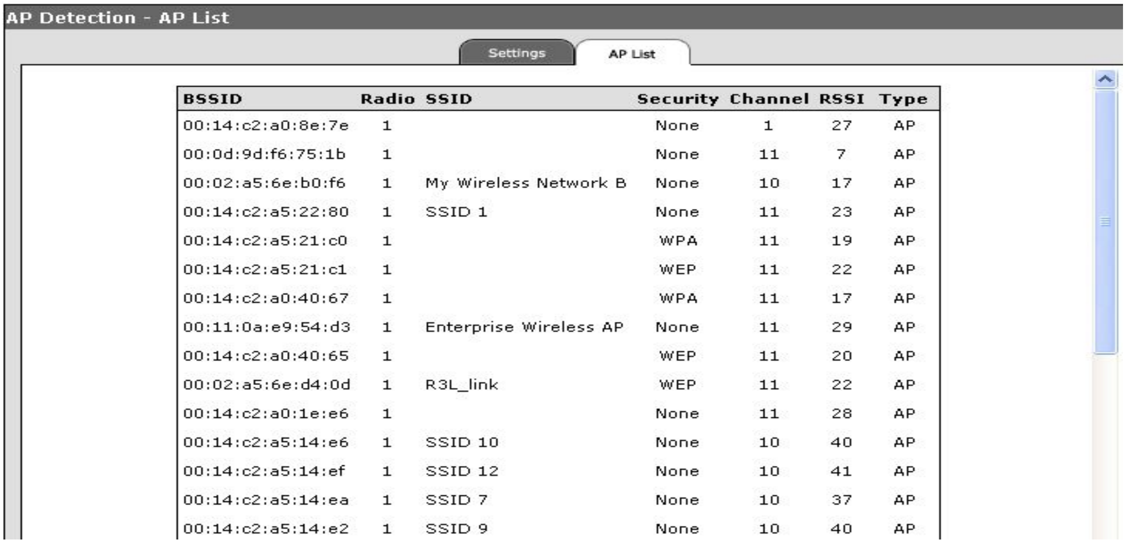
Web: Configuring AP Detection Parameters

The AP Detection window provides configuration for access point detection. The Settings tab enables you to modify these parameters:

- **AP Detection Radio 1/Radio 2:** Enables/Disables ability per radio for the access point to scan radio channels to discover other access points. (Default is Disable)
- **Scan Interval:** Sets the minimum amount of time that the access point will wait between background scans on each radio. This setting applies to background scanning only. Range: 10-3600 seconds (Default is 10)
- **Scan Duration:** Sets the amount of time spent scanning other channels when background scanning is being performed. This setting applies to background scanning only. Range: 5-30 milliseconds (Default is 30)
- **Entry Expiration Time:** Sets expiration value for the listed detected AP entries. Range: 1-604800 seconds (Default is 3600)
- **Max Entries**: Sets the maximum list amount of the detected APs. Range: 1-255 (Default is 255)
- **[Update]:** Updates the AP detection parameters.

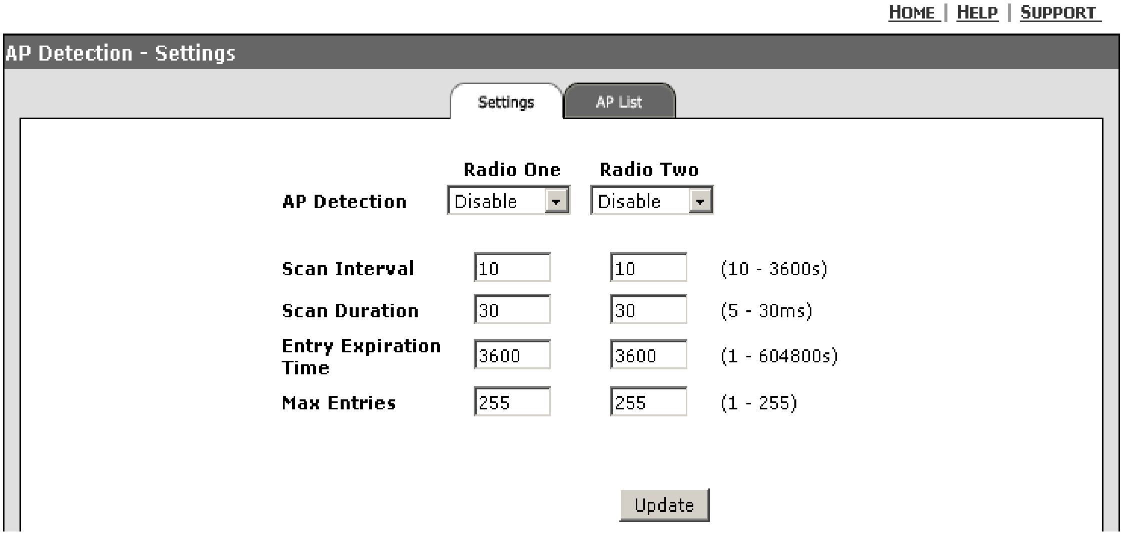
The AP List tab enables you to display and refresh the list of neighboring access points that have been detected during previous scans. For each detected access point, the following parameters are displayed:

- **BSSID:** Displays the MAC Address identifier for the access point.
- **Radio SSID:** Displays the alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.
- **Security:** Indicates whether WPA security is set for this access point.
- **Channel:** Displays the current broadcasting channel.
- **RSSI:** Displays the received signal strength of the detected access point.
- **Type:** Displays the detected type of wireless network device.
    - **AP:** Access point device (802.11 infrastructure)
    - **Ad-hoc:** Client device configured for ad-hoc (peer-peer) network connectivity.
- **[Refresh]:** Refreshes the AP scan results.



BSSID	Radio	SSID	Security	Channel	RSSI	Type
00:14:c2:a0:8e:7e	1		None	1	27	AP
00:0d:9d:f6:75:1b	1		None	11	7	AP
00:02:a5:6e:b0:f6	1	My Wireless Network B	None	10	17	AP
00:14:c2:a5:22:80	1	SSID 1	None	11	23	AP
00:14:c2:a5:21:c0	1		WPA	11	19	AP
00:14:c2:a5:21:c1	1		WEP	11	22	AP
00:14:c2:a0:40:67	1		WPA	11	17	AP
00:11:0a:e9:54:d3	1	Enterprise Wireless AP	None	11	29	AP
00:14:c2:a0:40:65	1		WEP	11	20	AP
00:02:a5:6e:d4:0d	1	R3L_link	WEP	11	22	AP
00:14:c2:a0:1e:e6	1		None	11	28	AP
00:14:c2:a5:14:e6	1	SSID 10	None	10	40	AP
00:14:c2:a5:14:ef	1	SSID 12	None	10	41	AP
00:14:c2:a5:14:ea	1	SSID 7	None	10	37	AP
00:14:c2:a5:14:e2	1	SSID 9	None	10	40	AP

Figure 8-10. AP Detection - AP List Tab



AP Detection - Settings

	Radio One	Radio Two	
AP Detection	Disable	Disable	
Scan Interval	10	10	(10 - 3600s)
Scan Duration	30	30	(5 - 30ms)
Entry Expiration Time	3600	3600	(1 - 604800s)
Max Entries	255	255	(1 - 255)

Figure 8-11. AP Detection - Settings Tab

To Enable AP Detection Parameters :

1. Select Special Features > AP Detection> Settings tab.
2. To enable scanning, choose **Enabled** for the AP Detection option.
3. To specify the beacon transmission interval, enter the **interval value** in the Scan Interval text field.
4. To specify the duration of scanning, enter the **duration value** in the Scan Duration text field.
5. Click **[Update]** to save the settings.

CLI: Configuring AP Detection

CLI Commands Used in This Section.

Command	CLI Reference Page
[no] **ap-detection [dedicated]**	9-111
ap-detection duration *<value>*	9-112
ap-detection interval *<value>*	9-113
ap-detection expire-time *<value>*	9-112
ap-detection max-entries *<value>*	9-113
show detected-ap	9-114

Using the CLI to Enable Dedicated Neighboring AP Detection. This example enables the dedicated detection of nearby access points and prevents this radio from being used by any other function.

```
ProCurve Access Point 530(radio1)#ap-detection dedicated
ProCurve Access Point 530(radio1)#
```

Using the CLI to Set Passive Neighboring AP Detection Parameters. This example enables the periodic detection of nearby access points, sets the duration of the passive scan in milliseconds, and establishes the interval between scans.

```
ProCurve Access Point 530(radio1)#ap-detection
ProCurve Access Point 530(radio1)#ap-detection duration 10
ProCurve Access Point 530(radio1)#ap-detection interval 15
```

Using the CLI to Set AP List Parameters. This example sets the time a detected AP remains on the AP list and sets the maximum number of AP entries displayed on the list.

```
ProCurve Access Point 530(radio1)#ap-detection expire-time
55
ProCurve Access Point 530(radio1)#ap-detection max-entries
100
```

Using the CLI to View the AP Scan Results. This example displays the current AP detection results.

```
ProCurve Access Point 530(radio1)#show detected-ap

Neighboring APs:
BSSID              SSID            Sec  Chan  Type
------------------------------------------------------------
00:14:02:A0:4F:BC   SSID1          none   3    AP
00:14:03:A2:4F:DE   SSID2          wpa    3    AP

ProCurve Access Point 530#
```

Identity Driven Management

Identity-Driven Management (IDM) is integrated with 802.1X authentication methods, and to successfully utilize IDM, the access point SSID slated to employ IDM must have one of the 802.1X security methods configured. IDM automatically configures the edge of the network, based on the identity of the user. IDM may restrict the network access by assigning VLAN, ACL, Rate Limiting and QoS.

Configuring an IDM solution on the Access Point 530 requires the implementation of the ProCurve Identity Driven Manager product and a supported RADIUS server. For access to the ProCurve Manager Manual and the IDM User's Guide, please refer to http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm.

The Access Point 530 supports the following IDM features:

- VLAN
- Access Control List (ACL)
- Rate Limiting

IDM on the Access Point 530 can be accomplished using either 802.1X authentication or MAC authentication. 802.1X authentication is more secure, while MAC Authentication can be used with stations that don't have 802.1X supplicant. Although it is possible to use MAC Authentication along with 802.1X, there are known user and ACL assignment overrides that occur. Essentially, both MAC and 802.1X can employ IDM individually, however, if used simultaneously, 802.1X takes precedence.

IDM VLAN

A VLAN ID can be assigned to each station after successful authentication. User VLAN IDs must be configured on the IDM server for each user authorized to access the network. The access point assigns any unassigned user the default VLAN ID of the associated WLAN (BSS/SSID) interface. For more information on VLAN support, See “Configuring VLAN Support” on page 5-48.

For IDM VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

IDM ACL

RADIUS-assigned ACLs provide Layer-3 filtering of inbound IP traffic from authenticated stations. A unique username/password pair or station MAC address identifies these ACLs and applies only to traffic from stations authenticated with the same unique credentials. Implementing this feature requires:

- RADIUS authentication using 802.1X or station MAC authentication.
- Configuring RADIUS-assigned ACLs, each ACL assigned the username/ password pair or MAC address of the stations to support.

Using RADIUS ACLs benefits the access point as it improves system performance and provides a less complex network edge filtering method than VLAN ACLs network core filtering method.

Configuring an ACL in a RADIUS Server

This section provides general guidelines for configuring a RADIUS server to specify RADIUS-based ACLs, please refer to the RADIUS server documentation for specifics. A RADIUS-based ACL configuration has the following:

- Vendor and ACL identifiers:
    - ProCurve (HP) Vendor-Specific ID: 11
    - Vendor-Specific Attribute for ACLs: 61 (string = HP-IP-FILTER-RAW)
    - Setting: HP-IP-FILTER-RAW = < "permit”or "deny" (Access Control Entry (ACE)>

      NOTE: permit (forwards inbound packets), deny (drops packets)
- ACL configuration, including:
    - one or more explicit "permit" and/or "deny" ACEs created by the system operator
    - implicit deny any any ACE automatically active after the last operator created ACE.

IDM Rate Limiting

User traffic on the inbound direction is restricted using this feature of IDM. The traffic limit is mentioned in Kbps. The inbound traffic limit is sent in the RADIUS Accept message using Vendor Specific attribute as explained below:

- ProCurve (HP) Vendor-Specific ID: 11
- VSA: 46 (integer = HP)
- Setting: HP-RATE-LIMIT = < *bandwidth-in-Kbps* >

— This page is intentionally unused. —

9

Command Line Reference

Contents

Overview

This chapter describes the commands provided by the CLI.

The CLI commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Initial commands for performing basic access point tasks.	9-9
System Management	Basic commands for performing basic status, management, and performance tasks.	9-16
System Logging Commands	Commands related to event logs on the system.	9-30
System Clock Commands	Commands related to SNTP.	9-34
SNMP	Commands for establishing SNMP community settings.	9-36
Flash/File Commands	Configures relating to resetting configuration and factory files.	9-43
RADIUS Accounting/ Authentication Commands	Configures RADIUS accounting and authentication parameters.	9-53
Radius Users	Configures RADIUS users.	9-57
MAC Address Authentication	Configures MAC parameters.	9-60
Filtering Commands	Configures filtering settings.	9-63
Ethernet Interface Commands	Configures Ethernet interface settings.	9-66
Wireless Interface	Configures wireless parameters.	9-76
Wireless Security	Configures wireless security settings.	9-100
Neighbor AP-Detection	Configures access point detection settings.	9-111
Vlan Commands	Configures management VLAN parameters.	9-116
QoS	Configures Quality of Service parameters.	9-119
WDS	Configures WDS settings.	9-128
STP	Configures STP parameters.	9-135

The access mode shown in the following tables is indicated by these abbreviations:

- **GC** (Global Configuration),
- **MC** (Manager Executive Configuration),
- **IC-E** (Ethernet Interface Configuration),
- **IC-WDS**(WDS Interface Configuration),
- **IC-R** (Radio Wireless Interface Configuration), and
- **IC-R-WLAN**(WLAN Wireless Interface Configuration)

General Commands

These commands are used to configure the basic commands on the access point.

Command	Function	Mode	Page
configure	Set the current context level to the Global Configuration level.	MC	9-9
copy	See "Flash/File Commands" on page 9-43		9-44
end	Sets the current context level to the Manager Exec level.	MC	9-10
erase	See "Flash/File Commands" on page 9-43		9-47
exit	Sets the current command level to the previous command level.	MC	9-10
log	See "System Logging Commands" on page 9-30		9-30
logout	Terminates the CLI session.	MC	9-11
ping	Sends ICMP echo request packets to another node on the network	MC	9-12
reload	Perform a warm reboot.	MC	9-13
Show	Show operation information and parameters for this device.	MC	9-13
terminal	Sets dimensions of the terminal window.	MC	9-15
write	See "Flash/File Commands" on page 9-43		9-48

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the access point. You must also enter Global Configuration mode prior to enabling the context modes for Interface Configuration. See "Using the CLI" on page 3-7.

Syntax

configure [terminal]

- **terminal** - Allows access to the Global Configuration mode. This is optional and may be omitted by the user.

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#
```

end

This command sets the current context level to the Manager Exec level.

Syntax

end

Default Setting

N/A

Command Mode

Manager Exec

Example

This example shows how to return to the Manager Exec level from the Ethernet Interface Configuration mode:

```
ProCurve Access Point 530(ethernet)#end
ProCurve Access Point 530#
```

exit

This command sets the current command level to the previous command level. At the Manager Exec level, this command acts the same as logout.

Syntax

exit

Default Setting

N/A

Command Mode

Manager Exec

Example

This example shows how to return to the previous command levels starting from the Interface Configuration mode and finally logging out of the CLI session:

```
ProCurve Access Point 530(ethernet)#exit
ProCurve Access Point 530(config)#exit
ProCurve Access Point 530#exit

Connection to host lost.
```

logout

This command terminates the CLI session.

Syntax

logout

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#logout

Connection to host is lost.
```

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping <hostname | ip>

- **hostname** - Alias of the host.
- **ip** - IP address of the host.

Default Setting

N/A

Command Mode

Manager Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  – *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  – *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  – *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  – *Network or host unreachable* - The gateway found no corresponding entry in the route table.

Example

```
ProCurve Access Point 530#ping 10.1.0.9
10.1.0.9 is alive
ProCurve Access Point 530#
```

reload

This command performs a warm reboot on the access point. This command causes all Telnet and SSH connections to loose connectivity.

Syntax

reload

Default Setting

N/A

Command Mode

Manager Exec

Example

This example shows how to perform a warm reboot of the system:

```
ProCurve Access Point 530#reload
Device will be rebooted, do you want to continue [y/n]?y
Do you want to save the current configuration [y/n]?n
Connection to host lost.
```

show

This command displays the status of the push button capabilities.

Syntax

show [basic-rate | buttons | config | console | copy | custom-default | debug | detected-ap | dot11 | filters | interfaces | ip | lldp | logging | mac-auth-local | qos | radios | radius-local | running-config | snmp-server | sntp | ssh | ssid | stations | supported-rate | system-information | time | version | wlans | wds]

- **basic-rate** - Shows advertised transmission rates for this device. See "show basic-rate" on page 9-98.
- **buttons** - Shows current status of the buttons on this device. See "show buttons" on page 9-25.
- **config** - Shows the startup configuration file of this device. See "show config" on page 9-49.
- **console** - Shows serial console configuration/status on this device. See "show console" on page 9-26.
- **copy** - Shows status of the last copy operation (ftp/scp/tftp). See "show copy" on page 9-49.

- **custom-default** -Shows custom default configuration file of device. See "show custom-default" on page 9-51.
- **debug** - Shows debug-related information on this device. See "show debug" on page 9-32.
- **detected-ap** - Shows detected neighboring wireless network details. See "show detected-ap" on page 9-114.
- **filters** - Shows settings for traffic/security filters on this device. See "show filters" on page 9-64.
- **interfaces** - Shows information about the interfaces on this device. See "show interface" on page 9-73.
- **ip -** Shows the current IP configuration on this device. See "show ip" on page 9-72.
- **lldp** - Shows Link Layer Discovery Protocol (LLDP) details. See "show lldp" on page 9-42.
- **logging** - Shows all the entries in the event log. See "show logging" on page 9-32.
- **mac-auth-local** - Show all the entries in the local MAC address authentication control lists. See "show mac-auth-local" on page 9-62.
- **qos -** Shows QoS details on this device and wireless system. See "show qos" on page 9-125.
- **radios -** Shows information about the radio(s) on this device. See "show radio" on page 9-92.
- **radius-local** - Shows status of the internal RADIUS server on device. See "show radius-local" on page 9-58.
- **running-config** - Shows the running configuration file of this device. See "show running-config" on page 9-52.
- **snmp-server** - Shows SNMP community and trap information. See "show snmp-server" on page 9-40.
- **sntp -** Shows configured time protocol and servers on this device. See "show sntp" on page 9-35.
- **ssh** - Shows SSH configuration and the status of active connections. See "show ssh" on page 9-26.
- **ssid -** Shows SSID information on this device or radio context. See "show ssid" on page 9-93.
- **stations** - Show associated wireless station details. See "show stations" on page 9-98.
- **supported-rate** - Show information about supported transmission rates on this device. See "show supported-rate" on page 9-99.

- **system-information** - Show global configured and operational system parameters on this device. See "show system-information" on page 9-27.
- **tech**- Shows status of a predefined command sequence used by technical support. See "show tech" on page 9-50.
- **time** - Show current date and time. See "show time" on page 9-35.
- **version** - Show software version. See "show version" on page 9-29.
- **wlans** - Show WLANs information on this device or radio context. See "show wlan" on page 9-95.
- **wds** - Show information about the WDS's on this device. See "show wds" on page 9-131.

terminal

This command sets terminal line parameters.

Syntax

terminal length | width

- **length** - Set number of lines on a screen.
  - <2-1000> - Number of lines on a screen.
- **width** - Set width of display terminal.
  - <61-1920> - Number of characters on a screen line.

Default Setting

N/A

Command Mode

Manager

Example

```
ProCurve Access Point 530#terminal length 1000
ProCurve Access Point 530#
ProCurve Access Point 530#terminal width 1900
ProCurve Access Point 530#
```

System Management Commands

These commands are used to configure the user name, password, system details, and a variety of other system information.

Command	Function	Mode	Page
country *<country code>*	Set the country code for the access point.	GC	9-17
hostname *<hostname>*	Specifies the hostname for the access point.	GC	9-19
[no] domain *<domain>*	Specifies the system domain name suffix for the access point.	GC	9-20
password manager *<password>*	Specifies the administrator password for management access	MC	9-20
[no] buttons	Enables the ability to clear the password(s) and/or configurations.	MC	9-21
[no] cli-configuration	Enables all CLI confirmation dialog prompts.	MC	9-24
[no] console	Enables the access point to be managed through a serial port.	MC	9-22
[no] telnet	Enables the access point to managed through a Telnet connection.	MC	9-23
[no] ssh	Enables remote Secure Shell access to the device.	MC	9-24
[no] web-management <plaintext | ssl>	Enables remote Web access to the device.	MC	9-24
show buttons	Displays button status.	MC	9-25
show console	Displays console status.	MC	9-26
show ssh	Displays ssh status.	MC	9-26
show system	Displays system information	MC	9-27
show version	Displays version information for the system	MC	9-29

country

This command configures the access point's Country Code, which identifies the country of operation and sets the correct authorized radio channels.

Syntax

country <*country_code*>

- ***country_code*** - A two character code that identifies the country of operation. See Table 9-1 on page 9-17 for a full list of the codes.

Table 9-1. Access Point Country Codes

Country	Code	Country	Code	Country	Code	Country	Code
Afghanistan	AF	Egypt	EG	Lebanon	LB	Russian Federation	RU
Albania	AL	El Salvador	SV	Lesotho	LS	San Marino	SM
Algeria	DZ	Estonia	EE	Libyan Arab Jamahiriya	LY	Saudi Arabia	SA
Andorra	AD	Finland	FI	Liechtenstein	LI	Serbia and Montenegro	CS
Angola	AO	France	FR	Lithuania	LT	Seychelles	SC
Argentina	AR	French Guiana	GF	Luxembourg	LU	Singapore	SG
Armenia	AM	Georgia	GE	Macau	MO	Slovakia	SK
Australia	AU	Germany	DE	Macedonia, The Former Yugoslav Republic Of	MK	Slovenia	SI
Austria	AT	Gibraltar	GI	Malaysia	MY	South Africa	ZA
Azerbaijan	AZ	Greece	GR	Malta	MT	Spain	ES
Bahamas	BS	Guam	GU	Mauritius	MU	Sri Lanka	LK
Bahrain	BH	Guatemala	GT	Mexico	MX	Swaziland	SZ
Bangladesh	BD	Guyana	GY	Moldova, Republic Of	MD	Sweden	SE
Belarus	BY	Haiti	HI	Monaco	MC	Switzerland	CH
Belgium	BE	Holy See (Vatican City State)	VA	Mongolia	MN	Syrian Arab Republic	SY
Belize	BZ	Honduras	HN	Morocco	MA	Taiwan, Province of China	TW

Country	Code	Country	Code	Country	Code	Country	Code
Bermuda	BM	Hong Kong	HK	Mozambique	MZ	Tajikstan	TJ
Bolivia	BO	Hungary	HU	Myanmar	MM	Thailand	TH
Bosnia and Herzegovina	BA	Iceland	IS	Nambia	NA	Trinidad and Tobago	TT
Botswana	BW	India	IN	Netherlands	NL	Tunisia	TN
Brazil	BR	Indonesia	ID	New Zealand	NZ	Turkey	TR
Brunei Darussalam	BN	Iran, Islamic Repubic Of	IR	Nicaragua	NI	Turkmenistan	TM
Bulgaria	BG	Iraq	IQ	Nigeria	NG	Ukraine	UA
Cambodia	KH	Ireland	IE	Norway	NO	United Arab Emirats	AE
Canada	CA	Israel	IL	Oman	OM	United Kingdom	GB
Chile	CL	Italy	IT	Pakistan	PK	United States	US
China	CN	Jamaica	JM	Palestinian Territory, Occupied	PS	Uruguay	UY
Colombia	CO	Japan	JP	Panama	PA	Uzbekistan	UZ
Costa Rica	CR	Jordan	JO	Paraguay	PY	Venezuela	VE
Croatia	HR	Kazakhstan	KZ	Peru	PE	Vietnam	VN
Cuba	CU	Korea, Democratic People Republic Of	KP	Philippines	PH	Yemen	YE
Cyprus	CY	Korea, Republic Of	KR	Poland	PL	Zambia	ZM
Czech Republic	CZ	Kuwait	KW	Portugal	PT	Zimbabwe	ZW
Denmark	DK	Kyrgyzstan	KG	Puerto Rico	PR		
Dominican Republic	DO	Lao People's Democratic Republic	LA	Qatar	QA		
Ecuador	EC	Latvia	LV	Romania	RO		

Default Setting

For NA units, preset to US

Command Mode

Global Configuration

Command Usage

- The access point's Country Code must be set before the radio can be enabled.
- After a Country Code has been set and the system rebooted, the **country** command is no longer available from the CLI. If you need to change the Country Code, the access point configuration must be reset to its default values by using the **erase-startup-config** command, or by pressing the reset button and clear buttons simultaneously, see Appendix A, "Resets the configuration back to factory defaults." on page A-16.

Example

```
ProCurve Access Point 530#country gb
ProCurve Access Point 530#
```

hostname

This command sets the system hostname.

Syntax

hostname <*hostname*>

- ***hostname*** - A text string to identify the system.
  (Maximum length: 50 characters)

Default Setting

ProCurve-AP-530

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#hostname Gary
```

domain

This command sets the system domain name suffix for the domain name. The suffix is not obtained through DHCP. The no version of this command clears the statically configured domain suffix.

Syntax

domain *<domain>*

no domain *<domain>*

- ***domain*** - A text string to set the domain name.
  (Maximum length: 50 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#domain example.com
```

password manager

This command sets the password for entering the Manager Exec level.

Syntax

password manager *<password>*

- ***password*** - A text string to establish security for entry into the Manager Exec level.
  Note: The password is case sensitive and must be at least 1 character and at most 32 characters long. However, only the first 8 characters of the password are used; character number 9 and above are ignored at log in.

Default Setting

admin

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#password manager admin
```

buttons

This command enables the ability to clear the password(s) and/or configuration(s) via the buttons on the device. The no command disables this ability.

Syntax

buttons <custom-reset | factory-reset | password-reset | system-reset>

- **custom-reset** - Enables the ability to reset this device to the custom-default configuration via the buttons. The no version of the command disables this devices ability to reset this device to the custom-default configuration via the buttons.
- **factory-reset** - Enables the ability to reset this device to the factory-default configuration via the buttons. The no version of the command disables this devices ability to reset this device to the factory-default configuration via the buttons. The no buttons factory-reset command will not work if the serial console is already disabled (e.g." no console" has been executed).
- **password-reset** - Enables the ability to reset the password(s) on this device via the buttons. The no version of the command disables this devices ability to reset the password(s) on this device via the buttons.
- **system-reset** - Enables the ability to reset the system via the buttons. The no version of the command disables this devices ability to reset the system via the buttons.

Default Setting

Enabled

Command Mode

Global Configuration

Example

This example shows how to disable all the push button capabilities.

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#no buttons custom-reset
ProCurve Access Point 530(config)#no buttons factory-reset
ProCurve Access Point 530(config)#no buttons password-reset
ProCurve Access Point 530(config)#no buttons system-reset
ProCurve Access Point 530(config)#
```

cli-confirmation

This command enables all CLI confirmation dialog prompts on the device. The no command disables this ability.

Syntax

cli-confirmation

no cli-confirmation

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#cli-confirmation
ProCurve Access Point 530(config)#
```

console

This command enables the serial console on the access point. The no version disables the serial console on the access point. The no console command will not work if the factory reset button is already disabled (e.g." no buttons factory-reset" has been executed).

Syntax

console

no console

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#console
ProCurve Access Point 530(config)#
```

telnet

This command enables remote Telnet access. The no version disables remote Telnet access to this device.

Syntax

telnet

no telnet

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#telnet
ProCurve Access Point 530(config)#
```

ssh

This command enables the remote ssh access to this device. The no version disables the remote ssh access to this device.

Syntax

ssh

no ssh

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#ssh
ProCurve Access Point 530(config)#
```

web-management

This command enables remote Web access to this device. The no version disables the remote Web access to this device.

Syntax

web-management <plaintext | ssl >

no web-management

- **plaintext** - Enables remote HTTP (insecure) access to the device. The no version of the command disables remote HTTP access
- **ssl** - Enable remote HTTPS (secure) access to the device. The no version of the command disables remote HTTPS access.

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#web-management ssl
ProCurve Access Point 530(config)#
```

show buttons

This command displays the status of the push button capabilities.

Syntax

show buttons

Default Setting

N/A

Command Mode

Manager Exec

General Configuration Context

Example

This example displays the status of the push buttons on the access point.

```
ProCurve Access Point 530# show buttons
------------------------------------------------------------
Custom Reset             Enabled
Factory Reset            Enabled
Password Reset           Enabled
System Reset             Enabled

ProCurve Access Point 530#
```

show console

This command displays the status of the console.

Syntax

show console

Default Setting

N/A

Command Mode

Manager Exec

General Configuration Context

Example

```
ProCurve Access Point 530(config)# show console
------------------------------------------------------------
CLI Access:
 Serial Interface           Enabled
 Telnet Interface           Enabled
 SSH Interface              Enabled

 CLI Confirmation Dialogs   Enabled
Web Access:
 HTTP Interface             Enabled
 SSL Interface              Enabled
ProCurve Access Point 530(config)#
```

show ssh

This command displays the current SSH configuration and the status of the active SSH connections on this device.

Syntax

show ssh

Default Setting

N/A

Command Mode

Manager Exec

General Configuration Context

Example

```
ProCurve Access Point 530(config)# show ssh
------------------------------------------------------------
SSH Status   Enabled

ProCurve Access Point 530(config)#
```

show system-information

This command shows information about the device and the hostname/DNS information. This command is the same as the **show system** command.

Syntax

show system-information

Default Setting

N/A

Command Mode

Manager Exec

Global Configuration

Example

```
ProCurve Access Point 530# show system-information
------------------------------------------------------------
Serial Number         TW547VV07X
System Name           ProCurve-AP-530
System Up Time        2 days 23 hours 35 mins 18 secs
System Location       not set
System Country Code   us
Software Version      WA.01.00
Ethernet MAC Address  00:14:C2:A5:08:CB
IP Address            192.168.15.100
Subnet Mask           255.255.255.0
Default Gateway       192.168.15.1
DHCP Client           Enabled
Management VLAN ID    1
Untagged-VLAN ID      1
Radio 1 MAC Address   00:14:C2:A5:22:E0
Radio 1 Status        Disabled (802.11g)
Radio 2 MAC Address   00:14:C2:A5:22:F0
Radio 2 Status        Disabled (802.11a)
HTTP Interface        Enabled
SSL Interface         Enabled
SSH Interface         Enabled
Telnet Interface      Enabled
Serial Interface      Enabled

ProCurve Access Point 530(config)#
```

show version

This command displays the version of the software running on the device.

Syntax

show version

Default Setting

N/A

Command Mode

Manager Exec

Global Configuration

Example

```
ProCurve Access Point 530# show version
Image Software Version  WA.01.00
Boot Software Version   WAB.01.00

ProCurve Access Point 530#
```

System Logging Commands

These commands are used to configure system logging on the access point.

Command	Function	Mode	Page
log	Displays all log entries in access point memory.	MC	9-30
[no] logging <syslog_host> [syslog_port]	Adds a syslog server host IP address and assign a port number that will receive logging messages.	GC	9-31
show debug	Displays the debugging results.	MC	9-32
show logging	Displays the state of logging.	MC	9-32

log

This command displays all the entries in the event log on the device. This command is functionally the same as the **show logging** command.

Syntax

log

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#log
 Keys:   M=eMergency   C=Critical   W=Warning
I=Information
         A=Alert       E=Error      N=Notice    D=Debug
-----  Event Log Listing: Most Recent Events First  ----
I 01/03/00 03:57:15 login[29765]: root login  on `ttyp0'
I 01/03/00 02:28:56 login[24466]: root login  on `ttyp0'
I 01/02/00 04:00:49 login[7445]: root login  on `ttyp0'
I 01/02/00 02:23:30 login[1248]: root login  on `ttyp0'
I 01/01/00 07:10:33 login[28706]: root login  on `ttyp0'
I 01/01/00 05:59:52 login[24293]: root login  on `ttyp0'
I 01/01/00 03:00:16 login[13449]: root login  on `ttyp0'
I 01/01/00 00:00:14 dropbear[602]: Not forking
ProCurve Access Point 530#
```

logging

This command configures log-related settings for the device. The no version of the command disables relaying of log entries to the specified syslog server, if any.

Syntax

logging <syslog_host> [syslog_port]

no logging

- **syslog_host** - The IP address of the receiving syslog server. The no version of the command disables relaying of log entries to the specified syslog server.
- **syslog_port** - The port number of the receiving syslog server.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to memory.

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#logging 10.1.0.3 514
ProCurve Access Point 530(config)#
```

Related Commands

show logging (page 9-32)

show debug

This command displays debug related details on this device.

Syntax

show debug

Default Setting

N/A

Command Mode

Manager Exec

Global Configuration

Example

```
ProCurve Access Point 530#show debug

Debug Logging:
Syslog Relay    10.1.0.3 (port 514)

ProCurve Access Point 530#
```

show logging

This command displays all the entries in the event log on the device. This command is functionally the same as the **log** command.

Syntax

show logging

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#log
 Keys:   M=eMergency   C=Critical   W=Warning
I=Information
         A=Alert       E=Error      N=Notice    D=Debug
-----  Event Log Listing: Most Recent Events First  ----
I 01/03/00 03:57:15 login[29765]: root login  on `ttyp0'
I 01/03/00 02:28:56 login[24466]: root login  on `ttyp0'
I 01/02/00 04:00:49 login[7445]: root login  on `ttyp0'
I 01/02/00 02:23:30 login[1248]: root login  on `ttyp0'
I 01/01/00 07:10:33 login[28706]: root login  on `ttyp0'
I 01/01/00 05:59:52 login[24293]: root login  on `ttyp0'
I 01/01/00 03:00:16 login[13449]: root login  on `ttyp0'
I 01/01/00 00:00:14 dropbear[602]: Not forking
ProCurve Access Point 530#
```

Related Commands

log (page 9-30)

System Clock Commands

These commands are used to configure SNTP on the access point.

Command	Function	Mode	Page
sntp *<server>*	Specifies one time servers	GC	9-34
show sntp	Shows current SNTP configuration settings.	MC	9-35
show time	Shows current date and time.	MC	9-35

sntp

This command enables the NTP client on the device. The no version of the command does not require parameters and resets the address of the NTP server, if any.

Syntax

sntp *<server>*

- ***server* -** The IP address or hostname of a time server (NTP or SNTP).

Default Setting

None

Command Mode

Global Configuration

Command Usage

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the access point only records the time starting from the factory default set at the last bootup (i.e., 00:14:00, January 1, 1970). When SNTP client mode is enabled, the **sntp server** command specifies the time servers from which the access point polls for time updates. The access point will poll the time servers in the order specified until a response is received.

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#sntp 10.1.0.19
```

show sntp

This command displays the current time and configuration settings for the SNTP client.

Syntax

show sntp

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show sntp
Status               : up
Server               : 10.1.0.19
ProCurve Access Point 530#
```

show time

This command displays the current date and time.

Syntax

show time

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show time
Sat Jan  3 16:35:14 1970
ProCurve Access Point 530#
```

Network Management Application Commands

These commands are used to configure Simple Network Management Protocol (SNMP) and Link Layer Discovery Protocol which defines standards for facilities network management..

Command	Function	Mode	Page
SNMP			
[no] snmp-server community *<comm>* restricted | unrestricted	Sets up the private community access string to permit access to SNMP commands	GC	9-36
snmp-server contact*<contact>*	Sets the system contact string.	GC	9-37
[no] snmp-server host *<host><comm>*	Sets the system location string.	GC	9-38
snmp-server port *<port>*	Sets the SNMP server port number.	GC	9-39
snmp-server location *<location>*	Sets the system location string.	GC	9-39
show snmp-server	Displays the status of SNMP communications.	MC	9-40
LLDP			
[no] lldp	Enables Link Layer Discovery Protocol service on the device.	GC	9-41
show lldp	Displays the Link Layer Discovery Protocol service status on the device.	GC	9-41

snmp-server community restricted | unrestricted

This command defines the community access string for the read-only or read-write access Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server < community *<comm>* <restricted | unrestricted >
no snmp-server community *<comm>* <restricted | unrestricted >

- ***comm*** - Community string that denotes it as private.
- **restricted** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. The no version of the command clears the read-only community value.
- **unrestricted** - Specifies read-write access. Authorized management stations are only able to retrieve MIB objects. The no version of the command clears the read-write community value.

Default Setting

Restricted community with a public access default.

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#no snmp-server community
<public> restricted
ProCurve Access Point 530(config)#no snmp-server community
<system> unrestricted
ProCurve Access Point 530(config)#
```

snmp-server contact

This command sets the system contact string.

Syntax

snmp-server contact <*contact*>

- ***contact*** - String that describes the system contact.Maximum length: 255 characters.

Default Setting

Contact

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530(config)#snmp-server contact Paul
ProCurve Access Point 530(config)#
```

snmp-server host

This command specifies the recipient of an SNMP trap notification. Use the **no** form to remove the specified trap host.

Syntax

snmp-server host <*host*> <*comm*>
no snmp-server host

- ***host*** - IP address of the host.
- ***comm***- Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

Default Setting

Host Address: None
Community String: public

Command Mode

Global Configuration

Command Usage

The **snmp-server host** command is used in conjunction with the **snmp-server enable server** command to enable SNMP notifications.

Example

```
ProCurve Access Point 530(config)#snmp-server host 10.1.0.15
public
ProCurve Access Point 530(config)
```

snmp- server port

This command specifies the port number that the SNMP server will use on this device.

Syntax

snmp-server port*<port>*

- ***port -*** The number specifying the port to which the SNMP server will listen. This must be an unused port on the AP.

Default Setting

161

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#snmp-server port 161
ProCurve Access Point 530(config)#
```

snmp- server location

This command specifies a text string that identifies the location of this SNMP device.

Syntax

snmp-server location *<location>*

- ***location***-The text string describing the location of this device.

  (Maximum length: 1-255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#snmp-server location 2F
R19
ProCurve Access Point 530(config)#
```

Related Commands

show snmp-server (page 9-40)

show snmp-server

This command displays information about the configuration and status of the SNMP server on this device.

Syntax

show snmp-server

Default Setting

None

Command Mode

Manger Exec

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#show snmp-server
SNMP Server Settings
---------------------------------------------------------------------------
SNMP Server Settings
---------------------------------------------------------------------------
SNMP Status      Enabled
SNMP Port        161
Community (ro)   public
Community (rw)   private
Location         not set
Contact          not set

Trap Destinations
Host      Community
-----------------------
1         192.168.1.15
2         192.168.1.19

hpWlanAdHocNetworkDetected        Enabled   hpWlanApDetectionUpdate    Enabled
hpWlanRadioAntennaUpdate          Enabled   hpWlanButtonUpdate         Enabled
hpWlanClientAssociation           Enabled   hpWlanApInterfaceUpdate    Enabled
hpWlanClientDeAuthentication      Enabled   hpWlanClientAuthentication Enabled
hpWlanClientRequestFailure        Enabled   hpWlanClientReAssociation  Enabled
hpWlanDot1XAuthNotInitiated       Enabled   hpWlanDot1XAuthFailure     Enabled
hpWlanLocalMacAuthClientFailure   Enabled   hpWlanDot1XAuthSuccess     Enabled
hpWlanLocalMacAuthClientSuccess   Enabled   hpWlanMgmtAccessUpdate     Enabled
hpWlanPossibleNeighborApDetected  Enabled   hpWlanMgmtVlanIdUpdate     Enabled
hpWlanRadiusAccountingUpdate      Enabled   hpWlanRadiusServerFailover Enabled
hpWlanRemoteMacAddrAuthFailure    Enabled   hpWlanSystemUp             Enabled
hpWlanRemoteMacAddrAuthSuccess    Enabled   hpWlanSystemDown           Enabled
hpWlanSystemFWUpgradeStatus       Enabled   hpWlanVlanUntaggedUpdate   Enabled
hpWlanSystemConfigFileTransfer    Enabled
ProCurve Access Point 530#
```

lldp

This command enables Link Layer Discovery Protocol (LLDP) service on the device. The no version of the command disables LLDP on the device.

Syntax

lldp
no lldp

Default

Enabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#lldp
ProCurve Access Point 530(config)#
```

show lldp

This command displays the status of the Link Layer Discovery Protocol (LLDP) service on the device.

Syntax

show lldp

Default

N/A

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#show lldp
LLDP Status   Enabled
ProCurve Access Point 530(config)#
```

Flash/File Commands

These commands are used to manage the system software or configuration files.

Command	Function	Mode	Page
copy <ftp | scp | tftp> <flash | startup-config> *<ip> <file>* [user-name *<user>* password *<pass>*]	Copy data from a remote server onto the device.	MC	9-46
copy startup-config <ftp | scp | tftp> <flash | startup-config> *<ip> <file>* [user-name *<user>* password *<pass>*]	Copy the startup configuration file from the device to the specified remote server.	MC	9-46
copy factory-default <startup-config | custom-default>	Reset a configuration file to the factory-default configuration on the device.	MC	9-46
copy running-config<startup-config | custom-default>	Reset a configuration file to the running configuration on the device.	MC	9-46
erase	Reset the specified configuration file stored on the device.	MC	9-47
write	View or save the running configuration of the device.	MC	9-48
show config	Display the startup configuration on the device.	MC	9-49
show copy	Display the status of the last copy operation.	MC	9-49
show tech	Display the technical support output.	MC	9-50
show custom-default	Display the customer-modified version of the factory-default configuration.	MC	9-51
show running-config	Display the running configuration of the device.	MC	9-52

copy

This command copies data from a remote server onto the device.

Syntax

copy <ftp | scp | tftp> <flash | startup-config> <ip> <file> [user-name <user> password <pass>]

- **ftp | scp | tftp**-Specify the type of remote server where the file is located. Possible servers are File Transfer Protocol (FTP), Secure Copy Protocol (SCP), and the Trivial File Transfer Protocol (TFTP).
- **flash**-Specify that the type of file to retrieve, is an image file that will be used to upgrade bootcode and/or software on the device.
- **startup-config**-Specify that the type of file to retrieve, is the startup configuration file. This operation will replace the existing startup configuration file on the device.
- ***ip***-The IP address of the remote server.
- ***file***-The filename of the file on the remote server.
- **user-name *<user>* password *<pass>***-Specify the username and password for the FTP and SCP remote servers.

Default Setting

N/A

Command Mode

Manager Exec

Example.

```
ProCurve Access Point 530#copy startup-config tftp
192.168.1.52 copystart
ProCurve Access Point 530#copy ftp flash 192.168.1.52
WA.01.00.img user-name Chris password chrispass
ProCurve Access Point 530#
```

copy custom-default startup-config

This command sets the startup configuration file to contain the same settings as the customer-modifiable configuration on the device and reloads the device. This option is functionally the same as the **erase startup-config** command.

Syntax

copy custom-default startup-config

Default Setting

N/A

Command Mode

Manager Exec

Example

In this example, the copy custom-default startup-config command resets the startup configuration to the same setting as the custom-default configuration.

```
ProCurve Access Point 530#copy custom-default startup-config
ProCurve Access Point 530#
```

Related Commands

erase (page 9-47)

copy startup-config

This command copies the startup configuration file from the device to the specified remote server.

Syntax

copy startup-config <ftp | scp | tftp> <flash | startup-config> <ip> <file> [user-name <user> password <pass>]

- **startup-config**-Specify that the type of file to copy, is the startup configuration file.
- **ftp | scp | tftp**-Specify the type of remote server where the file will be placed. Possible servers are File Transfer Protocol (FTP), Secure Copy Protocol (SCP), and the Trivial File Transfer Protocol (TFTP).
- ***ip***-The IP address of the remote server.
- ***file***-The filename of the file on the remote server.
- **user-name *<user>* password *<pass>***-Specify the username and password for the FTP and SCP remote servers. These parameters are not used for TFTP.

Default Setting

N/A

Command Mode

Manager Exec

Example.

```
ProCurve Access Point 530#copy stratup-config ftp
192.168.1.52 copystart user-name chris password open
ProCurve Access Point 530#copy startup-config tftp
192.168.1.52 copystart
```

copy factory-default

This command resets configuration file to the factory-default configuration on the device.

Syntax

copy factory-default <startup-config> | <custom-default>

- **startup-config**-Reset the startup configuration file to contain the same settings as the factory default configuration file.
- **custom-default**-Reset the default configuration file to contain the same settings as the factory default configuration file.

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#copy factory-default startup-
config
ProCurve Access Point 530#
```

copy running-config

This command saves the running-default to a configuration file on the device.

Syntax

copy running-default <startup-config> | <custom-default>

- **startup-config**-Copies the running configuration to the startup configuration file. This option is functionally the same as the write memory command.
- **custom-default**-Copies the running configuration to the customer-modifiable default configuration file.

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#copy running-default startup-
config
ProCurve Access Point 530#
```

Related Commands

write (page 9-48)

erase

This command resets the specified configuration file stored on the device.

Syntax

erase <custom-default | startup-config>

- **custom-default** - Resets the customer-modified version of the factory-default configuration.
- **startup-config** - Resets the startup-configuration to the custom-default configuration and reloads the device.

Default Setting

N/A

Command Mode

Manager Exec

Example

This example shows how to reset the startup configuration to the defaults.:

```
ProCurve Access Point 530#erase startup-config
ProCurve Access Point 530#
```

Related Commands

copy custom-default startup-config (page 9-44)

write

This command views or saves the running configuration of the device.

Syntax

write <memory | terminal>

- **memory**- Copies the running configuration to the startup configuration file. This is the same as the **copy running-default startup-config** command.
- **terminal**- Displays the running configuration of the device on the terminal.

Default Setting

N/A

Command Mode

Manager Exec

Example.

```
ProCurve Access Point 530#write memory

ProCurve Access Point 530#
```

Related Commands

copy running-config startup-config (page 9-46)

show config

This command displays the startup configuration on the device.

Syntax

show config

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show config
------------------------------------------------------------
<?xml version="1.0"?>
<config>
  <interface name="wlan0wds1">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 2</
description>
  </interface>
 --MORE-,next page: Space, next line: Enter, quit: Control-C
```

show copy

This command displays the status of the last copy operation (ftp/scp/tcfp).

Syntax

show copy

Default Setting

N/A

Command Mode

Manager Exec

Global Configuration

Example

```
ProCurve Access Point 530#show copy
------------------------------------------------------------
Copy Operation Status (FTP/SCP/TFTP)

 Last software image (flash) copy result:   not initiated
 Last configuration file copy result:       not initiated

ProCurve Access Point 530#
```

show tech

This command displays the output of a predefined command sequence used by technical support.

Syntax

show tech

Default Setting

N/A

Command Mode

Manager Exec

Global Configuration

Example

```
ProCurve Access Point 530#show tech
------------------------------------------------------------
Description   Radio 1 - WLAN 10
Status        Disabled               SSID   SSID 10
VLAN          None                   BSSID  not assigned yet
DTIM Period   2
Security Type   no-security (No Sec.)   Closed System   Disabled
MAC Auth Mode   local deny-list only    MAC Auth List   not set
Authentication  open-system only        WEP Key Type    hex
WEP Key 1       ***                     WEP Key Size    128bit
WEP Key 2       ***                     Default Key     WEP Key
1
WEP Key 3       ***
WEP Key 4       ***
WPA or WPA2     WPA and WPA2            WPA Cipher      TKIP
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

show custom-default

This command displays the custom configuration file in a readable text format.

Syntax

show custom-default

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show custom-default
------------------------------------------------------------
<?xml version="1.0"?>
<config>
  <interface name="wlan0wds1">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 2</
description>
  </interface>
  <interface name="wlan0wds0">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 1</
description>
 --MORE-,next page: Space, next line: Enter, quit: Control-C
```

show running-config

This command displays the running configuration file in a readable text format.

Syntax

show running-config

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show running-config
<config>
<interface name="wlan0wds1">
  <radio>wlan0</radio>
  <type>wds</type>
  <status>down</status>
  <wep-key-length>104</wep-key-length>
  <wep-key-ascii>no</wep-key-ascii>
  <description>Wireless Distribution System - Link 2</
description>
</interface>
<interface name="wlan0wds0">
  <radio>wlan0</radio>
  <type>wds</type>
  <status>down</status>
  <wep-key-length>104</wep-key-length>
  <wep-key-ascii>no</wep-key-ascii>
  <description>Wireless Distribution System - Link 1</
description>
</interface>
<interface name="wlan0wds3">
  <radio>wlan0</radio>
  <type>wds</type>
  <status>down</status>
  <wep-key-length>104</wep-key-length>
  <wep-key-ascii>no</wep-key-ascii>
  <description>Wireless Distribution System - Link 4</
description>
</interface>
MORE --, next page: Space, next line: Enter, quit: Control-C
```

RADIUS Accounting/Authentication

The access point provides configuration for RADIUS Accounting servers and Radius Authentication which can be used to provide valuable information on user activity in the network.

Command	Function	Mode	Page
[no] radius-accounting <primary | secondary> <ip <ip> | port <port> | key <key>>	Enables RADIUS Accounting.	IC-R-WLAN	9-53
[no] radius <failover-to local | retransmit >	Establishes RADIUS failover and retransmit parameters for this WLAN.	IC-R-WLAN	9-54
[no] radius <<primary | secondary> <ip <ip> | local | mac-auth-password <password> | mac-format <multi-colon | multi-dash | no-delimiter | single-dash> | port <port> | key <key>>	Configures RADIUS parameters.	IC-R-WLAN	9-54

radius-accounting

This command enables RADIUS Accounting for the SSID on the access point. Use the **no** form to disable RADIUS Accounting. To validate these settings, use the show wlan <index> command, see page 93.

Syntax

radius-accounting <primary | secondary> <ip *<ip>* | port *<port>* | key *<key>*>
no radius-accounting

- **primary**- Configure settings (IP, port, key) for the primary RADIUS accounting server. The no version of the command disables use of the primary RADIUS accounting server by clearing the IP address setting.
- **secondary-** Configure settings (IP, port, key) for the secondary RADIUS accounting server. The no version of the command disables use of the secondary RADIUS accounting server by clearing the IP address setting.
- **ip *<ip>***- The IP address of the RADIUS server.
- **port *<port>*-** The port of the RADIUS server.
- **key*<key>*-** The shared secret string for the RADIUS server.

Default Setting

Disabled

Command Mode

WLAN Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
primary ip 192.168.1.52
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
port 161
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
key blue
ProCurve Access Point 530(radio1-wlan1)#
```

radius failover-to-local | retransmit

This command configures RADIUS authentication failover and the RADIUS retransmit retry parameter for this WLAN. To validate these settings, use the show wlan <index> command, see page 93.

Syntax

radius <failover-to-local | retransmit <limit>>
no radius

- **failover-to-local**- Enable the use of the local (built-in) RADIUS authentication server in addition to any primary and secondary RADIUS authentication server. The no version of the command disables use of the local (built-in) RADIUS authentication server as an additional server.
- **retransmit *<limit>*-** Set the number of retry attempts that are made to a RADIUS authentication/accounting server until switching to the next server on the list. The no version of the command is not available for this parameter. (Valid values: 1-30)

Default Setting

Disabled. Retransmit value set to 3.

Command Mode

WLAN Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius failover-to-
local
ProCurve Access Point 530(radio1-wlan1)#radius retransmit 30
```

radius primary | secondary

This command configures RADIUS configures primary and secondary parameters for this WLAN. To validate these settings, use the show wlan <index> command, see page 93.

Syntax

radius <primary | secondary> <ip <ip> | local | mac-auth-password <password> | mac-format <multi-colon | multi-dash | no-delimiter | single-dash> | port <port> | key <key>>
no radius primary | secondary

- **primary** - Configure settings (IP, port, key) for the primary RADIUS authentication server. The no version of the command disables use of the primary RADIUS authentication server by clearing the IP address setting.
- **secondary** - Configure settings (IP, port, key) for the secondary RADIUS authentication server. The no version of the command disables use of the secondary RADIUS authentication server by clearing the IP address setting.
- **ip <ip>** - The IP address of the RADIUS server. Default is 192.168.1.10.
- **local** - Use the local (built-in) radius server.
- **port <port>** - The port of the RADIUS server.
- **key <string>** - The shared secret string for the RADIUS server.
- **mac-auth-password <password>** - Set the password that will be used by wireless stations for remote MAC authentication with the primary RADIUS server. The no version of the command clears the password and uses the wireless stations' MAC addresses as the password.
- **mac-format multi-colon** - MAC addresses are in the form xx:xx:xx:xx:xx:xx.
- **mac-format multi-dash** - MAC addresses are in the form xx-xx-xx-xx-xx-xx.

- **mac-format no-delimiter** - MAC addresses are in the form xxxxxxxxxxxx.
- **mac-format single-dash** - MAC addresses are in the form xxxxxx-xxxxxx.

Default Setting

DHCP is enabled.

Command Mode

WLAN Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#wlan 1
ProCurve Access Point 530(radio1-wlan1)#radius primary key
open
ProCurve Access Point 530(radio1-wlan1)#radius primary ip
192.168.1.53
ProCurve Access Point 530(radio1-wlan1)#radius primary mac-
format mutli-colon
ProCurve Access Point 530(radio1-wlan1)#
```

RADIUS Users

The access point provides configuration to add local RADIUS user information in the network.

Command	Function	Mode	Page
[no] radius-local <*username*>[disabled] | [password <*password*>] | realname <*realname*>]	Configure a new radius-local user account or modify a user account.	GC	9-57
show radius-local	Shows the radius-local users.	MC	9-58

radius-local

The commands are used to set up and manage user accounts on the built-in RADIUS server.

Syntax

radius-local <*username*> [disabled] | [password <*password*>] | [realname <*realname*>]

no radius-local

- ***username*** - Create a new user account or modify an already existing account with the specified username. The no version of the command removes the user account with the specified username. (Maximum characters - 50)
- **disabled** - Set the user account to be disabled. The no version of the command re-enables the user account.
- ***password***- Specify the password to be used with the user account. (Range: 1-32 alphanumeric characters)
- ***realname*** **-** Specify the real name for the account holder on the user account.
(No spaces. Maximum characters - 50)

Default Setting

None

Command Mode

Global Configuration

Example:

The following example first sets the radius-local username to "chris" and subsequently sets the password for the chris user account to "chrisopen".

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radius-local chris
ProCurve Access Point 530(config)# radius-local chris
password chrisopen

ProCurve Access Point 530(config)#
```

This example sets the real name of the chris user account to chris smith.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radius-local chris
ProCurve Access Point 530(config)# radius-local chris
realname CSmith

ProCurve Access Point 530(config)#
```

show radius-local

This command configures user account information for the internal RADIUS server on this device.

Syntax

show radius-local

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# show radius-local

Username   Real Name   Status
---------- ---------- ----------
MSmith     Mr Smith    Enabled
Chris      CSmith      Enabled

ProCurve Access Point 530(config)#
```

MAC Address Authentication

Use these commands to define MAC authentication on the access point. For local MAC authentication, first create the MAC authorization lists, enter the MAC addresses to be filtered and then define the default filtering policy using the address filter default command.

Command	Function	Mode	Page
[no] mac-auth-local <*listname*> mac **<***mac address***>**	Sets the MAC addresses to be filtered.	GC	9-60
[no] mac-auth-local <*listname*> **<**accept list| deny list**>**	Sets filtering to allow or deny listed addresses.	IC-R-WLAN	9-60
[no] mac-auth-remote	Enables remote MAC authentication.	IC-R-WLAN	9-60
show mac-auth-local [<name>]	Shows the MAC entries on the specified device.	MC	9-62

mac-auth-local

This command adds or removes entries in the local MAC address authentication control lists on the device.

Syntax

mac-auth-local <*listname*> mac <*mac address*> | <accept-list> |<deny-list>

no mac-auth-local <*listname*> mac <*mac address*>

- ***listname*** - Specifies the name of an entire MAC address authentication control list. The no version of the command removes the MAC address authentication list and all entries in the entire list.
- ***mac address***- Specifies an entry in the authentication control list by MAC address. The no version of the command removes the specific MAC address entry from the specific MAC address authentication control list. Valid format is 00:00:00:00:00:00 ~FF:FF:FF:FF:FF:FF.
- **accept list** -The wireless stations whose MAC address is on the list will be allowed access to the device.
- **deny list** -The wireless stations whose MAC address is on the access list will be prevented from having access to the device.

Default

None

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#mac-auth-local Bob
accept-list
ProCurve Access Point 530(radio1-wlan1)#
```

mac-auth-remote

This command enables remote MAC address authentication by using the RADIUS authentication server settings on this WLAN. The no version of the command disables remote MAC authentication on the BSS.

Syntax

mac-auth-remote

no mac-auth-remote

Default

None

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#mac-auth-remote
ProCurve Access Point 530(radio1-wlan1)#
```

show mac-auth-local

This command displays all the entries in the local MAC address authentication control lists on the device.

Syntax

show mac-auth-local [<*name*>]

- ***name***- Displays only MAC address entries for the specified list.

Default

N/A

Command Mode

WLAN Radio Interface Configuration

Example

```
ProCurve Access Point 530#show mac-auth-local mylist
MAC address entries for authentication control list "mylist":

MAC Addresses
----------------------------------------------------------------------
00:11:22:33:44:55
00:aa:bb:cc:dd:ee

ProCurve Access Point 530#
ProCurve Access Point 530
```

Filtering Commands

The commands described in this section are used to filter communications between wireless stations, control access to the management interface from wireless stations, and filter traffic using specific Ethernet protocol types.

Command	Function	Mode	Page
[no] inter-station-blocking	Enables communication between wireless stations.	GC	9-63
[no] wireless-mgmt-block	Enables communication between wireless stations.	GC	9-64
show filters	Display filter details.	MC	9-64

inter-station-blocking

This command enables inter station blocking on the device. The no version of the command disables inter station blocking on the device.

Syntax

inter-station-blocking
no inter-station-blocking

Default

Disabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#inter-station-blocking
ProCurve Access Point 530(config)#
```

wireless-mgmt-block

This command enables access to the management interfaces (http/telnet/etc.) from the wireless side on the device. The no version of the command disables this ability on the device.

Syntax

wireless-mgmt-block
no wireless-mgmt-block

Default

Disabled.

Command Mode

Global Configuration

Manager Exec

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)#wireless-mgmt-block

ProCurve Access Point 530(config)#
```

show filters

This command displays management/traffic/security filter settings for the device.

Syntax

show filters

Default

N/A

Command Mode

Global Configuration

Manager Exec

Example.

```
ProCurve Access Point 530#show filters
------------------------------------------------------------
Traffic/Security Filters:
Wireless Management Blocking   Enabled
Inter-Station Blocking         Disabled
ProCurve Access Point 530#
```

Ethernet Interface Commands

The commands described in this section configure connection parameters for the Ethernet interface.

Command	Function	Mode	Pag e
interface <*interface*>	Enters Ethernet interface configuration mode	GC	9-66
enable	Enables the interface.	IC-E	9-67
disable	Disables the interface.	IC-E	9-67
description	Specifies a text string description of this interface.	IC-E	9-68
dns primary <*server_1*>	Specifies the primary name server.	GC	9-68
dns secondary <*server_2*>	Specifies the secondary name server.	GC	9-69
[no] ip address <<ip> <mask> | <ip>/<bits> | dhcp>	Sets the IP address for the Ethernet interface.	IC-E	9-70
[no] ip default-gateway <*ip*>	Sets the static default gateway router for the device.	IC-E	9-71
speed-duplex <auto|auto-10|auto-100|10-half|100-half|10-full|100-full>	Sets the mode of operation for the Ethernet port.	IC-E	9-72
show ip	Shows the ip status on the device.	MC	9-72
show interfaces<*interface*>	Shows the status for the Ethernet interface.	MC	9-73

interface

This command configures the specified interface or enters the Interface Configuration Context.

Syntax

interface <*interface*>

- ***interface*** - The name of the interface. I.E. ethernet

Default Setting

N/A

Command Mode

Global Configuration

Example:

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#
```

enable (ethernet)

This command enables the specified interface.

Syntax

enable

Default Setting

N/A

Command Mode

Ethernet Interface Configuration

Example:

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#enable
ProCurve Access Point 530(ethernet)#
```

disable (ethernet)

This command disables the specified interface.

Syntax

disable

Default Setting

N/A

Command Mode

Ethernet Interface Configuration

Command Usage

This command allows you to disable the Ethernet interface due to abnormal behavior (e.g., excessive collisions), and re-enable it after the problem has been resolved. You may also want to disable the Ethernet interface for security reasons.

Example:

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#disable
Connection to the host is lost.
```

description

This command specifies a human-readable string description of this interface.

Syntax

description <*string*>

- ***string***- The alphabetical description of the interface.

  (Maximum characters 1-255)

Default Setting

None

Command Mode

Ethernet Interface Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#description Ethernet
ProCurve Access Point 530(config)#
```

dns primary

This command establishes the primary DNS server address. The no version of the command clears the primary IP address, if one is set and does not require for the IP to be specified.

Syntax

dns primary <*server_1*>

- ***server_1*** - A static ip address set to the primary dns server. (0.0.0.0~255.255.255.255)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The primary and secondary name servers are queried in sequence.
- The static ip address is used if the dhcp client is enabled, but can't contact a DHCP server. If contact is made with a DHCP server, then the DHCP client must be disabled in order to implement a static ip address.

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#dns primary 192.168.1.55
ProCurve Access Point 530(config)#
```

dns secondary

This command establishes the secondary DNS server address. The no version of the command clears the secondary IP address, if one is set and does not require for the IP to be specified.

Syntax

dns secondary <*server_2*>

- ***server_2*** - A static ip address set to the secondary dns server. (0.0.0.0~255.255.255.255)

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#dns secondary 10.1.0.55
ProCurve Access Point 530(config)#
```

ip address

This command configures the IP address settings for the interface. The no version of the command clears the statically assigned IP address and network mask.

Syntax

ip address <*ip*> [<*mask*>] | <*ip*>/<*bits*> | dhcp
no ip address

- ***ip*** - Specify the static IP address to be used when DHCP is not used. The no version of the command clears the statically assigned IP address and network mask.
- ***mask*** - Specify the static network mask to be used when DHCP is not used. The no version of the command clears the statically assigned IP address and network mask.
- ***bits*** - Specify the static network mask in CIDR notation to be used when DHCP is not used. The no version of the command clears the statically assigned IP address and network mask.
- **dhcp** - Enable the DHCP client on this interface. The no version of the command disables the DHCP client on this interface.

Default Setting

IP address: 192.168.1.1
Netmask: 255.255.255.0

Command Mode

Interface Configuration (Ethernet)

Command Usage

CAUTION

In order to disable the DHCP and assign a Static IP address, you must have a serial port connection to the AP. Otherwise, you will lose connectivity during the process of assigning a new static IP address.

- DHCP is enabled by default.The static ip address is used if the dhcp client is enabled, but can't contact a DHCP server. If contact is made with a DHCP server, then the DHCP client must be disabled in order to implement a static ip address.
- You must assign an IP address to this device to gain management access over the network or to connect to existing IP subnets. You can manually configure a specific IP address using this command, or direct the device to obtain an address from a DHCP server using the **ip dhcp** command. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the configuration program.

Example

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#ip address 192.168.1.2
255.255.255.0
ProCurve Access Point 530(ethernet)#
```

ip default-gateway

This command sets the static default gateway router for the device. The no version of the command does not require parameters and resets the address of the default gateway router, if any.

Syntax

ip default-gateway ***<ip>***

no ip default-gateway

- ***ip*** - The IP address of the default gateway router. The no version of the command is not available for this parameter

Default Setting

N/A

Command Mode

Ethernet Interface Configuration

Example:

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#ip default-gateway
192.168.1.1
ProCurve Access Point 530(ethernet)#
```

speed duplex

This command configures the mode of operation for the Ethernet port (Requires reboot).

Syntax

speed-duplex <auto |auto-10 |auto-100 |10-half |100-half |10-full |100-full >

- **auto** - Uses auto negotiation for speed and duplex mode.
- **auto-10** - 10 Mbps, uses auto negotiation for duplex mode.
- **auto-100** - 100 Mbps, uses auto negotiation for duplex mode.
- **10-half** - 10 Mbps, half-duplex.
- **100-half** - 100 Mbps, half-duplex.
- **10-full** - 10 Mbps, full-duplex.
- **100-full** - 100 Mbps, full-duplex

Default Setting

auto

Command Mode

Interface Configuration (Ethernet)

Example

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#speed-duplex auto
ProCurve Access Point 530(ethernet)#
```

show ip

This command displays the IP address information, static default gateway router configuration and the DHCP client configuration/status on the device.

Syntax

show ip

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show ip
IP Address Information:
-------------------------------------------------
System Host Name  ProCurve-AP-530
IP Address        192.168.1.2
Subnet Mask       255.255.255.0
Default Gateway   192.168.1.253
DHCP Client       Enabled

DNS Information (Obtained from DHCP):
Domain Name Suffix   example.ca.example.net.
Primary DNS Server   204.127.202.0
Secondary DNS Server 216.148.227.00

ProCurve Access Point 530
```

show interface

This command displays the status for the Ethernet interface.

Syntax

show interface *<interface>*

- ***interface*** - Display detailed information about the specified interface. i.e. ethernet

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show interface ethernet
Ethernet interface:
------------------------------------------------------------
Description            Ethernet
MAC address            00:14:C2:A5:08:CB
Speed-duplex           auto
Administrative status  Enabled
Link status            [add-in-future]
Management VLAN ID     1    (U)
Untagged-VLAN ID       1
Spanning Tree (STP)    Enabled
STP Port State         forwarding
STP Hello Interval     10.0
STP Forward Delay      10
STP Bridge Priority    255

Bytes Rx             70912184     Bytes Tx
30955292
Packets Rx           194926       Packets Tx
286333
Compressed Rx        0            Compressed Tx          0
Mcast packets Rx     0            Carrier errors Tx      0
Dropped Rx packets   0            Dropped Tx packets     0
FIFO overflows Rx    0            FIFO overflows Tx      0
Frame errors Rx      0            Packet collisions Tx   0
Total Rx errors      0            Total Tx errors        0
ProCurve Access Point 530#
```

show ip

This command displays the IP address information, static default gateway router configuration and the DHCP client configuration/status on the device.

Syntax

show ip

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530#show ip
IP Address Information:
-------------------------------------------------
System Host Name  ProCurve-AP-530
IP Address        192.168.1.2
Subnet Mask       255.255.255.0
Default Gateway   192.168.1.253
DHCP Client       Enabled

DNS Information (Obtained from DHCP):
Domain Name Suffix   example.ca.example.net.
Primary DNS Server   204.127.202.0
Secondary DNS Server 216.148.227.00

ProCurve Access Point 530
```

Wireless Interface Commands

The commands described in this section configure global parameters for the wireless interface.

Command	Function	Mode	Page
radio	Enters wireless interface configuration mode.	GC	9-77
ssid *<ssid>*	Sets SSID string.	IC-R	9-78
description	Adds a description to the wireless interface.	IC-R	9-79
closed-system	Closes access to stations without a pre-configured SSID.	IC-R-WLAN	9-79
mode*<value>*	Sets the radio working mode.	IC-R	9-80
antenna <external | internal>	Sets the antenna on this radio.	IC-R	9-81
antenna mode<diversity | single>	Sets the antenna mode.	IC-R	9-81
basic-rate*<value>*	Configures the maximum data rate at which the access point can transmit traffic.	IC-R	9-82
supported-rate*<value>*	Configures the maximum data rate at which the access point can transmit traffic.	IC-R	9-83
channel-policy *<static|auto>*	Sets the policy on the channel to static or automatic.	IC-R	9-83
beacon-interval *<interval>*	Configures the rate at which beacon frames are transmitted from the access point.	IC-R	9-84
dtim-period	Configures the rate at which stations in sleep mode must wake up to receive broadcast/ multicast transmissions	IC-R	9-85
max-stations	Configures the maximum number of stations that can be associated with the access point at the same time	IC-R	9-86
preamble	Sets the length of signal preamble.	IC-R	9-86
[no] protected-mode	Sets the 802.11 b/g CTS protection mode for this radio.	IC-R	9-87
fragmentation-thresh	Configures the minimum packet size that can be fragmented	IC-R	9-87

Command	Function	Mode	Page
inactivity-timeout	Configures the inactivity time.	IC-R	9-88
slot-time	Sets the wait time.	IC-R	9-89
rts-threshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-R	9-89
tx-power-reduction	Adjusts the power of the radio signals transmitted from the access point.	IC-R	9-90
enable	Enables the radio or SSID wireless interfaces.	IC-R IC-R-WLAN	9-91
disable	Disables the radio or SSID wireless interfaces.	IC-R IC-R-WLAN	9-92
show radio *<radio>*	Shows the status for the wireless interface	MC	9-92
show wlan *<ssid_index>*	Displays parameters for the specified SSID interface	MC	9-93
show basic-rate	Displays the specified basic rate for the interfaces.	MC	9-98
show stations	Display information about associated wireless stations.	MC	9-98
show supported-rate	Displays the supported rates for the interfaces.	MC	9-99

radio

This command enters the wireless interface configuration mode for configuring parameters for the radio interface.

Syntax

radio <*radio_name*>

- ***radio_name***- The name used to identify the radio. I.E. 1, 2.

Default Setting

None

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#
```

ssid

This command sets the Service Set Identifier (SSID) for this WLAN.

Syntax

ssid <SSID>

- **ssid** - The text string that specifies the SSID of the interface. (1 - 32 alphanumeric characters)

Default Setting

SSID 1 (to 16)

Command Mode

Interface Configuration (Wireless)

Command Usage

- The maximum number of supported SSID indexes is 16 Any index number in the range 1 to 16 can be selected for an SSID interface per radio.
- Each SSID interface name must be unique.
- stations that want to connect to the network via the access point must set their SSIDs to match one of the access point's SSID interfaces.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#ssid donna
ProCurve Access Point 530(radio1-wlan1)#
```

description

This command adds a description to the radio, ssid, or wds interfaces. Use the **no** form to remove the description. The interface description is displayed when using the **show wlan 1** command from the Manager Exec level.

Syntax

description <*string*>
no description

- ***string*** - Comment or a description for this interface.
(Range: 1-80 characters)

Default Setting

Radio: Radio 1 - WLAN 1

SSID: SSID 1

Command Mode

Radio Interface Configuration

WDS Radio Interface Configuration

WLAN Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#description RD-AP#3
ProCurve Access Point 530(radio1-wlan1)#
```

closed-system

This command closes access to stations without a pre-configured SSID. Use the **no** form to disable this feature.

Syntax

closed-system
no closed-system

Default Setting

Disabled

Command Mode

WLAN Interface Configuration

Command Usage

- When closed system is enabled, stations with a configured SSID of "any" are not able to associate with the access point.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#closed-system
ProCurve Access Point 530(radio1-wlan1)#
```

mode

This command sets the wireless mode for the interface.

Syntax

mode <a | b | g>

- **a**- 802.11a stations operate in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. **Supported only on the access point's second radio (radio2).**
- **b** -802.11b stations include 5.5 Mbp and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. **Supported on both the access point's radios (1 and 2).**
- **g** -802.11g stations operate at a higher speed extension (up to 54 Mbps) to the 802.11b PHY while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps. **Supported on both the access point's radios (1 and 2). By default 802.11g supports 802.11b.**

Default Setting

g

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# mode g
ProCurve Access Point 530(radio1)#
```

antenna

This command configures which antenna to use with this radio.

Syntax

antenna <external | internal>

- **external**- Use the external antenna sockets on the AP (for external antenna).
- **internal** -Use the internal (built-in) antenna(s).

Default Setting

internal

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# antenna external
ProCurve Access Point 530(radio1)#
```

antenna mode

This command sets the antenna diversity mode on this radio. These settings only have an effect if the external antenna configuration is used.

Syntax

antenna mode <diversity | single>

- **diversity**- Diversity (2 connections/elements) antenna system.

- **single** -Single antenna (using the "primary" antenna plug only.

Default Setting

Diversity

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# antenna mode diversity
ProCurve Access Point 530(radio1)#
```

basic-rate

This command configures the specified transmission rate to the **set** of advertised rates for this radio. The no version of the command removes the specified transmission rate from the **set** of advertised rates for this radio.

Syntax

basic-rate <*value*>

no basic rate

- ***value***- The transmit data rate value set. (Options: 1, 2, 5.5, 6, 9, 11 Mbps for a and b modes; 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 54 Mbps for g mode)

Default Setting

Radio 1: 1, 2, 5.5, 11 Mbps for g mode
Radio 2: 6, 12,24 for a mode

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# basic-rate 9
ProCurve Access Point 530(radio1)#
```

supported-rate

This command adds the specified transmission rate to the **set** of supported rates for this radio. The no version of the command removes the specified transmission rate from the **set** of supported rates for this radio.

Syntax

supported-rate <*value*>

no supported-rate

- ***value***- The transmission data rate value. (Options:1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 54 Mbps)

Default Setting

(Options:1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 54 Mbps)

Command Mode

Interface Configuration (Wireless)

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# supported-rate 24
ProCurve Access Point 530(radio1)#
```

channel-policy

This command sets the channel utilization policy on this radio.

Syntax

channel-policy auto | static <*channel* >

- **auto** - Automatically detect and use the least congested channel.
- **static**- Use the statically configured channel.
  - ***channel*** -The specific channel.

Default Setting

auto

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# channel-policy static 1
ProCurve Access Point 530(radio1)#
```

beacon-interval

This command configures the rate at which beacon frames are transmitted from the access point. See rate-limit (page 9-127) syntax for setting the broadcast/multicast rates and burst values (in packets per second).

Syntax

beacon-interval <*value*>

- ***value***- The rate for transmitting beacon frames.
  (Range: 20-2000 microseconds)

Default Setting

100. The default behavior is to send a beacon frame once every 100 microseconds (or 10 per second).

Command Mode

Radio Interface Configuration

Command Usage

The beacon frames allow wireless stations to maintain contact with the access point. They may also carry power-management information.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)#beacon-interval 150
```

Related Commands

rate-limit (page 9-127)

dtim-period

This command configures the frequency at which stations sleeping in low-power mode should wake up to receive broadcast/multicast transmissions.

Syntax

dtim-period <*value*>

- ***value***- Interval between the beacon frames that transmit broadcast or multicast traffic. Setting this value to "2", allows stations to check on every other beacon. (Range: 1-255 beacon frames)

Default Setting

2

Command Mode

WLAN Interface Configuration

Command Usage

- The Delivery Traffic Indication Map (DTIM) packet interval value indicates how often the MAC layer forwards broadcast/multicast traffic. This parameter is necessary to wake up stations that are using Power Save mode.
- The DTIM is the interval between two synchronous frames with broadcast/multicast information. The default value of 2 indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.
- Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)# dtim-period 100
ProCurve Access Point 530(radio1-wlan1)#
```

max-stations

This command sets the maximum number of wireless stations for this WLAN.

Syntax

max-stations*<value>*

- ***value***- The value of the maximum number of stations. Valid value is between 0 and 256.

Default Setting

256

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# max-stations 100
ProCurve Access Point 530(radio1#
```

preamble

This command sets the length of the signal preamble for this radio.

Syntax

preamble<long | short>

- **long -** Uses a long preamble only.
- **short -** Uses a short or long preamble.

Default Setting

long

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# preamble short
ProCurve Access Point 530(radio1#
```

protected-mode

This command configures the 802.11 b/g CTS protection mode for this radio. The no version of the command disables the protection mode.

Syntax

protected-mode

no protected-mode

Default Setting

Enabled

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# protected-mode
ProCurve Access Point 530(radio1#
```

fragmentation-thresh

This command configures the minimum packet (frame) size that can be fragmented when passing through the access point.

Syntax

fragmentation-thresh <*value*>

- ***value*** - Minimum packet (frame) size for which fragmentation is allowed. (Range: 256-2346 bytes)

Default Setting

2346 (This effectively disables fragmentation)

Command Mode

Radio Interface Configuration

Command Usage

- If the packet size is smaller than the preset fragment size, the packet will not be fragmented.
- Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.
- Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# fragmentation-thresh 512
ProCurve Access Point 530(radio1)#
```

inactivity-timeout

This command configures the length of time after which a wireless station is considered inactive if no traffic has been received from the station by this radio.

Syntax

inactivity-timeout <*value*>

- ***value*** - The inactivity value in seconds. (Range: 300-86400 seconds)

Default Setting

1800

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# inactivity-timeout 10
ProCurve Access Point 530(radio1)#
```

slot-time

This command sets the wait-time before transmitting data on this radio.

Syntax

slot-time <long | short>

- **long -** Uses a long wait-time.
- **short -** Uses a short wait-time.

Default Setting

short

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# slot-time short
ProCurve Access Point 530(radio1#
```

rts-threshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving station prior to the sending station starting communications.

Syntax

rts-threshold <*threshold*>

- ***threshold*** - Threshold packet size for which to send an RTS.
  (Range: 0-2347 bytes)

Default Setting

2347

Command Mode

Radio Interface Configuration

Command Usage

- If the threshold is set to 0, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.
- The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS frame to notify the sending station that it can start sending data.
- Access points contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node” problem.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# rts-threshold 216
```

tx-power-reduction

This command adjusts the power value of the radio signals transmitted from the access point.

Syntax

trx-power-reduction *<value>*

- ***value***- Set the value which is subtracted from the maximum signal strength value, then the resulting value is the power value used by the radio. This value is in dB.

Default Setting

0

Command Mode

Radio Interface Configuration

Command Usage

- The radio operates at maximum power when this parameter is set to 0 dB.
- It may be necessary to apply Tx Power Reduction, if your antenna gain causes the radio power to exceed the regulatory domain limit.
- You may also want to apply Tx Power Reduction to avoid overlap with another access point coverage area (Default is 0)

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# tx-power-reduction 5
ProCurve Access Point 530(radio1)#
```

enable (wireless)

This command enables either the radio, ssid, or wds interfaces.

Syntax

enable

Default Setting

N/A

Command Mode

Radio Interface Configuration

WDS Interface Configuration

WLAN Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# enable
```

disable (wireless)

This command disables either the radio, ssid, or wds interfaces.

Syntax

disable

Default Setting

N/A

Command Mode

Radio Interface Configuration

WDS Interface Configuration

WLAN Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# disable
ProCurve Access Point 530(radio1)#
```

show radio

This command displays detailed information about the radio.

Syntax

show radio [*<radio>]*

- ***radio-*** Display detailed information about the specified radio.

Default Setting

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530# show radio
------------------------------------------------------------
Radio  Status     Base MAC Address    Mode      Channel       TX-Power
-----------------------------------------------------------------------
1      Disabled   00:14:C2:A5:22:E0   802.11g   1  - Auto     0 dBm
2      Disabled   00:14:C2:A5:22:F0   802.11a   36 - Auto     0 dBm

ProCurve Access Point 530# show radio 1
------------------------------------------------------------
Description    Radio 1 - 802.11g
Base MAC       00:14:C2:A5:22:E0       Status                 Disabled
Mode           802.11g                 Channel-Policy         Auto
Channel        1                       WLANs Supported        16
Preamble       long                    CTS Protection         Enabled
Slot-time      short                   Beacon-Interval(K-us)  100
TX-Power(dBm)   10.0                   Power Reduction(dB)    5
Antenna Mode   diversity               Antenna(s) In Use      internal
RTS-Threshold  2347                    Fragment-Threshold     2346
WMM QoS        Enabled                 Inactivity Timeout     not set
Max Stations   not set

Rate-Limiting (Disabled)
Rate-Limit(packets/second)   50        Burst-Limit(packets/second)  75

802.11h (Disabled)                     Radar-Detection          Disabled
Blocked-Time     30                    Quiet Duration Interval  0
TX-Mitigation    3                     Quiet Period (Beacon)    0

AP-Detection (Disabled)
Periodic Scan Duration(ms)   30        Periodic Scan Interval(sec)   10
List Max Entries             255       List Expiration Time(sec)     3600
ProCurve Access Point 530#
```

show ssid

This command provides information about the Service Sets/Basic Service Sets of the radio(s) on the device. If in a radio or WLAN context, displays information only about the radio in context. This is functionally equivalent to the show wlan command.

Syntax

show ssid [*<name>*] [statistics] [all]

- ***<name>***- Displays detailed information about the specified WLAN (SSID/BSS).

- **statistics -** Display traffic counters in addition to information about the WLAN (SSID/BSS).
- **all** - Display information about the WLAN (SSID/BSS) on both radios (only has an effect when in a radio or WLAN context).

Default

N/A

Command Mode

Manager Exec

WLAN Interface Configuration

Example: show ssid 1

```
ProCurve Access Point 530# show ssid 1
WLAN #1 on Radio 1
Description   Radio 1 - WLAN 1
Status        Enabled                SSID   SSID 1
VLAN          1    - Untagged        BSSID  00:14:C2:A5:22:E0
DTIM Period   2
Security Type   no-security (No Sec.)          Closed System   Disabled
MAC Auth Mode   local accept-list only         MAC Auth List   mylist
Authentication  open-system only               WEP Key Type    hex
WEP Key 1       not set                        WEP Key Size    128bit
WEP Key 2       not set                        Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
WPA or WPA2     WPA and WPA2                   WPA Cipher      TKIP only
WPA Pre-auth.   Disabled
WPA Shared Key  not set
-- MORE --, next page: Space, next line: Enter, quit: Control-C#
```

Related Commands

show wlans (page 9-95)

show wlan

This command provides information about the Service Sets/Basic Service Sets of the radio(s) on the device. If in a radio or WLAN context, displays information only about the radio in context. This is functionally equivalent to the show ssid command.

Syntax

show wlans [<*name*>] [statistics] [all]

- **<*name*>**- Displays detailed information about the specified WLAN (SSID/BSS).
- **statistics -** Display traffic counters in addition to information about the WLAN (SSID/BSS).
- **all** - Display information about the WLAN (SSID/BSS) on both radios (only has an effect when in a radio or WLAN context).

Default

N/A

Command Mode

Manager Exec

WLAN Interface Configuration

Example: show wlans

```
ProCurve Access Point 530(radio1-wlan1)# show wlans
All WLANs on Radio 1:
#   WLAN                          BSSID              VLAN     Security Status
------------------------------------------------------------------------------
1   SSID 1                        00:14:C2:A5:22:E0  1   (U)  No Sec. Enabled
2   SSID 2                        not assigned yet   none(-)  No Sec. Disabled
3   SSID 3                        not assigned yet   none(-)  No Sec. Disabled
4   SSID 4                        not assigned yet   none(-)  No Sec. Disabled
5   SSID 5                        not assigned yet   none(-)  No Sec. Disabled
6   SSID 6                        not assigned yet   none(-)  No Sec. Disabled
7   SSID 7                        not assigned yet   none(-)  No Sec. Disabled
8   SSID 8                        not assigned yet   none(-)  No Sec. Disabled
9   SSID 9                        not assigned yet   none(-)  No Sec. Disabled
10  SSID 10                       not assigned yet   none(-)  No Sec. Disabled
11  SSID 11                       not assigned yet   none(-)  No Sec. Disabled
12  SSID 12                       not assigned yet   none(-)  No Sec. Disabled
13  SSID 13                       not assigned yet   none(-)  No Sec. Disabled
14  SSID 14                       not assigned yet   none(-)  No Sec. Disabled
15  SSID 15                       not assigned yet   none(-)  No Sec. Disabled
16  SSID 16                       not assigned yet   none(-)  No Sec. Disabled
All WLANs on Radio 2:
#   WLAN                          BSSID              VLAN     Security Status
------------------------------------------------------------------------------
1   SSID 1                        00:14:C2:A5:22:F0  1   (U)  WPA-.1X  Enabled
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

Example: show wlan1

```
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)# show wlan1
------------------------------------------------------------
WLAN #1 on Radio 1
Description   Radio 1 - WLAN 1
Status        Enabled                SSID   SSID 1
VLAN          1    - Untagged        BSSID  00:14:C2:A5:22:E0
DTIM Period   2

Security Type   no-security (No Sec.)          Closed System   Disabled
MAC Auth Mode   local accept-list only         MAC Auth List   mylist
Authentication  open-system only               WEP Key Type    hex
WEP Key 1       not set                        WEP Key Size    128bit
WEP Key 2       not set                        Default Key     WEP Key 1
WEP Key 3       not set
WEP Key 4       not set
WPA or WPA2     WPA and WPA2                   WPA Cipher      TKIP only
WPA Pre-auth.   Disabled
WPA Shared Key  not set

RADIUS
Failover To Local   Disabled                   Retransmit Num.  3
Primary Auth        not set                    Prim. Auth Port  1812
Prim. Auth Key      not set
Secondary Auth      not set                    Sec. Auth Port   1812
Sec. Auth Key       not set
Primary Acct        not set                    Prim. Acct Port  1813
Prim. Acct Key      not set
Secondary Acct      not set                    Sec. Acct Port   1813
Sec. Acct Key       not set
ProCurve Access Point 530(radio1-wlan1)#
```

Related Commands

show ssid (page 9-93)

show basic-rate

This command displays information about advertised transmission rates for this device.

Syntax

show basic rate

Default

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530# show basic-rate
Basic (advertised) data rates (Mbps).
--------------------------------------
Radio 1 (802.11g): 1, 2, 5.5, 11
Radio 2 (802.11a): 6, 12, 24, 54
ProCurve Access Point 530#
```

show stations

This command displays information about wireless stations.

Syntax

show stations [detail]

- **detail** - Display detailed information about associated wireless stations.

Default

N/A

Command Mode

Global Configuration

Example.

```
ProCurve Access Point 530#show stations
------------------------------------------------------------
Station           On WLAN (radio index/WLAN index)         Auth.  Assoc.  Fwd.
------------------------------------------------------------------------------
00:11:50:55:50:11  work1 (2/1)                              Yes    Yes     n/a
00:15:00:47:5f:6a  SSID 10 (1/10)                           Yes    Yes     Yes
ProCurve Access Point 530# show stations detail
Station     00:11:50:55:50:11                         Authenticated    Yes
Radio/WLAN  work1 (2/1)                               Associated       Yes
Last RSSI   66                                        Forwarding       n/a
Rate (Mbps) 54                                        Listen Interval  10
Transmitted (to station) packets:          0   bytes:          0
Received (from station)  packets:         13   bytes:       1374
 Station     00:15:00:47:5f:6a                         Authenticated    Yes
Radio/WLAN  SSID 10 (1/10)                            Associated       Yes
Last RSSI   -                                         Forwarding       Yes
Rate (Mbps) 54                                        Listen Interval  10
Transmitted (to station) packets:          1   bytes:        565
Received (from station)  packets:          2   bytes:       1254
ProCurve Access Point 530#
```

show supported-rate

This command displays information about supported transmission rates.

Syntax

show supported-rate

Default

N/A

Command Mode

Manager Exec

Example

```
ProCurve Access Point 530# show supported-rate
Supported data rates (Mbps).
-----------------------------
Radio 1 (802.11g): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
Radio 2 (802.11a): 6, 9, 12, 18, 24, 36, 48, 54
ProCurve Access Point 530#
```

Wireless Security Commands

The commands described in this section configure parameters for wireless security on SSID interfaces.

Command	Function	Mode	Page
security <no-security|static-wep|dynamic wep|wpa-psk|wpa-8021x>	Enables the type of security suite on a SSID interface.	IC-W-S	9-101
wep-default-key *<1/ 2/ 3/ 4>*	Defines the key index if using the static-wep security.	IC-W-S	9-103
[no] wep-key ascii	Sets the wep key to an ascii format.	IC-W-S	9-104
wep-key-length *<64/128>*	Sets the wep-key-length to either 64 or 128 bits if using the static-wep security.	IC-W-S	9-105
wep-key-*<1/ 2/ 3/ 4> <key>*	Defines the up to four security keys, if using the static-wep security.	IC-W-S	9-105
[no] open-system-authentication	Enables or disables open-system authentication for SSID association.	IC-W-S	9-106
[no] shared-key authentication	Enables or disables shared-key authentication for SSID association.	IC-W-S	9-107
[no] wpa-allowed | [no] wpa2-allowed	Enables or disables wireless stations to use the original WPA and WPA2 on this WLAN.	IC-W-S	9-107
wpa-preshared-key *<key>*	Defines a WPA preshared key.	IC-W-S	9-108
wpa-cipher-tkip	Enables TKIP for WPA on this WLAN.	IC-W-S	9-109
wpa-cipher-aes	Enables CCMP with the Advanced Encryption Algorithm (AES) for WPA on this WLAN.	IC-W-S	9-109
rsn-preauthentication	Enables WPA2 stations to pre-authenticate on this WLAN.	IC-W-S	9-110

security

This command defines the mechanisms employed by the access point for wireless security.

Syntax

security <no-security | static-wep | dynamic wep| wpa-psk| wpa-8021x>

- **no-security**- No encryption for data transfers. **This is not recommended.**
- **static-wep -** Use a Wired Equivalent Privacy static shared key.
- **dynamic wep**- Use the IEEE 802.1x port-based authentication and infrastructure.
- **wpa-psk** - Use the Wi-Fi Protected Access (WPA) and/or WPA2 with a pre-shared key.
- **wpa-8021x -**Use the Wi-Fi Protected Access (WPA) and/or WPA2 with a RADIUS server. **This is the recommended security mode.**

Default Setting

No security

Command Mode

WLAN Interface Configuration

Command Usage

- When using this command to configure WPA or 802.1X for authentication and dynamic keying, you must use the open-system argument.
- Shared key authentication can only be used when a static WEP key has been defined with the key command.
- WPA enables the access point to support different unicast encryption keys for each client. However, the global encryption key for multicast and broadcast traffic must be the same for all stations. This command can set the encryption type that is used for multicast and unicast traffic.

- WPA2 defines a transitional mode of operation for networks moving from WPA security to WPA2. WPA2 Mixed Mode allows both WPA and WPA2 stations to associate to a common SSID interface. When the encryption cipher suite is set to tkip-aes, the unicast encryption cipher (TKIP or AES-CCMP) is negotiated for each client. The access point advertises it's supported encryption ciphers in beacon frames and probe responses. WPA and WPA2 stations select the cipher they support and return the choice in the association request to the access point. For mixed-mode operation, the cipher used for broadcast frames is always TKIP. WEP encryption is not allowed.
- If any stations supported by the access point are not WPA enabled, the multicast-cipher algorithm must be set to WEP.
- When 802.1X is disabled, the access point does not support 802.1X authentication for any station. After successful 802.11 association, each client is allowed to access the network.
- When 802.1X is supported, the access point supports 802.1X authentication only for stations initiating the 802.1X authentication process. The access point does NOT initiate 802.1X authentication. For stations initiating 802.1X, only those stations successfully authenticated are allowed to access the network. For those stations not initiating 802.1X, access to the network is allowed after successful 802.11 association.
- When 802.1X is required, the access point enforces 802.1X authentication for all 802.11 associated stations. If 802.1X authentication is not initiated by the station, the access point will initiate authentication. Only those stations successfully authenticated with 802.1X are allowed to access the network.

Example

The following commands configure the access point to use the WPA-802.1X security mode, accept both the WPA and WPA2 stations, and allow pre-authentication.

Note

WPA-802.1X is the recommended security mode. The incorporation of the RADIUS Server makes it superior to the WPA-PSK security mode.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security wpa-8021x
ProCurve Access Point 530(radio1-wlan1)#wpa-allowed
ProCurve Access Point 530(radio1-wlan1)#wpa2-allowed
ProCurve Access Point 530(radio1-wlan1)#rsn-preauthentication
ProCurve Access Point 530(radio1-wlan1)#
```

wep-default-key

This command defines a Wired Equivalent Privacy (WEP) key index used for data encryption.

Syntax

wep-default-key <1 | 2 | 3 | 4>

- **<1 | 2 | 3 | 4>** - The wep key index (1-4).

Default Setting

1

Command Mode

WLAN Interface Configuration

Command Usage

- Up to four WEP keys can be defined on each BSS, each identified by a key index number.
- A SSID can use any or all of its 4 WEP keys, thus one SSID can't prevent another SSID from using any WEP keys.
- To enable WEP encryption, first use the **security** command before configuring a WEP key with this command.
- When WEP is enabled, all wireless stations must be configured with the same shared key to communicate with the access point’s SSID interface.
- When using IEEE 802.1X, the access point uses a dynamic WEP keys to encrypt data sent to 802.1X-enabled stations. However, because the access point sends the WEP keys during the 802.1X authentication process, these keys do not have to appear in the client’s WEP key list.

Example

The following example shows how to configure a WLAN to use static WEP keys for authentication and encryption.

These commands enable security and establish the transfer key index (set to 4).

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#security static-wep
ProCurve Access Point 530(radio1-wlan1)#wep-key-4
ProCurve Access Point 530(radio1-wlan1)#
```

wep-key-ascii

This command sets the WEP key type to ASCII when using static-wep security. The no version of the command sets the key type to hexadecimal.

Syntax

wep-key-ascii
no wep-key-ascii

Default Setting

Enabled

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530(radio1-wlan1)#wep-key-ascii
ProCurve Access Point 530(radio1-wlan1)#
```

wep-key-length

This command sets the WEP key length when using static-wep security.

Syntax

wep-key-length <64|128>

- **64 -** The 64 bit wep key length (with initializing vector, otherwise it is 40 bits).
- **128** - The 128 bit wep key length (with initializing vector, otherwise it is 104 bits).

Default Setting

128

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530(radio1-wlan1)#wep-key-length 64
ProCurve Access Point 530(radio1-wlan1)#
```

wep-key

This command defines the wep-keys used for static-wep security.

Syntax

wep-key <1 | 2 | 3 | 4> *<key>*

- **<1|2|3|4>** - Set the first, second, third, and fourth wep keys used with static-wep security (1-4).
- ***key*** - Sets the character string for security. The number of characters depend on the number of characters required for each WEP key depends on the Key Length and Key Type settings:
  - – If Key Length is 40 bits and the Key Type is "ASCII", then each WEP key must be five (5) characters long.
  - – If Key Length is 40 bits and Key Type is "Hex", then each WEP key must be 10 characters long.
  - – If Key Length is 104 bits and Key Type is "ASCII", then each WEP Key must be 13 characters long.
  - – If Key Length is 104 bits and Key Type is "Hex", then each WEP Key must be 26 characters long.

Default Setting

None

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530(radio1-wlan1)#wep-key-ascii
ProCurve Access Point 530(radio1-wlan1)#wep-key-length 64
ProCurve Access Point 530(radio1-wlan1)#wep-key-1 abcde
ProCurve Access Point 530(radio1-wlan1)#wep-key-2 fghi
ProCurve Access Point 530(radio1-wlan1)#wep-key-3 klmn
ProCurve Access Point 530(radio1-wlan1)#wep-key-4 opqr
ProCurve Access Point 530(radio1-wlan1)#
```

open-system-auth

This command enables Open System authentication for associating with this WLAN. The no version of the command disables Open System authentication.

Syntax

open-system-auth
no open-system-auth

Default Setting

Enabled

Command Mode

WLAN Interface Configuration

Command Usage

- Supported authentications are: open system, shared key, or both.

Example

```
ProCurve Access Point 530(radio1-wlan1)#open-system-auth
ProCurve Access Point 530(radio1-wlan1)#
```

shared-key-auth

This command enables shared-key authentication for associating with this WLAN. The no version of the command disables shared-key authentication.

Syntax

shared-key-auth
no shared-key-auth

Default Setting

Disabled

Command Mode

WLAN Interface Configuration

Command Usage

- Supported authentications are: open system, shared key, or both.

Example

```
ProCurve Access Point 530(radio1-wlan1)#shared-key-auth
ProCurve Access Point 530(radio1-wlan1)#
```

wpa-allowed | wpa2-allowed

Enables wireless stations to use the original WPA or WPA2 on this WLAN. The no version of these commands disables stations from being able to use the original WPA or WPA2 on this WLAN.

Syntax

wpa-allowed | wpa2-allowed
no wpa-allowed | no wpa2-allowed

Default Setting

Both enabled.

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530(radio1-wlan1)#wpa-allowed
ProCurve Access Point 530(radio1-wlan1)#wpa2-allowed
ProCurve Access Point 530(radio1-wlan1)#
```

wpa-pre-shared-key

This command defines a Wi-Fi Protected Access (WPA) pre-shared key when using WPA security.

Syntax

wpa-pre-shared-key <*key*>

- ***key*** - The key string must be a string of characters between 8 and 63.

Default Setting

None

Command Mode

WLAN Interface Configuration

Command Usage

- If WPA is used in pre-shared key mode, all wireless stations must be configured with the same pre-shared key to communicate with the access point.
- Shared secret keys can include spaces and special characters if the key is placed inside quotation marks (“goodsecret !”). If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# radio 1
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)#wpa-pre-shared-key
agoodsecret

ProCurve Access Point 530(radio1-wlan1)#
```

wpa-cipher-tkip

This command enables Temporal Key Integrity Protocol for WPA on this WLAN. The no command disables TKIP for WPA on this WLAN.

Syntax

wpa-cipher-tkip
no wpa-cipher-tkip

Default Setting

Enabled. This is the default CIPHER protocol.

Command Mode

WLAN Interface Configuration

Command Usage

- This is one of the authentication options required to establish proper WPA-PSK or WPA-802.1x security.
- When both TKIP and CCMP authentication methods are set, both TKIP and AES stations can associate with the access point. WPA stations must have either a valid TKIP or AES Key to communicate.

Example

```
ProCurve Access Point 530(radio1-wlan1)#wpa-cipher-tkip
ProCurve Access Point 530(radio1-wlan1)#
```

wpa-cipher-aes

This command enables Counter mode/CBC-MAC Protocol (CCMP) with the Advanced Encryption Standard (AES) for WPA on this WLAN. The no version of the command disables CCMP/AES for WPA on this WLAN.

Syntax

wpa-cipher-aes
no wpa-cipher-aes

Default Setting

Disabled

Command Mode

WLAN Interface Configuration

Command Usage

- This is one of the authentication options required to establish proper WPA-PSK or WPA-802.1x security.
- When both TKIP and CCMP authentication methods are set, both TKIP and AES stations can associate with the access point. WPA stations must have either a valid TKIP or AES Key to communicate.

Example

```
ProCurve Access Point 530(radio1-wlan1)#wpa-cipher-aes
ProCurve Access Point 530(radio1-wlan1)#
```

rsn-preauthentication

This command enables WPA2 stations to pre-authenticate on this WLAN. The no version of the command disables WPA2 stations from being able to pre-authenticate.

Syntax

rsn-preauthentication
no rsn-preauthentication

Default Setting

Disabled

Command Mode

WLAN Interface Configuration

Example

```
ProCurve Access Point 530(radio1-wlan1)#rsn-
preauthentication
ProCurve Access Point 530(radio1-wlan1)#
```

Neighbor AP Detection Commands

The access point can be configured to periodically scan all radio channels and find other access points within range. Alternatively, the access point can scan continuously in a dedicated mode with no stations supported. A database of nearby access points is maintained where detected APs can be identified.

Command	Function	Mode	Page
[no] ap-detection [dedicated]	Enables the periodic or dedicated detection of nearby access points	IC-R	9-111
ap-detection duration *<value>*	Sets the duration of the passive detection of nearby access points	IC-R	9-112
ap-detection expire-time *<value>*	Sets the time a dedicated AP remains on the AP list after its last received beacon.	IC-R	9-112
ap-detection interval *<value>*	Sets the wait time between scans when performing periodic (passive) scanning.	IC-R	9-113
ap-detection max-entries *<value>*	Sets the maximum amount of entries of the detected APs on the detected AP list.	IC-R	9-113
show detected-ap	Shows the current configuration for AP detection	MC	9-114

ap-detection

This command enables the background detection of nearby access points. The no command disables AP detection by this radio.

Syntax

ap-detection [dedicated]
no ap-detection

- **[dedicated]** - Dedicate this radio to be used for continuous AP detection. This radio will not be able to service wireless stations or WDS links if it is dedicated to AP-detection. The no version of this command is not available for this parameter.

Default Setting

Disabled

Command Mode

Radio Interface Configuration

Command Usage

- While the access point scans a channel for neighbor APs, wireless stations will not be able to connect to the access point. Therefore, frequent scanning or scans of a long duration will degrade the access point's performance. If more extensive scanning is required, use the dedicated scanning mode.

Example

```
ProCurve Access Point 530(radio1)#ap-detection dedicated
ProCurve Access Point 530(radio1)#
```

ap-detection duration

This command sets the duration of channel scanning for the background scanning detection of nearby access points.

Syntax

ap-detection duration *<value>*

- ***value*** - The length of time in milliseconds. Range: 5-30.

Default Setting

30 ms

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#ap-detection duration 10
ProCurve Access Point 530(radio1)#
```

ap-detection expire-time

This command sets the amount of time that a dedicated AP will remain on the detected AP-list after its last beacon is received.

Syntax

ap-detection expire-time *<value>*

- ***value*** - The length of time in seconds. Range: 1-604800.

Default Setting

3600 s

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#ap-detection expire-time
15
ProCurve Access Point 530(radio1)#
```

ap-detection interval

This command sets the amount of time to wait between scans when performing periodic (passive) scanning.

Syntax

ap-detection interval *<value>*

- ***value*** - The length of time in seconds between scans. Range: 10-3600.

Default Setting

10 s

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#ap-detection interval 50
ProCurve Access Point 530(radio1)#
```

ap-detection max-entries

This command sets the maximum amount of AP entries to be saved to the detected AP list.

Syntax

ap-detection max-entries*<value>*

- ***value*** - The maximum size of the AP list. Range: 1-255.

Default Setting

255

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#ap-detection max-entries
30
ProCurve Access Point 530(radio1)#
```

show detected-ap

This command displays the current AP detection configuration.

Syntax

show detected-ap

Default Setting

N/A

Command Mode

Manager Exec

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#show detected-ap
Neighboring AP detection status:
Radio 1 AP detection: Enabled
Radio 2 AP detection: Enabled

Neighboring APs:
BSSID              SSID            Sec  Chan  Type
------------------------------------------------------------
00:14:02:a0:4F:bc   SSID1          none   3    AP
00:14:03:a2:4F:de   SSID2          wpa    3    AP


ProCurve Access Point 530#
```

VLAN Commands

The VLAN commands supported by the access point are listed below.

Command	Function	Mode	Page
vlan	Configures the default VLAN for an SSID interface.	IC-R-WLAN	9-116
[no] untagged-vlan *<vid>*	Configure the global untagged VLAN ID for the AP. The no version of the command sets any untagged VLAN to become tagged.	GC	9-117
management-vlan *<vid>*	Configure the VLAN ID for the management interfaces (Web UI, SNMP, Telnet, etc.).	MC	9-117

vlan

This command configures the static VLAN-related settings for the ssid.

Syntax

vlan

Default Setting

None (Range: 1-4094)

Command Mode

WLAN Interface Configuration

Command Usage

- When dynamic VLANs are enabled on the access point, a VLAN ID (a number between 1 and 4094) can be assigned to each client after successful authentication using IEEE 802.1X and a central RADIUS server. If a user does not have a configured VLAN ID, the access point assigns the user to the default VLAN ID (a number between 1 and 4094) of the associated SSID interface.

Example

```
ProCurve Access Point 530(radio1-wlan1)#vlan 3
ProCurve Access Point 530(radio1-wlan1)#
```

untagged-vlan

This untagged-vlan command sets the specified vlan number to be treated as untagged by the AP, device-wide (globally). The no version of the command sets any untagged VLAN to become tagged.

Syntax

untagged-vlan ***<vid>***
no untagged-vlan

- ***vid***- The identifier must be a number between 1 and 4094.

Default Setting

vlan-1 untagged

Command Mode

Ethernet Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface ethernet
ProCurve Access Point 530(ethernet)# untagged-vlan 9
ProCurve Access Point 530(ethernet)#
```

management-vlan

This command configures the VLAN ID for the management interfaces (Web UI, SNMP, Telnet, etc.). The management-vlan is for the "remote" or "network" management of the AP.

Syntax

management-vlan ***<vid>***

- ***vid***- The VLAN identifier to use for management.

Default Setting

1

Command Mode

Ethernet Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface ethernet
ProCurve Access Point 530(ethernet)# management-vlan 9
ProCurve Access Point 530(ethernet)#
```

QoS Commands

The QoS commands supported by the access point are listed below.

CAUTION

The default WMM parameters settings are usually adequate for WMM operation. Incorrect WMM settings can adversely affect network performance. Changes to WMM parameters should be reserved for someone with an advanced knowledge of how WMM operates. For more on WMM, see the IEEE 802.11e standard.

Command	Function	Mode	Page
qos ap-params <voice|video|best-effort|background> {<[aifs <aifs>] [cwmin <swmin>] [cwmax <cwmax>] [burst <burst>]}	Configure QoS-related parameters on the device for this radio	IC-R	9-120
qos sta-params <voice|video|best-effort|background>{<[aifs <aifs>] [cwmin <swmin>] [cwmax <cwmax>] [txop-limit <txop-limit>]}	Configure QoS-related parameters on the wireless stations.	IC-R	9-122
[no] qos wmm	Enables using Wireless Multimedia Extensions on this WLAN.	IC-R	9-124
show qos	Displays details about QoS settings on the device and wireless client.	IC-R	9-125
[no] rate-limit *<rate><burst>*	Configures the maximum rate at which the access point transmits multicast and broadcast traffic.	IC-R	9-125

qos ap-params

This command configures QoS-related parameters on the device for this radio.

Syntax

qos ap-params <voice|video|best-effort|background> {<[aifs *<aifs>*] [cwmin *<cwmin>*] [cwmax *<cwmax>*] [burst *<burst>*]}

- **voice** - High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **video** - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **best effort** - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- **background** - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- **[aifs <*aifs*>] -** Arbitration Inter-Frame Spacing (AIFS) specifies a wait time in milliseconds for data frames. Valid values are: **1-255.**
- **[cwmin <*cwmin*>]** - Specifies the Minimum Contention Window QoS parameter. The value specified is the **lower** limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmin" are **1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.** The value for "cwmin" must be lower than the value for "cwmax".
- **[cwmax <*cwmax*>**] - Specifies the Maximum Contention Window QoS parameter. The value specified is the **upper** limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmax" are **1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024**. The value for "cwmax" must be higher than the value for "cwmin".
- **[burst <*burst*>]** - Specifies the Maximum Burst Length QoS parameter. This value specifies the length of time allowed for a packet burst (collection of transmitted multiple frames without header information) on a wireless network.Valid values for maximum burst length are **0.0 through 999.9**.

Defaults: See tabled output.

```
Radio 1      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
-------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0

Radio 2      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
-------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0
```

Command Mode

Radio Interface Configuration

Examples

This example sets the quality of service AIFS wait time parameter to 10 seconds on the AP EDCA medium priortiy queue.

```
ProCurve Access Point 530(radio1)#qos ap-params voice aifs
10
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service CWIM minimum and CMAX maximum contention window parameters on the AP EDCA medium priority queue. .

```
ProCurve Access Point 530(radio1)#qos ap-params video cwmin
1
ProCurve Access Point 530(radio1)#qos ap-params video cwmax
7
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service BURST parameter on the AP EDCA medium priority queue. .

```
ProCurve Access Point 530(radio1)#qos ap-params background
burst 1
ProCurve Access Point 530(radio1)#
```

qos sta-params

This command configures QoS related parameters on the device for the wireless stations.

Syntax

qos sta-params <voice|video|best-effort|background> {<[aifs *<aifs>*] [cwmin *<cwmin>*] [cwmax *<cwmax>*] [txop-limit *<txop-limit>*]}

- **voice** - High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **video** - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **best effort** - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- **background** - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- **[aifs <*aifs*>] -** Arbitration Inter-Frame Spacing (AIFS) specifies a wait time in milliseconds for data frames. Valid values are: **1-255.**
- **[cwmin <*cwmin*>]** - Specifies the Minimum Contention Window QoS parameter. The value specified is the **lower** limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmin" are **1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024.** The value for "cwmin" must be lower than the value for "cwmax".
- **[cwmax <*cwmax*>**] - Specifies the Maximum Contention Window QoS parameter. The value specified is the **upper** limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the "cwmax" are **1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024**. The value for "cwmax" must be higher than the value for "cwmin".
- **[txop-limit <*txop-limit*]** - Specifies the Transmission Opportunity Limit QoS parameter. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network. Valid values are **0.0 through 65535.**

Default Setting: See tabled output.

```
Radio 1       Adaptive Inter-    Contention    Contention    Maximum Burst
Queue         Frame Space        Min. Window   Max. Window   Length
------------------------------------------------------------------------------
Voice          1                  3             7             47
Video          1                  7             15            94
Best-Effort    3                  15            63            0
Background     7                  15            1023          0

Radio 2       Adaptive Inter-    Contention    Contention    Maximum Burst
Queue         Frame Space        Min. Window   Max. Window   Length
------------------------------------------------------------------------------
Voice          1                  3             7             47
Video          1                  7             15            94
Best-Effort    3                  15            63            0
Background     7                  15            1023          0
```

Command Mode

Radio Interface Configuration

Examples

This example sets the quality of service AIFS wait time parameter to 10 seconds on the Station EDCA high priortiy queue.

```
ProCurve Access Point 530(radio1)#qos sta-params voice aifs
10
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service CWMIN minimum and CWMAX maximum contention window parameters on the Standard EDCA high priority queue. .

```
ProCurve Access Point 530(radio1)#qos sta-params video cwmin
1
ProCurve Access Point 530(radio1)#qos sta-params video cwmax
15
ProCurve Access Point 530(radio1)#
```

This example sets the quality of service TXOP-LIMIT (transmission opportunity limit) parameter on the Standard EDCA high priority queue. .

```
ProCurve Access Point 530(radio1)#qos sta-params background
txop-limit 1
ProCurve Access Point 530(radio1)#
```

qos wmm

This command enables using Wireless Multimedia Extensions on this WLAN. The no version of this command is set at the "[no] qos" and disables the quality of service on this WLAN.

Syntax

qos wmm

no qos wmm

Default Setting

Disabled

Command Mode

Radio Interface Configuration

Example .

```
ProCurve Access Point 530(radio1)#qos wmm
ProCurve Access Point 530(radio1)#
```

show qos

This command displays details about QoS settings on the device.

Syntax

show qos [ap-params |sta-params]

- **ap-params**- Displays detailed information about QoS settings on the device.
- **sta-params**- Display detailed information about QoS settings on the wireless client.

Default Setting

None

Command Mode

Radio Interface Configuration

Example: tx-queue .

```
ProCurve Access Point 530(radio1)# show qos ap-params
Transmission Queue QoS Settings for the Access Point:
-------------------------------------------------------------------------------
Radio 1      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
-------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0

Radio 2      Adaptive Inter-   Contention    Contention    Maximum Burst
Queue        Frame Space       Min. Window   Max. Window   Length
-------------------------------------------------------------------------------
Voice         1                 3             7             1.5
Video         1                 7             15            3.0
Best-Effort   3                 15            63            0
Background    7                 15            1023          0

ProCurve Access Point 530(radio1)#
```

Example: wme-queue .

```
ProCurve Access Point 530(radio1)# show qos sta-params
Transmission queue QoS settings for wireless stations:
Radio 1      Adaptive Inter-   Contention    Contention    Transmission
Queue        Frame Space       Min. Window   Max. Window   Opportunity Limit
-------------------------------------------------------------------------------
Voice         2                 3             7             47
Video         2                 7             15            94
Best-Effort   3                 15            1023          0
Background    7                 15            1023          0

Radio 2      Adaptive Inter-   Contention    Contention    Transmission
Queue        Frame Space       Min. Window   Max. Window   Opportunity Limit
-------------------------------------------------------------------------------
Voice         2                 3             7             47
Video         2                 7             15            94
Best-Effort   3                 15            1023          0
Background    7                 15            1023          0

ProCurve Access Point 530(radio1)
```

rate-limit

This command configures the maximum rate at which the access point transmits multicast and broadcast traffic. The no version of the command disables rate-limiting on the radio.

Syntax

rate-limit <*rate*> <*burst*>

no rate-limit

- ***rate-*** The broadcast/multicast rate limit value in packets per second. The no version is disabled for this parameter. Valid values are 0.0 through 999.9.
- ***burst-*** The broadcast/multicast rate burst value in packets per second. This value specifies the length of time allowed for a packet burst. Valid values are 0.0 through 999.9.

Default Setting

Disabled. Rate-limit rate is 50, Rate-limit burst is 75.

Command Mode

Radio Interface Configuration

Example

```
ProCurve Access Point 530(radio1)#rate-limit 2 5
ProCurve Access Point 530(ratio1)#
```

Related Commands

beacon-interval (page 9-84)

Wireless Distribution System (WDS)

The WDS commands supported by the access point are listed below.

Command	Function	Mode	Page
description	Establishes the WDS link description	IC-WDS	9-129
disable	Disables the WDS link.	IC-WDS	9-129
enable	Establishes the WDS link.	IC-WDS	9-129
radio-used	Sets the radio that will be used by this WDS link.	IC-WDS	9-130
remote-mac	Sets the mac address for the remote connection to the access point.	IC-WDS	9-131
show wds	Displays WDS link information.	IC-WDS	9-131
wds-ssid <ssid>	Establishes the SSID name for this WDS link.	IC-WDS	9-130
wep-key	Sets wds security key for the wireless connection.	IC-WDS	9-132
wep-key-ascii	Sets wds security to ascii format.	IC-WDS	9-133
wep-key-length	Sets wds security key length.	IC-WDS	9-133
wpa-pre-shared-key	Sets wds pre-shared key.	IC-WDS	9-134

description (wds)

This command creates a human-readable string description of this WDS.

Syntax

description *<string>*

- ***string-*** Description of the WDS.

Default Setting

N/A

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface wds1
ProCurve Access Point 530(wds1)# description WDSEXAMPLE
ProCurve Access Point 530(wds1)#
```

disable (wds)

This command disables the WDS link.

Syntax

disable

Default Setting

Disabled

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface wds1
ProCurve Access Point 530(wds1)# disable
ProCurve Access Point 530(wds1)#
```

enable (wds)

This command enables the WDS link.

Syntax

enable

Default Setting

Disabled

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface wds1
ProCurve Access Point 530(wds1)# enable
ProCurve Access Point 530(wds1)#
```

wds-ssid

This command sets the WDS SSID string for this WDS link. This command is only used for the wpa-psk security mode only.

Syntax

wds-ssid <ssid>

- **ssid-** The text string that specifies the SSID of the interface. (1 - 32 alphanumeric characters).

  Note: When using WPA over WDS, an SSID is required and must match the SSID on the WDS partner access point for successful operation.

Default Setting

WDS SSID X, where X is the index of the WDS interface.

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#interface wds1
ProCurve Access Point 530(wds1)#wds-ssid marge
ProCurve Access Point 530(wds1)#
```

radio-used

This command sets the radio used with this WDS link.

Syntax

radio-used <1 | 2>

- **1 | 2**- Specifies the radio number.

Default

2

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#radio-used 1
```

remote-mac (wds)

This command sets the remote MAC address associated with this WDS link.

Syntax

remote-mac <*mac*>

- ***mac*** - Specifies an entry in the authentication control list by MAC address. Valid format is 00:00:00:00:00:00~FF:FF:FF:FF:FF:FF.

Default

None

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#remote-mac 00:0D:9D:C6:98:7E
```

show wds

This command information about the Wireless Distribution System (WDS) settings. on the device.

Syntax

show wds <wds_name>

- **wds_name**- Displays detailed information about the specified WDS.

Default

Wireless Distribution System - Link 1

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#show wds 1
WDS #1
Description  WDSLINK
Status       Enabled            Use Radio   1
Local MAC    00:14:03:A2:4F:DE  Remote MAC 00:0D:9D:C6:98:7E
STP State    forwarding         WDS SSID    marge

Security Type  no-security (from WLAN 1)      WEP Key Type
hex
WEP Key        not set                        WEP Key Size
128bit
WPA Key        goodsecret

Bytes Rx             0            Bytes Tx              0
Packets Rx           0            Packets Tx            0
Compressed Rx        0            Compressed Tx         0
Mcast packets Rx     0            Carrier errors Tx     0
Dropped Rx packets   0            Dropped Tx packets    0
FIFO overflows Rx    0            FIFO overflows Tx     0
Frame errors Rx      0            Packet collisions Tx  0
Total Rx errors      0            Total Tx errors       0

ProCurve Access Point 530(wds1)#
```

wep-key (wds)

This command defines the wep-keys used for data encryption on an WDS interface.

Syntax

wep-key *<key>*

- ***key*** - Sets the character string for security. The number of characters depend on the number of characters required for each WEP key depends on the Key Length and Key Type settings:
  - If Key Length is 40 bits and the Key Type is "ASCII", then each WEP key must be five (5) characters long.
  - If Key Length is 40 bits and Key Type is "Hex", then each WEP key must be 10 characters long.
  - If Key Length is 104 bits and Key Type is "ASCII", then each WEP Key must be 13 characters long.

- If Key Length is 104 bits and Key Type is "Hex", then each WEP Key must be 26 characters long.

Default Setting

None

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#wep-key abcde
ProCurve Access Point 530(wds1)#
```

wep-key-ascii (wds)

This command sets the WDS WEP key type to ASCII when using static-wep security. The no version of the command sets the key type to hexadecimal.

Syntax

wep-key-ascii
no wep-key-ascii

Default Setting

Enabled

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#wep-key-ascii
ProCurve Access Point 530(wds1)#
```

wep-key-length (wds)

This command sets the WDS WEP key length when using static-wep security.

Syntax

wep-key-length <64|128>

- **64 -** The 64 bit wep key length (with initializing vector, otherwise it is 40 bits).

- **128** - The 128 bit wep key length (with initializing vector, otherwise it is 104 bits).

Default Setting

128

Command Mode

WDS Interface Configuration

Example

```
ProCurve Access Point 530(wds1)#wep-key-length 64
ProCurve Access Point 530(wds1)#
```

wpa-pre-shared-key (wds)

This command defines a Wi-Fi Protected Access (WPA) personal key associated with this link.

Syntax

wpa-pre-shared-key ***<key>***

- ***key*** - The key string must be a string of characters between 8 and 63.

Default Setting

None

Command Mode

WDS Interface Configuration

Command Usage

- If WPA is used in pre-shared key mode, all wireless stations must be configured with the same pre-shared key to communicate with the access point.
- Shared secret keys can include spaces and special characters if the key is placed inside quotation marks (“goodsecret !”). If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary.

Example

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# interface wds1
ProCurve Access Point 530(wds1)#wpa-pre-shared-key talented
```

Spanning Tree Protocol (STP)

The STP commands supported by the access point are listed below.

Command	Function	Mode	Page
[no] stp [hello-time <value>] [forward-delay <value>] [priority <value>]	Sets stp parameters for this device.	GC	9-135

stp

This command configures Spanning Tree Protocol settings for the device. The no version of the command disables STP on the device.

Syntax

stp [hello-time *<value>*] [forward-delay *<value>*] [priority *<value>*]

no stp

- **hello-time *<value>*** - Specifies the STP hello time interval. (Range 1-10).
- **forward-delay *<value>*** - Specifies the STP forward delay interval. (Range 4-30)
- **priority *<value>*** - Specifies the STP bridge priority. (Range 0-65535)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.
- Do not create duplicate WDS links between the same two access points.
- If you can trace more than one path between any pair of APs going through any combination Ethernet or WDS links, you have a loop.

Example.

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# stp
ProCurve Access Point 530(config)# stp hello-time 5
ProCurve Access Point 530(config)# stp forward-delay 10
ProCurve Access Point 530(config)# stp priority 255
ProCurve Access Point 530(config)#
```

— This page is intentionally unused. —

A

File Uploads, Downloads, and Resets

Contents

Overview

You can download new access point software and upload or download configuration files. These features are useful for acquiring periodic access point software upgrades and for storing or retrieving a switch configuration.

This appendix includes the following information:

- Downloading access point software
- Transferring access point configurations

Downloading Access Point Software

The ProCurve support site periodically provides access point software updates through the ProCurve Web site (**http://www.procurve.com**). For more information, see the support and warranty booklet shipped with the access point. After you acquire a new access point software file, you can use one of the following methods for downloading the software code to the access point.

General Software Download Rules

After an access point software download, the access point will automatically reboot and implement the newly downloaded code.

Note

Downloading new software does not change the current access point configuration. The access point configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another access point of the same model. It is recommended that you save a copy of the configuration file before upgrading your access point software. See *"Transferring Configuration Files" on page A-8*, for information on saving the access point's configuration file.

Assumptions for Using TFTP, FTP, or SCP To Download Software from a Server

This procedure assumes that:

- A software file for the access point has been stored on a TFTP, FTP, or SCP server accessible to the access point. (The access point software file is typically available from the ProCurve Web site at **http://www.procurve.com**.)
- The access point is properly connected to your network and has already been configured with a compatible IP address and subnet mask.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP, FTP, or SCP server on which the access point software file has been stored.
- If VLANs are configured on the access point, determine the name of the VLAN in which the TFTP, FTP, SCP server is operating.
- Determine the name of the access point software file stored in the TFTP, FTP, or SCP server for the access point

Note

If your TFTP, FTP, or STP server is a Unix workstation, *ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the access point software filenames on the server.*

Web: TFTP, FTP, or STP Software Download to the Access Point

The Software tab enables the access point's system software to be upgraded by downloading a new file to the access point's flash memory. The new software file must be stored remotely on an FTP or TFTP server.

Note

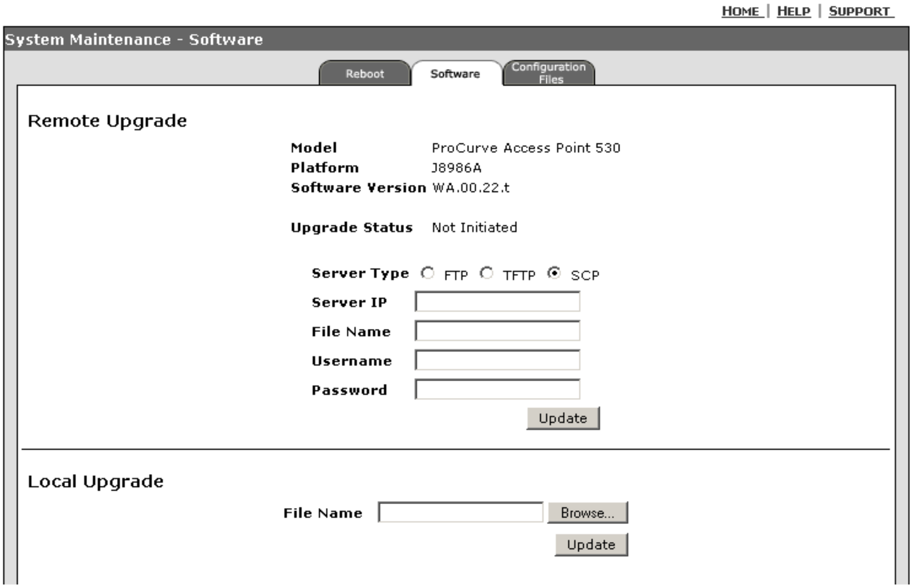
Due to the size limit of the flash memory, the access point can store only two software files. There are two images, a primary and a secondary that are automatically selected and if in the event the primary is corrupted, the secondary image is utilized as a backup.

The Web interface enables you to modify these parameters:

- **Remote Upgrade:** Parameters and actions needed to perform a remote software upgrade.
  - **Model:** Indicates the model identifier of the access point.
  - **Platform:** Indicates the platform on the access point.
  - Software Version: Indicates the current value of software on the device.
  - **Server Type:** Indicates the type of server to complete the upgrade transaction (FTP, TFTP, SCP). (Default is FTP)
  - **Direction:** Indicates whether to save the file remotely or import the file (Download-Restore; Upload-Save). (Default is Download)
  - **Server IP:** Indicates the IP address of the server.
  - **File Name:** Indicates the name of the upgrade file.
  - **Username:** Indicates the username on the server.
  - **Password:** Indicates the password on the server.
  - **[Update]:** Updates the system with the specified parameters and performs any requested actions.
- **Local Upgrade:** Parameters and actions needed to perform a local software upgrade.

- **File Name:** Specifies the name of the software file on the server.

  The new software file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **[Browse]:** Performs local system search for upgrade file.
- **[Update]:** Updates the system with the specified parameters and performs any requested actions.



System Maintenance - Software

Remote Upgrade

Model ProCurve Access Point 530
Platform J8986A
Software Version WA.00.22.t

Upgrade Status Not Initiated

Server Type ○ FTP ○ TFTP ● SCP
Server IP
File Name
Username
Password

Local Upgrade

File Name

Figure A-1. Software Tab

To Upload/Download A Remote Software File:

1. Select Management> System Maintenance > Software tab.
2. Select **FTP, TFTP, or SCP** for the Server Type option.
3. Enter **IP Address, File Name, Username, and Password** for the server details
4. Click **[Update]** to perform the operation.

To Upload a Local Software File:

1. Select Management> System Maintenance > Software tab.

2. Specify the path and file name of the software on the local computer in the **File Name** text field. You can use **[Search]** to find the software upgrade file on a local system.

3. To begin the upload of the discovered Software File, click **[Update]**. When the download is complete, restart the access point by clicking on the **[Reboot]** button. Alternatively, you can reset the access point defaults and reboot the system by clicking on the **[Reset]** button on the Reset tab. Resetting the access point is highly recommended.

CLI: Viewing Software Versions

CLI Commands Used in This Section.

Command	CLI Reference Page
show version	9-29

Using the CLI to View Software Versions. This example displays how to display the version of the software running on the device.

```
ProCurve Access Point 530# show version
Image Software Version  WA.01.00
Boot Software Version   WAB.01.00

ProCurve Access Point 530##
```

Transferring Configuration Files

Using the Web user interface and CLI commands described in this section, you can copy access point configuration files to and from an FTP, TFTP, or STP server.

When you copy the access point configuration file to a specified server type, that file can later be downloaded to the access point to restore the system configuration. The success of the file transfer depends on the accessibility of the specified server type and the quality of the network connection.

Web: Configuration File Upload and Download

The Configuration Files tab on the System Maintenance window enables the access point's configuration to be saved to a file on a remote FTP or TFTP server.

The Web interface enables you to modify these parameters:

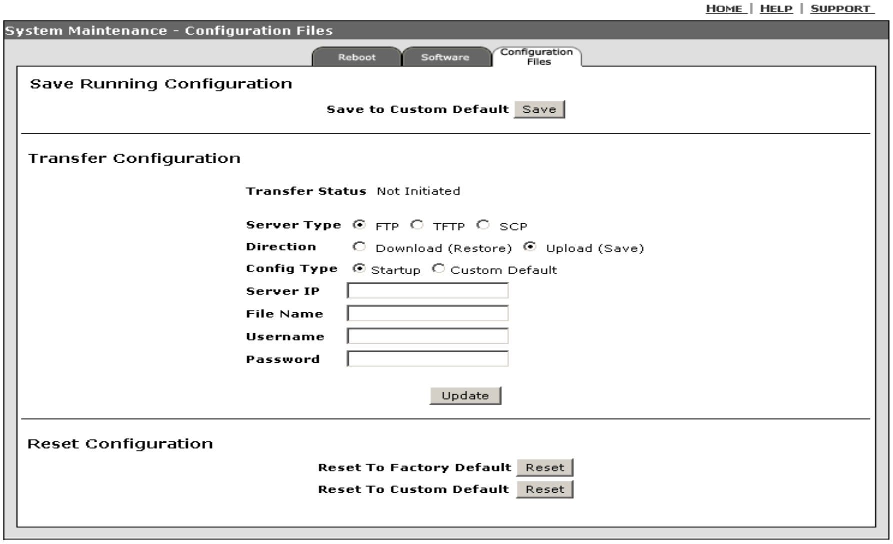
- **Save Running Configuration:** Parameters and actions needed to save a running configuration.
  - **[Save]:** Saves the current configuration as a personalized default.
- **Transfer Configuration:** Parameters and actions needed to upload or download a configuration.
  - **Server Type:** Indicates the type of server to configure (FTP, TFTP, SCP). (Default is FTP)
  - **Direction:** Indicates whether to save the file remotely or import the file (Download-Restore; Upload-Save). (Default is Download)
  - **Server IP:** Indicates the IP address of the server.
  - **File Name:** Indicates the name of the config file.

    The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

    The file name extension also needs to be specified. To avoid overwriting files on the server, it is recommended to add the ".txt" extension to the file name for readable text configuration files and the ".bin" extension for binary files.
  - **Username:** Indicates the username on the server.
  - **Password:** Indicates the password on the server.

  - **[Update]:** Updates the system with the specified parameters and performs any requested actions.

- **Reset Configuration:** Parameters and actions needed to reset a configuration.
  - **[Reset to Factory Default]:** Resets the AP to original settings.
  - **[Reset to Custom Default]:** Resets the AP to the saved custom config file.



System Maintenance - Configuration Files

Save Running Configuration

Save to Custom Default [Save]

Transfer Configuration

Transfer Status Not Initiated

Server Type ● FTP ○ TFTP ○ SCP
Direction ○ Download (Restore) ● Upload (Save)
Config Type ● Startup ○ Custom Default
Server IP
File Name
Username
Password

[Update]

Reset Configuration

Reset To Factory Default [Reset]
Reset To Custom Default [Reset]

Figure A-2. Configuration Files Tab

To Save A Running Configuration:

1. Select Management> System Maintenance > Configuration Files tab.
2. To save the current running configuration, click **[Save]** to save the file as a custom default configuration file.

To Transfer A Configuration File:

1. Select Management> System Maintenance > Configuration Files tab.
2. Select **FTP, TFTP, or SCP** for the Server Type option.
3. Select **Download or Upload** for the Direction option.
4. Enter **IP Address, File Name, Username, and Password** for the server details
5. Click **[Update]** to perform the upload or download operation.

To Reset A Configuration:

1. Select Management> System Maintenance > Configuration Files tab.
2. To reset the configuration back to the factory default configuration, click **[Reset]** on the Reset to Factory Default option.
3. To reset the configuration back to the custom default configuration, click **[Reset]** on the Reset to Custom Default option.

CLI: Performing Configuration File Commands

CLI Commands Used in This Section.

Command	CLI Reference Page
Copy Commands:	
copy <ftp | scp | tftp> <flash | startup-config> *<ip>* *<file>* [user-name *<user>* password *<pass>*]	9-44
write <memory>	9-48
copy startup-config <ftp | scp | tftp> <flash | startup-config> *<ip>* *<file>* [user-name *<user>* password *<pass>*]	9-45
copy factory-default <startup-config | custom-default>	9-46
copy running-config<startup-config | custom-default>	9-46
Erase/Reset Commands:	
erase	9-47
reload	9-13
Show Commands:	
write <terminal>	9-48
show config	9-49
show custom-default	9-51
show running-config	9-52

Using the CLI to Copy and Reset Config Files. This example displays how to reset the configuration file back to the factory-default configuration on the device.

```
ProCurve Access Point 530#copy factory-default startup-
config
ProCurve Access Point 530#
```

This example shows how to reset by ‘erasing’ the specified configuration file stored on the device.

```
ProCurve Access Point 530#erase custom-default

ProCurve Access Point 530#
```

This example displays how to copy the running configuration to a startup configuration file on the device.

```
ProCurve Access Point 530#copy running-default startup-
config
ProCurve Access Point 530#
```

This example displays how to ‘write’ the running configuration to a startup configuration file on the device.

```
ProCurve Access Point 530#write memory
ProCurve Access Point 530#
```

Using the CLI to Copy Config files to a Remote Server. This example displays how to copy the startup configuration from the device to a remote server (TFTP). If using this command for a FTP or STP server, you will need to include the username and password for the server.

```
ProCurve Access Point 530#copy startup-config tftp
192.168.1.52 copystart
ProCurve Access Point 530#
```

Using the CLI to Copy Data From a Remote Server to the Device. This example displays how to copy data from a remote server (FTP) to this device. If using this command for a FTP or STP server, you will need to include the username and password for the server. The TFTP server does not need a password or username..

```
ProCurve Access Point 530#copy ftp flash 192.168.1.52
copystart user-name chris password open
ProCurve Access Point 530#
```

Using the CLI to View Config Files. This example shows how to view the running configuration of the device. This is an alias for the "show running-config" command.

```
ProCurve Access Point 530#write terminal
------------------------------------------------------------
<?xml version="1.0"?>
<config>
  <interface name="wlan0wds1">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 2</
description>
  </interface>
 --MORE-,next page: Space, next line: Enter, quit: Control-C
```

This examples shows how to view the startup configuration on the device.

```
ProCurve Access Point 530#show config
------------------------------------------------------------
<?xml version="1.0"?>
<config>
  <interface name="wlan0wds1">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 2</
description>
  </interface>
 --MORE-,next page: Space, next line: Enter, quit: Control-C
```

This example displays the custom configuration file in a readable text format.

```
ProCurve Access Point 530#show custom-default
------------------------------------------------------------
<?xml version="1.0"?>
<config>
  <interface name="wlan0wds1">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 2</
description>
  </interface>
  <interface name="wlan0wds0">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 1</
description>
  </interface>
  <interface name="wlan0wds3">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 4</
description>
  </interface>
  <interface name="wlan0wds2">
    <radio>wlan0</radio>
    <type>wds</type>
    <status>down</status>
    <wep-key-length>104</wep-key-length>
    <wep-key-ascii>no</wep-key-ascii>
    <description>Wireless Distribution System - Link 3</
description>
  </interface>
 --MORE-,next page: Space, next line: Enter, quit: Control-C
```

Rebooting the Access Point

Using the Web user interface and CLI described in this section, you can reboot the access point, which cycles the system back to the last saved configuration.

Web: Rebooting the System

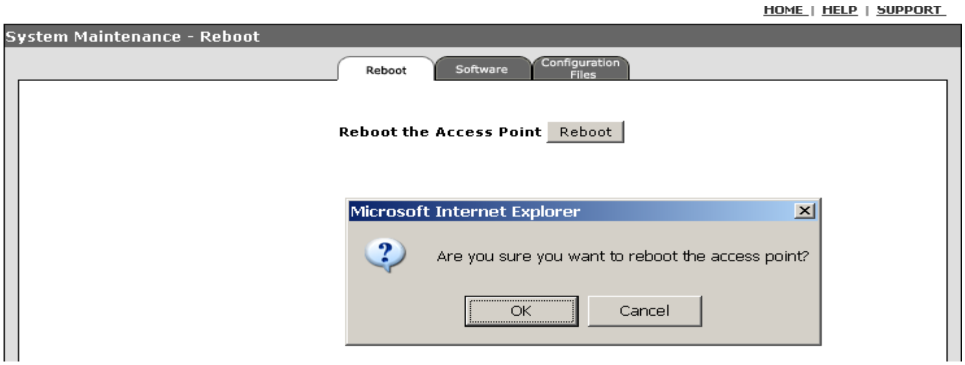
The Reboot tab on the System Maintenance window enables the access point to reboot to the last saved configuration file.

The Web interface enables you to perform this action:

- **[Reboot]:** Submits a request to reboot the access point. A system confirmation message appears and provides opportunity to cancel.

NOTE

During a reboot, connection to the AP is lost and the browser will not stay on the System Maintenance screen while the reboot takes place. Test the connection to find out when the process has completed.



Are you sure you want to reboot the access point?

Figure A-3. Reboot Tab

To Reboot the Access Point:

1. Select Management> System Maintenance > Reboot tab.
2. To initiate the reboot process, click **[Reboot]**.
3. To continue the process, select **[Okay]**.
4. To discontinue the process, select **[Cancel]**.
5. To validate the reboot process worked, test the connection through any option available (Web, Telnet, SSH).

CLI: Rebooting the System

CLI Commands Used in This Section.

Command	CLI Reference Page
reload	9-13

Using the CLI to Reboot the Access Point. This example displays how to perform a warm reboot of the access point.

NOTE

The reload command will cause a loss of connectivity for all Telnet connections and SSH connections.

.

```
ProCurve Access Point 530#reload
Device will be rebooted, do you want to continue [y/n]?y
Do you want to save the current configuration [y/n]?n
Connection to host lost.
```

Manual: Using the Reset and Clear Buttons

The Access Point unit possesses two buttons that when pressed perform reset and clear operations.

Caution

The Reset button is provided for your convenience, but if you are concerned with the security of the access point configuration and operation, you should disable it.

The two push buttons located on the back panel of the access point enables you to perform these actions:

- **[Reset]:** Reboots the AP.
  - Use a pointed object to press the reset button. Once pressed, all LEDs shut off within one second. The LED shutdown is followed by all LEDs flashing rapidly (about 10 times/second). If you release the reset button while the LEDs are still flashing, then the AP is rebooted. Please note that this function can be disabled by the CLI or Web UI. See "Disabling the Access Point Push Buttons" on page A-17.

- **[Clear]:** Resets the password.
  - Use a pointed object to press the clear button. Once pressed, all LEDs shut off within one second. The LED shutdown is followed by all LEDs flashing rapidly (about 10 times/second). If you release the clear button while the LEDs are still flashing, then the password is reset. Please note that this function can be disabled by the CLI or Web UI. See "Disabling the Access Point Push Buttons" on page A-17.
- **[Reset] & [Clear]:** Resets the configuration.
  - Resets the configuration back to custom defaults.
    i. Press the reset and clear buttons simultaneously.
    ii. Once the LEDs shut off, release the reset button. The LEDs will then flash about once per second.
    iii. While the LEDs are still flashing, release the clear button. The configuration sets to the custom default settings and the AP is rebooted.

NOTE

Please note that only the reset function can be disabled by the CLI or Web UI. See "Disabling the Access Point Push Buttons" on page A-17.

  - Resets the configuration back to factory defaults.
    i. Press the reset and clear buttons simultaneously.
    ii. Once the LEDs shut off, release the reset button. The LEDs will then flash about once per second.
    iii. Push the reset button (while continuing to hold the clear button). After about one second, all LEDs will flash rapidly (about 10 times/second) .
    iv. When the clear button is released, the AP will then be reset to factory defaults and reboot.

NOTE

Please note that this function can be disabled by the CLI or Web UI. See "Disabling the Access Point Push Buttons" on page A-17.

Disabling the Access Point Push Buttons

Using the Web user interface and CLI described in this section, you can disable the ability to use the push buttons on the back panel of the access point.

Web: Disabling the Push Buttons

The Remote Access tab on the Management window allows disabling of the push buttons on the access point. For details on configuring other management controls see, "Setting Management Access Controls" on page 5-8.

The Web interface enables you to perform this action:

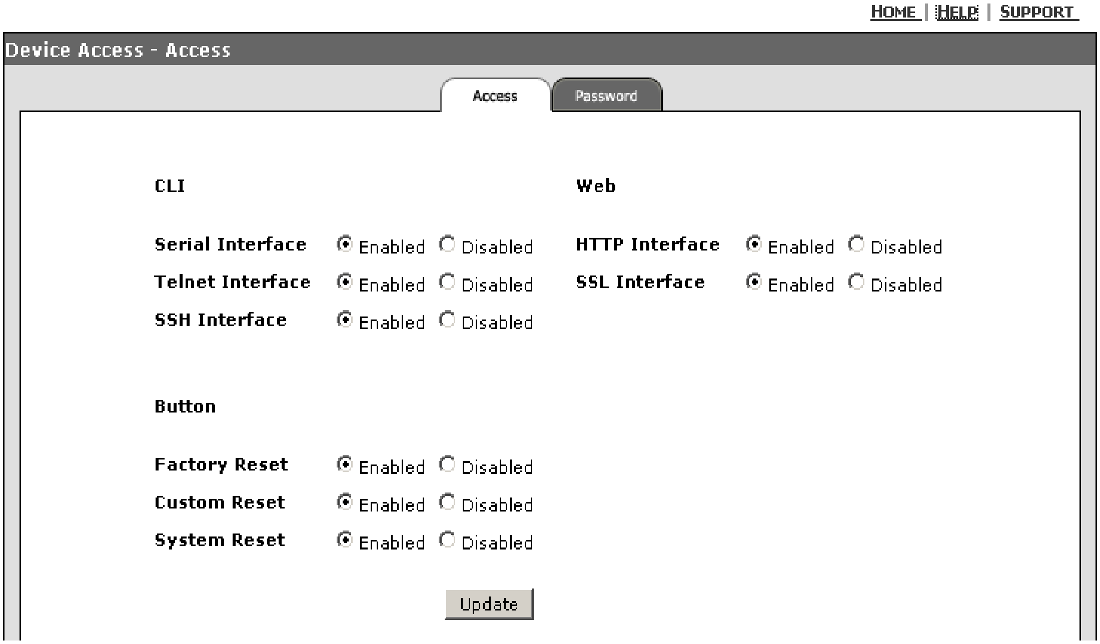
- **Factory Reset**: Enables or disables button control access (back panel of the access point) to a factory default file reset. (Default is Disabled)

NOTE

You can not disable the factory reset if you already have disabled the Serial Interface. See "Setting Management Access Controls" on page 5-8.

- **Custom Reset**: Enables or disables button control access (back panel of the access point) to a custom config file reset.(Default is Disabled)
- **System Reset**: Enables or disables button control access (back panel of the access point) to a system reset. (Default is Disabled)

- **[Update]:** Updates the management and button control modifications.



CLI

Serial Interface ● Enabled ○ Disabled

Telnet Interface ● Enabled ○ Disabled

SSH Interface ● Enabled ○ Disabled

Web

HTTP Interface ● Enabled ○ Disabled

SSL Interface ● Enabled ○ Disabled

Button

Factory Reset ● Enabled ○ Disabled

Custom Reset ● Enabled ○ Disabled

System Reset ● Enabled ○ Disabled

Figure A-4. Remote Access Tab - Button Access

To Disable the Access Point Push Buttons:

1. Select Management> Device Access > Remote tab.
2. To shut down the push button(s) on the back panel of the access point controlling the password reset capability, select **Disabled** for the Password Reset option.
3. To shut down the push button(s) on the back panel of the access point controlling the factory default file reset capability, select **Disabled** for the Factory Reset option.
4. To shut down the push button(s) on the back panel of the access point controlling the customer file reset capability, select **Disabled** for the Customer Reset option.
5. To shut down the push button(s) on the back panel of the access point controlling the system reset capability, select **Disabled** for the System Reset option.
6. Click **[Update]** to set the push button parameters.

CLI: Disabling the Access Point Buttons

CLI Commands Used in This Section.

Command	CLI Reference Page
[no] **buttons** <custom-reset | factory-reset | password-reset | system-reset>	9-21
show buttons	9-21

Using the CLI to Disable the Reset and Clear Buttons On the Access Point. This example displays how to disable the ability to manually use the reset and clear push buttons on the back panel of the device.

.

```
ProCurve Access Point 530#configure
ProCurve Access Point 530(config)#no buttons custom-reset
ProCurve Access Point 530(config)#no buttons factory-reset
ProCurve Access Point 530(config)#no buttons password-reset
ProCurve Access Point 530(config)#no buttons system-reset
ProCurve Access Point 530(config)#
```

Using the CLI to View the Reset and Clear Buttons Status. This example displays how to view the push button status.

.

```
ProCurve Access Point 530(config)# show buttons
------------------------------------------------------------
Custom Reset             Disabled
Factory Reset            Disabled
Password Reset           Disabled
System Reset             Disabled

ProCurve Access Point 530(config)#
```

— This page is intentionally unused. —

B

Defaults

Contents

Overview

This section features useful tables detailing the defaults of the commands configured on the access point.

Note

The following command groupings are not included in this default appendix as they are not applicable (Show CLI, General, Flash/File,

This appendix follows the syntax grouping structure in the Chapter 9 reference CLI section and includes the following information:

- System Management
- System Logging Commands
- System Clock Commands
- Network Management Application Commands
- RADIUS Accounting/Authentication Commands
- RADIUS Users
- MAC Address Authentication
- Filtering Commands
- Ethernet Interface Commands
- Wireless Interface
- Wireless Security
- Neighbor AP-Detection
- Vlan Commands
- QoS
- WDS

System Management Commands

Command	Default Settings	Mode	Page
country *<country code>*	For NA units, preset to US	GC	9-17
hostname *<hostname>*	ProCurve-AP-530	GC	9-19
password manager *<password>*	admin	MC	9-20
[no] buttons	Enabled	MC	9-21
[no] cli-confirmation	Enabled	MC	9-22
[no] console	Enabled	MC	9-22
[no] telnet	Enabled	MC	9-23
[no] ssh	Enabled	MC	9-24
[no] web-management	Enabled	MC	9-24

System Logging Commands

Command	Default Setting	Mode	Page
[no] logging *<syslog_host> [syslog_port]*	Disabled	GC	9-31

System Clock Commands.

Command	Default Setting	Mode	Page
sntp *<server>*	None. GUI is disabled. NOTE: The GUI System Uptime parameter displays the Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude	GC	9-34

Network Management Application Commands

Command	Default Settings	Mode	Page
[no] snmp-server *<comm>* restricted | unrestricted	Restricted community with a public access default.	GC	9-36
snmp-server contact*<contact>*	Contact	GC	9-37
[no] snmp-server host *<host><comm>*	Host Address: None Community String: public	GC	9-38
snmp-server port *<port>*	By default an SNMP agent only listens to requests from port 161. However, you can configure this so the agent listens to requests on another port.	GC	9-39
snmp-server location *<location>*	None	GC	9-39
[no] lldp	Enabled	GC	9-41

RADIUS Accounting/Authentication.

Command	Default Settings	Mode	Page
[no] radius-accounting	Disabled	GC	9-53
[no] radius failover-to-local | retransmit	Disabled, retransmit value is 3.	GC	9-54
[no] radius primary | secondary	Disabled	GC	9-55

RADIUS Users.

Command	Default Settings	Mode	Page
[no] radius-local <*username*>[disabled] | [password <*password*>] | realname <*realname*>	Ip address is 192.168.1.10. DHCP is enabled.	GC	9-57

MAC Address Authentication

Command	Default Settings	Mode	Page
[no] mac-auth-local <*name*> mac **<*mac*>**	None. GUI-MAC Authentication is disabled.	GC	9-60
[no] mac-auth-remote	None. GUI-MAC Authentication is disabled.	GC	9-61

Filtering Commands

Command	Default Settings	Mode	Page
[no] inter-station-blocking	Disabled	GC	9-63
[no] wireless-mgmt-block	Disabled.	GC & MC	9-64

Ethernet Interface Commands

Command	Default Settings	Mode	Pag e
interface <*interface*>	N/A	GC	9-66
enable	N/A	IC-E	9-67
disable	N/A	IC-E	9-67
description	None	IC-E	9-68
dns primary <*server_1*>	Disabled	GC	9-68
dns secondary <*server_2*>	Disabled	GC	9-69
[no] ip address <ip> [<mask>] <ip><bits> <dhcp>	IP address: 192.168.1.1 Netmask: 255.255.255.0	IC-E	9-70

Wireless Interface Commands

Command	Default Settings	Mode	Page
radio	None	GC	9-77
ssid	SSID 1 (1-16)	IC-W	9-78
description	Radio: Radio 1 - WLAN 1 SSID: SSID 1	IC-W	9-79
closed-system	Disabled	IC-W-S	9-79
mode<*value*>	g	IC-W	9-80
antenna <external | internal>	Internal	IC-W	9-81
antenna mode<diversity | single>	Diversity	IC-W	9-81
basic-rate<*value*>	Radio 1: 1,2,5.5, and 11 Mbps for g mode Radio 2: 2, 6, 12, and 24 Mbps for a mode	IC-W	9-82
supported-rate<*value*>	(Options:1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 54 Mbps)	IC-W	9-83
channel-policy <static [CHANNEL] | auto>	Auto	IC-W	9-83

Command	Default Settings	Mode	Page
beacon-interval *<interval>*	100. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).	IC-W	9-84
dtim-period	2	IC-W	9-85
max-stations	256	IC-R	9-86
preamble	long	IC-R	9-86
protected mode	Enabled	IC-R	9-87
fragmentation-thresh	2346 (This effectively disables fragmentation)	IC-W	9-87
inactivity-timeout	1800	IC-R	9-88
slot-time	short	IC-W	9-89
rts-threshold	2347	IC-W	9-89
tx-power-reduction	0 in dB	IC-W	9-90

Wireless Security Commands

Command	Default Settings	Mode	Page
security <no-security|static-wep|dynamic wep|wpa-psk|wpa-8021x>	no-security	IC-W-S	9-101
wep-default-key *<1/ 2/ 3/ 4>*	1	IC-W-S	9-103
[no] wep-key ascii	Enabled	IC-W-S	9-104
wep-key-length *<64/128>*	128	IC-W-S	9-105
wep-key-*<1/ 2/ 3/ 4> <key>*	None	IC-W-S	9-105
[no] open-system-auth	Enabled	IC-W-S	9-106
[no] shared-key auth	Disabled	IC-W-S	9-107
[no] wpa-allowed | [no] wpa2-allowed	Both Enabled	IC-W-S	9-107
wpa-pre-shared-key *<key>*	None	IC-W-S	9-108
wpa-cipher-tkip	Enabled. This is the default CIPHER protocol.	IC-W-S	9-109
wpa-cipher-aes	Disabled	IC-W-S	9-109
rsn-preauthentication	Disabled	IC-W-S	9-110

Neighbor AP Detection Commands

Command	Default Settings	Mode	Page
[no] ap-detection	Disabled	IC-R	9-111
ap-detection duration	30 milliseconds	IC-R	9-112
ap-detection expire-time	3600 seconds	IC-R	9-112
ap-detection interval	10 seconds	IC-R	9-113
ap-detection max-entries	255	IC-R	9-113

VLAN Commands

Command	Default Settings	Mode	Page
[no] vlan	None	IC-W-S	9-116
[no] untagged-vlan *<vid>*	1	GC	9-117
management-vlan *<vid>* [tagged | untagged]	1	MC	9-117

QoS Commands

Command	Default Settings	Mode	Page
qos ap-params	Radio 1 Adap Inter- Content Content Max Burst Queue Frame Space Min. Window Max. Window Length -- Voice 1 3 7 1.5 Video 1 7 15 3.0 Best-Eff 3 15 63 0 Background 7 15 1023 0 Radio 2 Adap Inter- Content Content Max Burst Queue Frame Space Min. Window Max. Window Length -- Voice 1 3 7 1.5 Video 1 7 15 3.0 Best-Eff 3 15 63 0 Background 7 15 1023 0	IC-W-S	9-120
qos sta-params	Radio 1 Adap Inter- Content Content Max Burst Queue Frame Space Min. Window Max. Window Length -- Voice 1 3 7 47 Video 1 7 15 394 Best-Eff 3 15 63 0 Background 7 15 1023 0 Radio 2 Adap Inter- Content Content Max Burst Queue Frame Space Min. Window Max. Window Length -- Voice 1 3 7 47 Video 1 7 15 94 Best-Eff 3 15 63 0 Background 7 15 1023 0	IC-W-S	9-122
[no] qos wmm	Disabled	IC-W-S	9-124
[no] rate-limit] *<rate><burst>*	Rate limiting is disabled. Rate-limit rate is 50, Rate-limit burst is 75.	IC-W-S	9-127

Wireless Distribution System (WDS)

Command	Default Settings	Mode	Page
description (wds)	None	IC-W-W	9-128
enable (wds)	Disabled	IC-W-W	9-129
wds-ssid	WDS SSID X, where X is the index of the WDS interface.	IC-W-W	9-130
radio-used	2	IC-W-W	9-130
remote-mac	None	IC-W-W	9-131
wep-key (wds)	None	IC-W-W	9-132
wep-key-ascii (wds)	Enabled	IC-W-W	9-133
wep-key-length (wds)	128	IC-W-W	9-133
wpa-pre-shared-key (wds)	None	IC-W-W	9-134

C

Open Source Licenses

Contents

Overview

This appendix includes the following information:

- Open Source licenses

GPL2 (GNU General Public License, v.2)

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that

distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GPL + Linking Exception

“GPL2 (GNU General Public License, v.2)” plus an exception permitting linking the library with other software.

ClearSilver

Neotonic ClearSilver is available under the following license, derived from the Apache Software License v1.1

For alternative licensing, please contact the authors at clearsilver@neotonic.com Neotonic ClearSilver Software License

Version 1.0

Copyright (c) 2001 Brandon Long and Neotonic Software Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

> "This product includes software developed by the Neotonic Software Corporation. (http://www.neotonic.com/)."
>
> Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4.The names "Neotonic" and "Neotonic ClearSilver" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact clearsilver@neotonic.com.

5.Products derived from this software may not be called "ClearSilver", nor may "ClearSilver" appear in their name, without prior written permission of Neotonic Software Corporation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NEOTONIC, INC., OR ITS CLEARSILVER CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of Neotonic Software Corporation. For more information on Neotonic Software Corporation, please see http://www.neotonic.com/.

Some of the concepts of this software are based on previous software developed by Scott Shambarger, Paul Clegg, and John Cwikla. The current authors wish to thank them for their efforts.

Dropbear License

The majority of code is written by Matt Johnston, under the following license:

=====

LibTomCrypt and LibTomMath are (c) Tom St Denis, under TDCAL (Tom Doesn't Care About Licenses) some files are from public domain sources, see libtomcrypt/legal.txt

=====

sshpty.c is taken from OpenSSH 3.5p1,
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed
under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

LGPL (GNU Lesser General Public License)

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offerwarranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be

distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

> a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source

code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or

distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that

distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the library's name and a brief idea of what it does.>Copyright (C) <year> <name of author>
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.
>
> <signature of Ty Coon>, 1 April 1990Ty Coon, President of Vice

That's all there is to it!

Intel (2)

Copyright (c) 2000-2003 Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MIT

BSD

CMU (Carnegie Mellon University)

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

> Office of Technology Transfer
> Carnegie Mellon University
> 5000 Forbes Avenue
> Pittsburgh, PA 15213-3890
> (412) 268-4387, fax: (412) 268-7395
>
> tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

> "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL

LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4.The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5.Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6.Redistributions of any form whatsoever must retain the following acknowledgment:"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement::

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Index

ProCurve Networking
HP Innovation

Technical information in this document
is subject to change without notice.

Printed in Taiwan
May 2006

Manual Part Number
5991-2193