ProCurve Wireless Edge Services zl Module and ProCurve Redundant Wireless Services zl Module

Management and Configuration Guide

August 2007
WT.01.XX and greater
This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number
5991-8626
August 2007

Applicable Products
ProCurve Wireless Edge Services zl Module (J9051A)
ProCurve Redundant Services zl Module (J9052A)

Trademark Credits
Microsoft, Windows, Windows NT, and Windows XP are U.S. 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 Acknowledgment 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.
Wireless Edge Services zl Module 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 B in this guide.
## Contents

1 Introduction

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProCurve Wireless Edge Services zl Module</td>
<td>1-1</td>
</tr>
<tr>
<td>Wireless Networks and WLANs</td>
<td>1-4</td>
</tr>
<tr>
<td>The Interface Between the Wireless and Wired Networks</td>
<td>1-5</td>
</tr>
<tr>
<td>Communicating with RPs: Radio Port VLANs</td>
<td>1-7</td>
</tr>
<tr>
<td>Communicating with the Ethernet Network: Uplink VLANs</td>
<td>1-8</td>
</tr>
<tr>
<td>Forwarding Traffic Between the Wireless Network and the Ethernet Network</td>
<td>1-12</td>
</tr>
<tr>
<td>Layer 2 and Layer 3 Operation</td>
<td>1-14</td>
</tr>
<tr>
<td>RP Operations</td>
<td>1-16</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module Operations</td>
<td>1-17</td>
</tr>
<tr>
<td>Determining the Layer 3 Services Your Wireless Edge Services zl Module Should Provide</td>
<td>1-18</td>
</tr>
<tr>
<td>Using the Same VLANs for Wireless and Wired Users</td>
<td>1-18</td>
</tr>
<tr>
<td>Reserving VLANs for Wireless Users</td>
<td>1-19</td>
</tr>
<tr>
<td>Reserving VLANs for Wireless Users in a Network</td>
<td>1-21</td>
</tr>
<tr>
<td>IP Routing</td>
<td>1-23</td>
</tr>
<tr>
<td>DHCP Services</td>
<td>1-24</td>
</tr>
<tr>
<td>Security Features</td>
<td>1-24</td>
</tr>
<tr>
<td>Authentication Options for WLANs</td>
<td>1-24</td>
</tr>
<tr>
<td>Encryption Options for WLANs</td>
<td>1-32</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>1-34</td>
</tr>
<tr>
<td>Controlling Traffic with Policies</td>
<td>1-35</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module Firewall</td>
<td>1-38</td>
</tr>
<tr>
<td>PKI and Digital Certificates</td>
<td>1-45</td>
</tr>
</tbody>
</table>
Traffic Management and QoS ........................................ 1-46
  SVP .......................................................... 1-48
  WMM .......................................................... 1-48
  WLAN Classification ........................................... 1-49
  Voice Prioritization .......................................... 1-49
  WFQ .......................................................... 1-50
Management Capabilities and sFlow ......................... 1-50
  RP Licensing .................................................. 1-50
Radio Ports ...................................................... 1-53
  802.11 Overview ............................................. 1-54
    Physical Layer Standards ................................ 1-54
    802.11 Frames ............................................. 1-56
    BSS .......................................................... 1-56
    BSSID ....................................................... 1-58
    ESS .......................................................... 1-58
    SSID Versus BSSID ....................................... 1-59
    Beaconing .................................................. 1-61
  RP Modes ..................................................... 1-62
    Master Mode .............................................. 1-62
    Detector Mode ............................................ 1-63
Configuring the ProCurve RPs ................................ 1-64
  Radio Adoption Default Configurations ................... 1-65
  Specific Radio Configurations ............................... 1-67
Communications Between an RP and the Wireless Edge
  Services zl Module: Layer 2 and Layer 3 Adoption ........ 1-68
    Managing RPs in a Self-Healing Network ............... 1-73
  802.1X Client ................................................. 1-74
  RP Deployment Requirements ................................ 1-75
    Power over Ethernet (PoE) ............................... 1-75
    Antennas ................................................... 1-75
Redundancy Groups ............................................ 1-76
  Redundant Wireless Services zl Module .................... 1-76
  Rules of Redundancy Groups ................................ 1-77
  Redundancy Group Operation Modes ......................... 1-78
2 Configuring the ProCurve Wireless Edge Services zl Module

Contents ................................................................. 2-1

Management Interfaces ............................................... 2-5

The Web Browser Interface ........................................... 2-5

  Determining the Dynamic IP Address or Assigning a Static Address ........................................... 2-6
  Accessing the Web Browser Interface ......................................... 2-9
  Logging In to the Web Browser Interface ................................ 2-11
  Overview of the Web Browser Interface .................................. 2-12
  Applying or Saving Changes ............................................. 2-12
  Logging Out or Refreshing the Screen ................................... 2-14
  Accessing the Online Help ............................................... 2-14
  Using Filtering Options .................................................. 2-16

CLI ................................................................. 2-21

  Accessing the Switch CLI Through a Serial Session .................. 2-21
  Accessing the Switch CLI Through a Telnet or SSH Session ............ 2-22
  Accessing the Wireless-Services Context ............................... 2-22
  Navigating the CLI ...................................................... 2-22
  Saving Changes to the startup-config ................................... 2-23
  CLI Commands .......................................................... 2-23

Security ................................................................. 2-24

  SSH Access .......................................................... 2-24
  HTTPS Access .......................................................... 2-24
  SNMP Support .......................................................... 2-24
Controlling Management Access to the Module ............... 2-27
   Enabling HTTP and HTTPS Access to the Module .......... 2-27
   Choosing SNMP Versions ..................................... 2-29
   Setting Up the Internal FTP Server ......................... 2-32
   Changing the Password for the Default SNMP v3 Users
      (Operator or Manager) ..................................... 2-35
   Configuring Web-Users ....................................... 2-40
Logging In to the Module as a WebUser Administrator .... 2-49
   Creating Guest Accounts on the Local RADIUS Database .... 2-50
   Viewing and Deleting Guest Accounts ..................... 2-53
   Printing Records of Guest Accounts ...................... 2-55
Radio Port Adoption ........................................... 2-57
   Network Requirements for Layer 2 Adoption ............... 2-58
      Auto-Provisioning on the Wireless Services-Enabled Switch .. 2-58
      Attaching RPs to Infrastructure Switches .................. 2-59
   Network Requirements for Layer 3 Adoption ............... 2-62
      Enabling Layer 3 Adoption Through DHCP Option 189 ..... 2-65
      Enabling Layer 3 Adoption Through DNS Lookup ......... 2-67
      Verifying Layer 3 Adoption ............................... 2-69
   Automatic or Manual Adoption of RPs ...................... 2-70
      Configuring Manual Adoption for RPs ..................... 2-72
      Controlling Which Wireless Edge Services zl Module
         Adopts Particular RPs—Adoption Preference ID .......... 2-76
   802.1X Authentication for RPs ............................... 2-78
      Configuring 802.1X Authentication for RPs ............... 2-79
System Maintenance ............................................ 2-81
   Software Images ............................................. 2-81
      Viewing the Software Images ........................... 2-82
      Selecting the Software Image That Is Used to Reboot ..... 2-83
      Changing the Image Failover Setting .................... 2-83
      Manually Updating the Software Image ................... 2-85
Configuration Files ..................................................... 2-86
  Viewing Configuration Files ...................................... 2-87
  Transferring, or Copying, Files ................................. 2-89
  Transferring Configuration Files from an FTP or TFTP
  Server to the Wireless Edge Services zl Module ............ 2-89
  Transferring Configuration Files from the Wireless
  Edge Services zl Module to Another Destination ......... 2-91
  Managing the Directory Structure and Browsing for Files 2-95
  Deleting a Configuration File ................................... 2-97
  Returning the Startup-Config File to Factory
  Default Settings .................................................... 2-98
Update Server .......................................................... 2-98
  Checking the Software Image File ............................... 2-99
  Checking the Configuration File ................................. 2-99
  Avoiding Problems in Using the Update Server ............ 2-100
  Configuring the Update Server Settings ..................... 2-104
Password Encryption ................................................... 2-105
SNMP Traps and Error Reporting ................................. 2-109
  SNMP Communities ................................................. 2-109
    Modifying SNMP v2 Communities .............................. 2-110
  SNMP Statistics .................................................... 2-111
  SNMP Traps ............................................................ 2-112
    Enabling SNMP Traps ............................................ 2-113
    Disabling SNMP Traps .......................................... 2-115
    Setting Thresholds .............................................. 2-116
    Sending Traps to an SNMP Receiver .......................... 2-117
Radio Port Licenses ..................................................... 2-122
  Installing or Uninstalling Licenses on a Wireless Edge
  Services zl Module ................................................. 2-127
    Registering on the My ProCurve Web Portal .................. 2-127
    Understanding the Numbers: IDs and Keys .................. 2-128
  Installing RP Licenses .......................................... 2-128
  Removing RP Licenses ............................................ 2-132
  Redundancy Groups and RP Licensing .......................... 2-135
Setting System Information— Name, Time, and Country Code .............. 2-136

Enabling Secure Network Time Protocol (NTP) ......................... 2-138
  Secure NTP Overview ................................... 2-138
  NTP Modes and Communications ............................ 2-139
  NTP Hierarchy ............................................ 2-139
  Secure NTP Enhancements ................................ 2-141
Configuring a Secure NTP Server ........................................... 2-142
  Configuring Secure NTP Options ............................ 2-144
  Applying ACLs to NTP Services ............................. 2-146
  Configuring Authentication for Secure NTP ..................... 2-148
  Configuring NTP Neighbors .................................. 2-152
  Configuring the Wireless Edge Services zl Module
    as a Broadcast Server .................. 2-155
Viewing NTP Associations and Status ........................... 2-158
Viewing Secure NTP Status ........................................ 2-163

Digital Certificates .................................................. 2-166
  Overview .................................................... 2-166
  Configuring Digital Certificates ............................. 2-167
  Using the Certificates Wizard ................................ 2-170
    Creating Certificates ................................... 2-171
    Uploading a Certificate to the Module .................. 2-181
    Deleting Trustpoints, Certificates, and Keys .......... 2-184
  Uploading a CRL to a Trustpoint ............................ 2-187
  Transferring Trustpoints ................................... 2-187
    Transferring Trustpoints from the Wireless Edge
      Services zl Module to a Server ...................... 2-188
    Transferring Trustpoints from a Server to the Wireless
      Edge Services zl Module ............................... 2-189
  Certificate Keys ........................................... 2-191
    Creating a Key .......................................... 2-191
    Transferring Keys ...................................... 2-193
3 Radio Port Configuration

Contents .................................................................................. 3-1
Overview .................................................................................. 3-2
Country-Code and Regulatory Procedures ............................... 3-4
Configuring Radio Settings ....................................................... 3-5
   Creating a Radio Adoption Default Configuration ............... 3-8
   Viewing and Configuring Properties .................................... 3-10
   Configuring Radio Settings .................................................. 3-12
   Setting Advanced Radio Properties .................................... 3-17
   Creating a Radio Configuration for a Particular Radio .......... 3-25
   Configuring Properties ......................................................... 3-28
   Configuring Radio Settings for a Particular Radio ............... 3-31
   Configuring Advanced Properties for a Particular Radio ...... 3-33
   Configuring Multiple Radios at Once ................................. 3-36
   Running ACS ........................................................................ 3-36
   Resetting a Radio .............................................................. 3-38
   Managing RP Radios ............................................................ 3-40
Considerations for Enabling Client Roaming ........................... 3-44
Quality of Service (QoS) on RP Radios ................................. 3-46
   WMM .............................................................................. 3-46
   SpectraLink Voice Priority (SVP) ......................................... 3-48

4 Wireless Local Area Networks (WLANs)

Contents .................................................................................. 4-1
Overview .................................................................................. 4-3
Configuration Options: Normal Versus Advanced Mode .......... 4-4
   Normal Mode Configuration ............................................... 4-4
   Why Use Normal Mode ....................................................... 4-4
   Enabling WLANs Using Normal Mode ............................... 4-5
   Enabling More Than Four WLANs Using Normal Mode ....... 4-7
Advanced Mode Configuration ........................................... 4-11
Why Use Advanced Mode ............................................. 4-12
Enabling WLANs Using Advanced Mode Configuration ........ 4-13
Using Normal and Advanced Mode Together ...................... 4-22
Changing from Advanced Mode to Normal Mode
Configuration .............................................................. 4-23

Configuring a WLAN ......................................................... 4-26
Setting Basic Configuration Options: SSID and
VLAN Interface ............................................................. 4-30
Necessary Configurations on the Wireless
Services-Enabled Switch ............................................... 4-33
Configuring Security Options .......................................... 4-33
Configuring Authentication ............................................. 4-33
Configuring Encryption .................................................. 4-47
Configuring Advanced WLAN Settings ......................... 4-62
Controlling Inter-Station Traffic ..................................... 4-63
Enabling Closed System Operations ............................... 4-65
Configuring the Inactivity Timeout ................................. 4-67
Configuring Accounting on a WLAN ......................... 4-68
Enabling Logging to a Syslog Server on a WLAN .......... 4-69
Enabling RADIUS Accounting on a WLAN ................. 4-71
Configuring Global WLAN Settings ......................... 4-75
Enabling the WLAN ....................................................... 4-76

VLAN Assignment ........................................................... 4-80
WLAN-Based VLAN Assignment ................................. 4-82
Considerations for WLAN-Based VLAN Assignment ........ 4-84
Identity-Based, or Dynamic, VLAN Assignment ............. 4-87

Traffic Management (QoS) ............................................... 4-89
SVP ................................................................. 4-90
5 Web Authentication for Mobile Users

Contents ................................................................. 5-1

Overview ................................................................. 5-2
The Web-Auth Process .................................................. 5-3
Authentication Through a RADIUS Server ......................... 5-5
Web Pages for the Login Process .................................... 5-6
Allow List ................................................................. 5-8
Creating a VLAN Interface for the Web-Auth VLAN ............. 5-9

Configuring Web-Auth .................................................. 5-10
Configuring Basic Options and Accessing the Web-Auth Screen .................................................. 5-11
Configuring Internal Web-Auth Pages ............................... 5-16
Configuring Web-Auth to an External Web Server ................ 5-24
Loading Custom Pages onto the Wireless Edge Services zl Module's Internal Server (Advanced) ......................... 5-26
Configuring the Allow List ............................................ 5-28
Configuring Encryption for a Web-Auth WLAN .................. 5-30

Copying Logo Files to the Module’s Flash ......................... 5-33

Configuring Custom Web-Auth Pages ............................... 5-36
Configuring the CGI Commands for the Login Page ............... 5-36
Configuring the CGI Commands for the Welcome Page .......... 5-38
6 IP Services—IP Settings, DHCP, and DNS

Contents ................................................................. 6-1

IP Settings ................................................................. 6-3
- Viewing VLAN Interfaces and Enabling Secure Management ........ 6-4
- Assigning an IP Address to a VLAN ........................................ 6-5
- Deleting the IP Address Assigned to a VLAN ................. 6-6
- Editing the IP Address Assigned to a VLAN .............. 6-7
- Viewing Statistics for VLANs That Are Assigned IP Addresses . 6-7
- Viewing a Graph for VLANs That Are Assigned IP Addresses .... 6-10

IP Routing .............................................................. 6-12
- Route Table .................................................................... 6-12
- Adding Static Routes to the Route Table .................. 6-14
  - Specifying a Default Route and Gateway .................. 6-15
- Address Resolution Table ............................................. 6-17

DNS Client ................................................................. 6-19
- Adding DNS Servers .................................................. 6-19
- Deleting a DNS Server ............................................... 6-21
- Specifying a Default Domain Name .............................. 6-21

DHCP Server .......................................................... 6-22
- Overview ...................................................................... 6-22
- Configuring the DHCP Server ........................................ 6-23
  - Creating DHCP Pools ............................................... 6-23
  - Excluding Addresses from a Network Pool ............... 6-32
  - Enabling the DHCP Server .................................. 6-33
- Configuring Global DHCP Settings: Ignoring BOOTP and Setting the Ping Interval .................. 6-35
- Configuring Extended DHCP Options ......................... 6-37
  - Setting Up Global Options ..................................... 6-37
  - Specifying the Value for an Extended Option in a DHCP Pool . 6-39
- Configuring Dynamic DNS (DDNS) ............................. 6-41
- Viewing DHCP Bindings ............................................. 6-43
- Configuring DHCP Relay ............................................. 6-45
7 Access Control Lists (ACLs)

Contents

Overview .................................................. 7-2
Stateful ACLs ........................................... 7-2
ACL Types ................................................. 7-3
  Standard IP ACLs ..................................... 7-3
  Extended IP ACLs ..................................... 7-3
  MAC Standard ACLs .................................. 7-4
  MAC Extended ACLs .................................. 7-4
ACL Rules .................................................. 7-4
  Precedence ............................................. 7-5
  Filters .................................................. 7-5
  Operation .............................................. 7-7
ACL Strategies ........................................... 7-8
Configuring ACLs ........................................ 7-10
  Creating ACLs ........................................ 7-10
  Configuring Rules for ACLs ......................... 7-13
    Creating Rules for Standard IP ACLs ............. 7-14
    Creating Rules for Extended IP ACLs ............. 7-17
    Creating Rules for MAC Extended ACLs .......... 7-23
  Modifying ACL Rules ................................ 7-25
  Applying ACLs to Interfaces ......................... 7-26
  Using ACLs with DHCP Services ...................... 7-28
  Viewing ACL Statistics ............................... 7-29

8 Configuring Network Address Translation (NAT)

Contents .................................................... 8-1
Overview .................................................. 8-3
  Translating Between an Inside and an Outside Network ..... 8-3
  Local and Global Addresses ............................ 8-4
NAT Implementation Methods ........................................ 8-5
  Dynamic, or Many-to-One, NAT ................................ 8-5
  Dynamic NAT for Wireless Traffic .............................. 8-5
  Dynamic NAT for Wired Traffic ................................. 8-7
  Port Address Translation for Dynamic NAT .................. 8-8
Static, or One-to-One, NAT ........................................ 8-8
  Static NAT on Destination Addresses ......................... 8-9
  Using Port Forwarding with Static Destination NAT ....... 8-10
  Static NAT on Source Addresses ............................... 8-12
Understanding Local and Global Addresses ....................... 8-12

Planning the NAT Configuration ................................. 8-15
  Consider Your Company’s Requirements for NAT ............ 8-15
  Record Necessary IP Addresses and Select the NAT
    Implementation Method ....................................... 8-17
    Planning the Configuration for Dynamic NAT ............ 8-17
    Planning the Configuration for Static NAT ............... 8-19

Configuring Standard ACLs for Dynamic NAT .................. 8-22
Configuring NAT .................................................... 8-24
  Defining Interfaces as Outside or Inside ..................... 8-24
  Configuring Dynamic NAT ..................................... 8-26
  Configuring Static Translation ............................... 8-29
    Configuring Static Source NAT ............................. 8-30
    Configuring Static Destination NAT ....................... 8-33
  Viewing NAT Status ............................................. 8-38

9 Fast Layer 2 Roaming and Layer 3 Mobility

Contents ............................................................. 9-1
Overview ............................................................ 9-2
  Layer 2 Roaming on a Single Wireless Edge Services zl Module ... 9-2
  Fast Layer 2 Roaming for WPA/WPA2 with 802.1X ........... 9-3
    Pre-authentication ........................................... 9-3
  Layer 2 Roaming on a Web-Auth WLAN Between Different
    Wireless Edge Services zl Modules ......................... 9-4
  Layer 3 Mobility ................................................ 9-5
  Roaming Behavior ............................................... 9-8
10 Redundancy Groups

Contents ................................................................. 10-1

High Availability for Wireless Services .................. 10-2
    Redundant Wireless Services zl Module ................ 10-2
    Redundancy Group ............................................. 10-3
    Active or Standby Mode ..................................... 10-4
    Adopting RPs .................................................. 10-5
        Adopting RPs in Active Mode ......................... 10-5
        Adopting RPs in Standby Mode ....................... 10-6
    RP Licensing for Redundancy Groups .................... 10-6
    Establishing a Redundancy Group ......................... 10-7
    Creating Matching Configurations for the Redundancy Group 10-9
        Redundancy Group Configuration Mode Context .... 10-9
    Redundancy Group Behavior When a Member Fails .... 10-10

Configuring a Redundancy Group ......................... 10-11
    Configuring Redundancy Group Settings ................. 10-12
    Adding Members to the Redundancy Group ............... 10-14
    Enabling Redundancy ....................................... 10-16
    Viewing Information about the Redundancy Group .... 10-18
        History .................................................... 10-21
    Viewing Information about the Other Members of the Redundancy Group ......................... 10-22
11 RADIUS Server

Contents .......................................................... 11-1

Overview .......................................................... 11-2

RADIUS Authentication ............................................. 11-3

Configuring the Internal RADIUS Server ....................... 11-4
- Choosing the Authentication Type for 802.1X/EAP .......... 11-5
- Specifying the RADIUS Server’s Digital Certificate ....... 11-8
- Choosing the Source for User Credentials .................. 11-9
- Configuring the Local RADIUS Database ................... 11-12
- Using LDAP for the Data Source ............................. 11-19
- Specifying a Domain Proxy RADIUS Server ............... 11-27
- Specifying Global RADIUS Settings ......................... 11-30
- Adding RADIUS Clients ....................................... 11-31
- Starting and Stopping the RADIUS Server ............... 11-32

Enabling Authentication to the Internal Server on a WLAN .... 11-33

RADIUS Accounting ................................................. 11-37

Enabling Accounting to the Internal RADIUS Server on a WLAN .......... 11-39

Viewing the Internal RADIUS Server’s Accounting Logs ........ 11-43
12 Wireless Network Management

Contents ................................................................. 12-1

Overview ............................................................... 12-3

Monitoring the Wireless Network .............................. 12-4
  Wireless Stations .................................................. 12-4
    Viewing Wireless Stations ..................................... 12-4
    Disconnecting a Wireless Station ............................ 12-6
    Viewing Details about a Wireless Station ................. 12-7
    Viewing All Stations in a Layer 3 Mobility Domain .... 12-10
  Wireless Statistics ............................................... 12-12
    Viewing Detailed Wireless Statistics ..................... 12-13
    Viewing a Graph of Wireless Station Statistics ....... 12-15
  Radio Statistics .................................................. 12-19
    Viewing Detailed Radio Statistics ......................... 12-20
    Viewing a Graph of Radio Statistics ....................... 12-21
  WLAN Statistics .................................................. 12-26
    Viewing Traffic Statistics for the WLAN ................. 12-27
    Viewing Detailed WLAN Statistics ......................... 12-28
    Viewing a Graph of WLAN Statistics ....................... 12-30
  Module Statistics ............................................... 12-34
    Radio Port Adoption Statistics ............................ 12-36

AP Detection ........................................................ 12-39
  Configuring AP Detection ..................................... 12-40
  Creating Lists of Detected APs ............................. 12-46
    Creating Rules That Define Allowed APs ................. 12-47
  Monitoring Detected APs ..................................... 12-51
    Managing the Unapproved APs List ......................... 12-51
    Managing the Approved APs List ............................ 12-54
    Configuring the Module to Report Unapproved APs .... 12-55

Configuring Station Intrusion Detection ...................... 12-58
  Configuring Thresholds for Station Intrusion Detection .. 12-59
  Configuring the Module to Report Station Intrusion .... 12-60
  Viewing Blocked Stations ..................................... 12-62
Logging and Alarms .................................................. 12-63
  Configuring Logging ............................................. 12-64
    Enabling Logging ............................................. 12-64
    Forwarding Logs to an External Server ................. 12-65
    Viewing Events in the Local Log File .................. 12-66
    Deleting and Transferring the Local Log File .......... 12-69
  Managing the Alarm Log ....................................... 12-71
    Details .......................................................... 12-73
    Delete ........................................................... 12-73
    Acknowledge .................................................... 12-74
    Export .......................................................... 12-74
MAC Filters (Local MAC Authentication) ...................... 12-75
  Configuring MAC Standard ACLs (Filters) ................. 12-76
  Configuring WLAN Memberships .............................. 12-78
  Exporting and Importing MAC Standard ACLs (Filters) ..... 12-82
    Exporting MAC Standard ACLs ............................... 12-82
    Importing MAC Standard ACLs ............................... 12-84
Network Self Healing ............................................. 12-89
  Neighbor Recovery ............................................ 12-89
    Enabling Neighbor Recovery ............................... 12-90
    Specifying Neighbors Manually ........................... 12-92
    Configuring Radios to Automatically Detect Neighbors ... 12-94
    Selecting the Self-Healing Action ....................... 12-95
    Configuring a Self Healing Offset ....................... 12-98
  Interference Avoidance ...................................... 12-100
13 sFlow Agent

Contents ................................................................. 13-1
Overview ................................................................. 13-2
  Flow Sampling by the sFlow Agent .............................. 13-2
  Counter Polling by the sFlow Agent ......................... 13-3
  sFlow Receiver ...................................................... 13-4
  Configuring sFlow Receiver Instances ....................... 13-4
Configuring sFlow Using the Web Browser Interface ........ 13-7
  Manually Configuring sFlow Receiver Instances Using the Web Browser Interface .......................... 13-8
  Manually Activating Flow Sampling ......................... 13-11
  Manually Activating Counter Polling ...................... 13-14

A ProCurve Wireless Services zl Module Command Line Reference

B Software License Agreements
Introduction

Contents

ProCurve Wireless Edge Services zl Module ............................................ 1-4
Wireless Networks and WLANs ................................................... 1-5
The Interface Between the Wireless and Wired Networks ........ 1-7
  Communicating with RPs: Radio Port VLANs ......................... 1-8
  Communicating with the Ethernet Network: Uplink VLANs ... 1-12
  Forwarding Traffic Between the Wireless Network and
  the Ethernet Network ....................................................... 1-14
Layer 2 and Layer 3 Operation .............................................. 1-16
  RP Operations ........................................................................ 1-16
  Wireless Edge Services zl Module Operations ...................... 1-17
Determining the Layer 3 Services Your Wireless Edge Services
  zl Module Should Provide .................................................. 1-18
  Using the Same VLANs for Wireless and Wired Users ........... 1-18
  Reserving VLANs for Wireless Users ...................................... 1-19
  Reserving VLANs for Wireless Users in a Network with
  Multiple Wireless Edge Services zl Modules ......................... 1-21
IP Routing ................................................................................. 1-23
DHCP Services ........................................................................ 1-24
Security Features ........................................................................ 1-24
  Authentication Options for WLANs ........................................ 1-24
  Encryption Options for WLANs .............................................. 1-32
  Intrusion Detection .................................................................. 1-34
  Controlling Traffic with Policies ............................................. 1-35
  Wireless Edge Services zl Module Firewall ............................ 1-38
  PKI and Digital Certificates .................................................. 1-45
Traffic Management and QoS ........................................ 1-46
SVP ......................................................... 1-48
WMM ......................................................... 1-48
WLAN Classification ........................................... 1-49
Voice Prioritization ............................................ 1-49
WFQ .......................................................... 1-50
Management Capabilities and sFlow ................................ 1-50
RP Licensing .................................................. 1-50
Radio Ports ................................................... 1-53
802.11 Overview .............................................. 1-54
  Physical Layer Standards .................................. 1-54
  802.11 Frames .............................................. 1-56
  BSS ........................................................... 1-56
  BSSID ......................................................... 1-58
  ESS ............................................................ 1-58
  SSID Versus BSSID ......................................... 1-59
  Beaconing .................................................... 1-61
RP Modes ..................................................... 1-62
  Master Mode ................................................ 1-62
  Detector Mode .............................................. 1-63
Configuring the ProCurve RPs .................................. 1-64
  Radio Adoption Default Configurations .................... 1-65
  Specific Radio Configurations ............................. 1-67
Communications Between an RP and the Wireless Edge Services zl Module: Layer 2 and Layer 3 Adoption .......... 1-68
  Managing RPs in a Self-Healing Network .................... 1-73
  802.1X Client ................................................ 1-74
  RP Deployment Requirements ................................ 1-75
  Power over Ethernet (PoE) .................................. 1-75
  Antennas ..................................................... 1-75
Redundancy Groups ............................................. 1-76
  Redundant Wireless Services zl Module .................. 1-76
  Rules of Redundancy Groups ................................ 1-77
  Redundancy Group Operation Modes ....................... 1-78
Layer 2 and Layer 3 Roaming Between RPs and Modules ............. 1-81
  Roaming Between RPs on a Single Wireless Edge
  Services zl Module .................................................. 1-81
  Roaming Between RPs on Different Wireless Edge
  Services zl Modules at Layer 2 .................................. 1-82
  Roaming Between RPs on Different Wireless Edge
  Services zl Modules at Layer 3 .................................. 1-84
ProCurve Wireless Edge Services zl Module

The ProCurve Wireless Edge Services zl Module transforms a ProCurve Switch 5400zl Series or ProCurve Switch 8200zl Series into a wireless services-enabled switch. Together with one or more radio ports (RPs), this wireless services-enabled switch creates a Wireless LAN System.

With its default RP license, each Wireless Edge Services zl Module can support up to 12 RPs (for a total of 24 radios). If you purchase and install additive RP licenses, the module can support up to 156 RPs (for a total of 312 radios). Each RP radio can support up to 64 stations simultaneously, although more stations always translates to less bandwidth for each.

A wireless network can include several Wireless Edge Services zl Modules. These modules can function independently, or you can combine them in several ways. You can join up to twelve modules in a group to provide redundancy. You can also group modules in a Layer 3 mobility domain, which enables wireless stations to roam from a module in one Ethernet subnetwork to a module in a different subnetwork.

A ProCurve Wireless LAN System—which includes a Wireless Edge Services zl Module and its adopted RPs—can provide these services:

- **Association**—Mobile users must be able to locate and connect to the wireless network.
- **Authentication**—Typically, users and the wireless access provider should authenticate each other so that each knows that it is connecting to the correct peer.
- **Encryption**—Wireless network traffic may be encrypted to protect it from interception.
- **Bridging**—Traffic crossing from the wireless network to the wired network should be placed in the proper subnetwork, or virtual LAN (VLAN), and appropriately controlled.

As the interface between the wireless and the wired network, the Wireless Edge Services zl Module manages these services. After bridging traffic to the wired network, the module can also provide Layer 3 capabilities, such as Dynamic Host Configuration Protocol (DHCP) services, Network Address Translation (NAT), and filtering with a firewall.
Among other functions, the Wireless Edge Services zl Module:

- manages a set of wireless LANs (WLANs)—each of which is identified by a service set identifier (SSID) and defines various network and security policies
- receives traffic from wireless stations via RPs and places this traffic into the correct VLAN to be forwarded into the wired network
- adopts connecting RPs and automatically deploys configurations to them

Depending on how you configure the Wireless Edge Services zl Module, it may also:

- enforce users’ 802.1X, MAC, or Web authentication (Web-Auth) to either:
  - an external Remote Authentication Dial-In User Service (RADIUS) server
  - its internal RADIUS server
- apply quality-of-service (QoS) settings to traffic received from and destined to wireless stations
- provide DHCP services
- route among up to eight VLANs
- implement a firewall between VLANs, applying both MAC and IP access control lists (ACLs) and Network Address Translation (NAT)
- enable seamless and fast Layer 2 roaming, as well as Layer 3 roaming, between one of its own RPs and an RP adopted by itself or by another module
- monitor the wireless network for signs of an attack or intrusion
- collect information about the wireless network and control self-healing functions such as neighbor recovery and interference avoidance
- sample wireless traffic and send the samples to an sFlow collector such as ProCurve Manager Plus (PCM Plus)

This chapter provides a brief overview of these functions, as well as some of the technologies on which they are based.

Wireless Networks and WLANs

In this guide, the term wireless network is used to encompass all the devices (such as stations, RPs, access points [APs], Wireless Edge Services zl Modules, and wireless services-enabled switches) involved in your organization’s wireless functions.

The term Wireless LAN System refers to a Wireless Edge Services zl Module and all of its adopted RPs, which function together as a single entity.
The Wireless Edge Services zl Module acts the Wireless LAN System's brain. The RPs produce the wireless signal, but the module enforces wireless authentication, generates and encrypts wireless frames, and sets all other policies in the Wireless LAN System as a whole. A large part of the Wireless Edge Services zl Module’s duties lie in establishing the settings for WLANs.

A wireless LAN (WLAN), as opposed to a wireless network, refers more precisely to a set of wireless stations that connect to one or more RPs using the same SSID, or network name. (For a more technical definition of a WLAN, as well as its relation to an SSID, an extended service set (ESS), a basic service set (BSS), and a basic SSID (BSSID), see “ESS” on page 1-58.)

For the purposes of configuring a WLAN on the Wireless Edge Services zl Module, you can think of a WLAN as a set of parameters on which an RP and its associated stations agree. These parameters include:

- the SSID that identifies the WLAN
- the type of authentication a station must complete before connecting to the WLAN
- the encryption algorithms and keys that secure wireless data
- support for QoS protocols and, in the case of a protocol such as Wi-Fi Multimedia (WMM), the settings for priority queues

The Wireless Edge Services zl Module defines these settings, and RPs broadcast them to wireless stations in beacon and other 802.11 management frames.

For RPs, the module’s WLAN settings also control:

- whether the RPs broadcast the WLAN’s SSID and respond to probe requests about the SSID (operate in open system)
- whether the RPs forward frames directly between wireless stations or force all traffic to travel through the Wireless Edge Services zl Module (inter-station blocking)

One of the Wireless Edge Services zl Module’s primary tasks is act as the interface between the wireless and wired networks. That is, the module bridges traffic from a WLAN to a VLAN. The WLAN is said to be mapped to that VLAN.
Although you configure the Wireless Edge Services zl Module to assign WLAN traffic to a particular VLAN, a WLAN in the wireless network does not necessarily have a one-to-one relationship with a VLAN in the Ethernet network.

The module can tag traffic received from several WLANs for the same VLAN. Conversely, by implementing user-based VLANs, the module can tag traffic from different stations in the same WLAN for different VLANs. For more information about user-based, also called dynamic, VLANs, see “Controlling Traffic with User-Based Policies” on page 1-35.

After bridging the traffic to the VLAN, the Wireless Edge Services can handle the traffic in a variety of ways at both Layer 2 and Layer 3. You will learn about these capabilities later in this chapter; first you must understand more precisely how the module joins the wireless and wired networks, receiving and forwarding traffic on its downlink and uplink ports.

The Interface Between the Wireless and Wired Networks

As the interface between the wireless and wired networks, the Wireless Edge Services zl Module includes two internal ports:

- a downlink port
- an uplink port

The downlink port is associated with the wireless world. It sends traffic to and receives traffic from the external switch interfaces that connect, either directly or indirectly, to RPs. The downlink port carries traffic tagged for Radio Port VLANs.

The uplink port sends traffic to and receives traffic from external switch interfaces that connect to other devices in the Ethernet network. The uplink port carries traffic in one or more uplink VLANs—VLANs used in the Ethernet network.

The following sections describe how the module forwards traffic between RPs and the Ethernet network, focusing in particular on the VLAN to which the traffic is assigned at various points in this process.
Communicating with RPs: Radio Port VLANs

The Wireless Edge Services zl Module uses a Radio Port VLAN to send traffic to and receive traffic from the RPs it adopts.

The RPs are designed to isolate traffic that they transmit into your network until the Wireless Edge Services zl Module can control this traffic. An RP encapsulates each wireless frame, leaving the 802.11 header and any encryption intact, and forwards it to the module on the Radio Port VLAN.

The Radio Port VLAN can be established in one of three ways:

- with auto-provisioning on the wireless services-enabled switch
- manually on an infrastructure switch (or, if you want, on the wireless services-enabled switch)
- dynamically on either a wireless services-enabled switch or an infrastructure switch based on a VLAN assignment stored on a RADIUS server

**Note**

The rule that the Wireless Edge Services zl Module receives RP traffic on its downlink port and a Radio Port VLAN has one exception. When an RP is adopted at Layer 3, it can communicate with the module on either the uplink or the downlink port. The only rule for the VLAN on which an RP is adopted at Layer 3 is that this VLAN be tagged on *only one* of the internal ports.

For more information on Layer 3 adoption, see “Communications Between an RP and the Wireless Edge Services zl Module: Layer 2 and Layer 3 Adoption” on page 1-68.

**Using Auto-Provisioning to Establish a Radio Port VLAN.** When you install a Wireless Edge Services zl Module in a zl switch, auto-provisioning is enabled by default: the switch automatically establishes VLAN 2100 as the default Radio Port VLAN, or the Auto-VLAN. (If VLAN 2100 is unavailable, the switch uses the next available VLAN number.)

The switch also automatically configures the module’s internal downlink port as a *tagged* member of this Radio Port VLAN. (The port is a tagged member because the module drops all untagged traffic.)

When an RP is connected to a port on the wireless services-enabled switch, the switch uses Link Layer Discovery Protocol (LLDP) to identify itself to the switch. The switch then automatically configures the port as an *untagged* member of the Radio Port VLAN. (Because the RP does not support 802.1Q, the port must be an untagged member of the VLAN.)
Figure 1-1 shows the VLAN tagging if auto-provisioning remains enabled on the wireless services-enabled switch.

**Note**

If, for whatever reason, you do not want an RP placed in the default Radio Port VLAN, you can manually create a different Radio Port VLAN on the wireless services-enabled switch. (In this case, you should turn off auto-provisioning.) The instructions in “Manually Establishing a Radio Port VLAN” on page 1-10 apply to a wireless services-enabled switch as well as to an infrastructure switch.

However, take care never to tag the same VLAN on the uplink and downlink port.
**Manually Establishing a Radio Port VLAN.** If you connect an RP to an infrastructure switch instead of directly connecting it to the wireless services-enabled switch, you must manually establish the Radio Port VLAN on that infrastructure switch.

The wireless services-enabled switch still uses auto-provisioning to create VLAN 2100 and tag the module's internal downlink port for this VLAN. However, you must configure the infrastructure switch's port that connects to the RP as an *untagged* member of the Radio Port VLAN.

Remember that the external switch interfaces that link the infrastructure switch and the wireless services-enabled switch must also carry traffic on the Radio Port VLAN. You must make these interfaces either tagged or untagged for the Radio Port VLAN, depending on whether they must carry other traffic in addition to the wireless traffic transmitted to and from the RP. Figure 1-2 shows the VLAN assignments if you connect an RP to an infrastructure switch.

![Diagram](image)

**Figure 1-2. Manually Establishing a Radio VLAN for an Indirectly Connected RP**
Although it is usually a good idea to use auto-provisioning on the wireless services-enabled switch and to create the same Radio Port VLAN on the infrastructure switches that directly connect to RPs, you can use any valid VLAN numbers for Radio Port VLANs. Simply remember to tag the Wireless Edge Services zl Module’s downlink port for that VLAN.

In Figure 1-3, the network administrator has decided to use VLAN 300 for one of the RPs. (Although you typically place all RPs in the same VLAN, such a design is not mandatory.)

![Figure 1-3. Manually Creating Radio Port VLANs](image)

Remember that the internal downlink port must always be *tagged* for the Radio Port VLAN, while the external switch port that connects to the RP must always be *untagged.*
Note

You might also need to perform some configuration tasks on the wireless services-enabled switch, such as raising the maximum number of VLANs. (See the management and configuration guide for your zl switch.

**Dynamically Establishing a Radio Port VLAN.** If the RP authenticates itself to a RADIUS server, this server may send a dynamic VLAN assignment to the switch to which the RP connects. The switch configures the RP's port as an untagged member of the dynamic VLAN.

Both infrastructure and wireless services-enabled switches can receive settings for dynamic Radio Port VLANs, depending, of course, on their capabilities. The dynamic VLAN takes precedence over both manually configured and auto-provisioned settings.

See “802.1X Client” on page 1-74 for more information on how ProCurve RPs authenticate themselves.

**Communicating with the Ethernet Network: Uplink VLANs**

The Wireless Edge Services zl Module communicates with the Ethernet network on the uplink VLANs.

Although the Wireless Edge Services zl Module receives traffic from RPs in a Radio Port VLAN and this traffic has been transmitted over the Ethernet network, the 802.11 frame is still intact. When the module receives this traffic, it must bridge the traffic into the Ethernet network. As part of this process, the module must place the traffic in a VLAN. The module does so according to the VLAN assignment stored in the association with the wireless station that sent the traffic.

This VLAN assignment is important because it determines the subnetwork in which wireless stations are placed, as well as the type of network access they receive. When the user authenticates and associates, the Wireless Edge Services zl Module makes the VLAN assignment as follows:

- The module assigns the station to a dynamic VLAN if two conditions are met:
  - Dynamic VLANs are enabled on the station's WLAN.
  - A RADIUS server (either an external server or the module's internal server) sends a dynamic VLAN assignment for the successfully authenticated user.
- Otherwise, the module determines the WLAN to which the station belongs and assigns it to the VLAN specified for that WLAN.
By default, the only uplink VLAN is VLAN 1, and the module's internal uplink port is tagged for this VLAN. As for any switch port, you must tag the uplink port for other VLANs if you want the module to forward network traffic in those VLANs. The Wireless Edge Services zl Module never forwards untagged traffic to the wireless services-enabled switch.

However, you do not have to tag the uplink for every VLAN that you create on the module. Instead, you can have the module route traffic in a module VLAN to a VLAN used in the wired network. This strategy isolates VLANs assigned to wireless users from VLANs used for traditional, wired users.

You configure the actual tagging through the management interface on the wireless services-enabled switch. (For instructions on tagging ports, see the management and configuration guides for your zl switch.)

Figure 1-4 illustrates a network in which traffic from WLAN 1 is forwarded into the Ethernet network in VLAN 10. Note that the station receives an IP address from the network's DHCP server (rather than from the module's internal DHCP server).
Figure 1-5 illustrates a network in which the Wireless Edge Services zl Module assigns traffic from WLAN 1 to VLAN 24, a VLAN reserved for wireless traffic. In this network, the wireless station receives an IP address from the module’s internal DHCP server, and the module routes the station’s traffic to servers in the private, Ethernet network.

Figure 1-5. Routing Traffic to VLANs Used on the Wired Network

Forwarding Traffic Between the Wireless Network and the Ethernet Network

In summary, the Wireless Edge Services zl Module follows this process to forward traffic that is sent from wireless stations (via RP radios) into the Ethernet network:

1. The module receives wireless traffic on its internal downlink port in a Radio Port VLAN.
2. The module enforces any controls applied to the downlink port. Such controls can include ACLs, either manual or user-based, and user-based rate limits. (For more information about such controls, see “Controlling Traffic with Policies” on page 1-35 and “ACLs” on page 1-40.)
3. The module assigns the traffic to the VLAN specified in that station’s association.

4. The module determines whether it is acting as the router for this traffic and takes action accordingly:
   a. If the module is acting as router (that is, the frame’s destination MAC address belongs to the module), the module looks up the route for the packet’s destination.
      However, before forwarding the traffic, the module applies any controls, such as manual IP ACLs, configured on the VLAN on which the traffic arrived. (See “ACLs” on page 1-40.)
      The Wireless Edge Services zl Module’s firewall also filters the traffic as it is routed from its original VLAN. (See “Wireless Edge Services zl Module Firewall” on page 1-38.)
      If the packet passes all checks, the module forwards the traffic to the gateway device listed in the route. The gateway device’s VLAN must be tagged on the module’s internal uplink port.
   b. If the source station is sending the traffic to a destination in its own VLAN, the module forwards the traffic at Layer 2.
      Typically, the module forwards the traffic on the uplink port toward a device in the Ethernet network. If you have not enabled the uplink port to carry tagged traffic for the uplink VLAN, then the module drops the traffic.
      Sometimes a wireless station attempts to communicate with another wireless station. In this case—given that you allow such inter-station traffic—the module forwards the traffic on the downlink port toward the RP listed in the 802.11 association with the destination device.
      When the module forwards traffic at Layer 2, IP ACLs applied to the incoming VLAN interface do not filter the traffic, nor does the firewall.

5. The wireless services-enabled switch forwards the traffic toward its destination.

The Wireless Edge Services zl Module follows a similar process to forward traffic from the Ethernet network to wireless stations:
1. The module receives the traffic on its uplink port in an uplink VLAN.
2. The module applies controls to the traffic, if any are configured. The controls can include:
   • a user-based ACL or rate-limit assigned by ProCurve IDM
   • a manual IP or MAC extended ACL applied to the uplink port
   • a manual IP ACL applied to the VLAN interface

3. The module creates the correct 802.11 frame, drawing on information specified in the association with the destination station. The module also encrypts the frame, if necessary.

4. The module encapsulates the 802.11 frame. The encapsulation header includes a tag for the Radio Port VLAN specified for the radio to which the destination station has associated.

5. The module forwards the traffic toward its destination on its downlink port.

**Layer 2 and Layer 3 Operation**

You have been introduced to how the Wireless Edge Services zl Module receives, processes, and forwards traffic. You can now become better acquainted with specific operations that the module applies to traffic. For example, the module might apply an ACL to the traffic or perform NAT on it. To understand when the module performs specific functions, you must first understand how the module (and adopted RPs) operate at Layer 2 and Layer 3.

The Wireless Edge Services zl Module's *downlink* port and associated RPs function as Layer 2 devices. The Wireless Edge Services zl Module itself, as well as its *uplink* port, can operate at Layer 3 as well as Layer 2.

**RP Operations**

RPs typically function at Layer 2 and do not have IP addresses; the Wireless Edge Services zl Module manages all communications with them.

In some configurations, however, an RP can receive an IP address and operate at Layer 3. When an RP cannot reach a Wireless Edge Services zl Module at Layer 2, it obtains a dynamic IP address and learns the module's IP address. In this case, the RP communicates with the module at Layer 3. See “Communications Between an RP and the Wireless Edge Services zl Module: Layer 2 and Layer 3 Adoption” on page 1-68.
Wireless Edge Services zl Module Operations

The downlink port does not have an IP address; it is tagged for the Radio Port VLAN, and the module does not require an IP address on this VLAN.

The Wireless Edge Services zl Module operates at Layer 2 on its downlink port. On the downlink port, the module receives encapsulated 802.11 frames. It decapsulates and processes these frames and then bridges them to an Ethernet subnetwork (VLAN). When transmitting traffic back to wireless stations, the module also acts at Layer 2, forwarding traffic based on the associations to those stations.

After the module bridges a frame to a VLAN interface, the module can handle the inner packet at Layer 3. Note that this VLAN interface may or may not be tagged on the uplink port.

The module can also act at Layer 3 on traffic received on its uplink port, which can be tagged for one or several VLANs.

Note

Never tag the internal uplink and the downlink ports for the same VLAN.

In total, the Wireless Edge Services zl Module can support up to eight VLAN interfaces with IP addresses and Layer 3 functionality. (The module can tag traffic for these VLANs or for other VLANs that operate at Layer 2 only; in this guide, a VLAN interface refers only to those VLANs that have been configured with IP addresses.)

Whether traffic arrives on a VLAN interface on the uplink port or is bridged to the VLAN from a WLAN, the module can handle the traffic as follows:

- respond to or relay DHCP requests
- apply IP ACLs to packets
- perform NAT on packets
- filter packets using the internal firewall
- route packets to their destinations

The following section helps you to consider when your environment requires your Wireless Edge Services zl Module to provide these services. The sections that follow provide more information about each particular capability.
Determining the Layer 3 Services Your Wireless Edge Services zl Module Should Provide

When you are designing your network, you must consider which operations you want the Wireless Edge Services zl Module to perform on wireless and wired traffic. The answer often lies in the degree to which you want to separate wireless traffic from your Ethernet network.

Using the Same VLANs for Wireless and Wired Users

If you want to handle wireless stations just as you do wired, you can configure the Wireless Edge Services zl Module to assign WLAN traffic to the user VLANs already in place in your wired network. On the wireless services-enabled switch, you tag the module’s uplink port for those VLANs.

The module then forwards the traffic to the wireless services-enabled switch at Layer 2, and the same devices that route and control traffic from traditional users can handle traffic from the wireless users. In this scenario, the module may perform few or none of the Layer 3 functions listed in “Wireless Edge Services zl Module Operations” on page 1-17.

Figure 1-6 shows how the Wireless Edge Services zl Module can forward traffic into VLANs used on a wired network.
Reserving VLANs for Wireless Users

On the other hand, wireless networks are different from wired networks—different in the services that they provide and different in the level of trust that they inspire. You might use your wireless network to grant access to limited services, such as only email and the Internet. You might open the wireless network to guests and less trusted users.

If your wired network has adequate firewalls and other security measures, you might prefer having the wired infrastructure handle the wireless traffic. In this case, follow a similar design to that in “Using the Same VLANs for Wireless and Wired Users” on page 1-18. However, create a VLAN just for wireless traffic:

- Have the Wireless Edge Services zl Module map a WLAN to a VLAN reserved for wireless users. (Or set up dynamic VLAN assignments for wireless users.)
- Configure that VLAN on wired infrastructure devices. The devices should be able to route traffic in and out of the VLAN.
- Tag the Wireless Edge Services zl Module’s uplink port for the VLAN.

Figure 1-8 shows a wireless network that separates VLANs used on the wireless network from VLANs used on the wired network. In this network, wired devices route traffic from the wireless network.
On the other hand, you might want the Wireless Edge Services zl Module itself to router, filter, and otherwise control traffic. In this case, follow this design:

- Have the Wireless Edge Services zl Module map a WLAN to a VLAN reserved for wireless stations. (Or set up dynamic VLAN assignments for wireless users.)
- Terminate that VLAN on the module. In other words, do not tag the module's uplink port for the VLAN.
- Enable routing on the module.

This design requires the Wireless Edge Services zl Module to take over many of the functions otherwise performed by network servers and infrastructure devices. For example, the module can act as the DHCP server for wireless stations, and it can perform dynamic NAT, masquerading as the source for all wireless traffic.

Figure 1-8 shows a wireless network that separates VLANs used on the wireless network from VLANs used on the wired network. In this network, the Wireless Edge Services zl Module routes traffic from the wireless network.
Reserving VLANs for Wireless Users in a Network with Multiple Wireless Edge Services zl Modules

A network that has more than one Wireless Edge Services zl Module introduces another factor that you must consider: roaming between the modules. To facilitate roaming and consistent network services, every module should assign the same WLAN to the same VLAN (subnetwork) when possible.
The instructions in the rest of this section are based on the assumption that the same VLAN ID corresponds to the same subnetwork throughout your network. This assumption is usually, but not always, true. The important consideration for roaming is that modules assign traffic in the same WLAN to the same subnetwork.

Sometimes, however, your network design makes it impossible for modules to forward traffic on the same subnetworks. If so, using the same VLAN ID for the WLAN on every module is no longer valid. Instead configure Layer 3 roaming, making sure to associate each different subnetwork with a different VLAN ID. See “Roaming Between RPs on Different Wireless Edge Services zl Modules at Layer 3” on page 1-84.

If the VLAN and subnetwork that you choose for the WLAN is one used in the traditional wired network, the design is much the same as that for a network with a single module. If you want to reserve the VLAN for wireless users, however, you must alter the design slightly. You must be careful not to terminate the VLAN for wireless users on each module. Instead, extend the VLAN through your infrastructure. However, do not configure the infrastructure devices to route traffic in and out of this VLAN but simply to forward the VLAN traffic between the modules.

This design addresses several issues. When a station first associates to an RP, the module that supports that RP assigns the station a DHCP address with itself as the default gateway. If the station later roams to a new module, its traffic must be able to reach the original module. In addition, when all modules use the same Layer 2 subnetwork, they can exchange pre-authentication messages, speeding roaming in WLANs that require 802.1X authentication.

Figure 1-9 shows a network that includes multiple Wireless Edge Services zl Modules and separates VLANs for the wireless network from VLANs for the wired network.
Now that you have considered the services that your Wireless Edge Services zl Module should provide, you can start to look at individual services in more detail. The following sections describe the capabilities of the module, including, in addition to the Layer 3 services introduced above, the module’s many capabilities in securing and managing the wireless network.

**IP Routing**

The module can implement basic routing between its VLANs. It can have up to eight directly connected routes (one on each VLAN interface), and you can manually add static routes. The module also has one active default route.

IP routing is disabled by default. Even if wireless stations use a different router, you might want to enable IP routing because several module capabilities require routing to be active. These functions are:

- DHCP relay
- the internal firewall
- IP ACLs applied to logical (VLAN or tunnel) interfaces
- NAT
DHCP Services

The Wireless Edge Services zl Module can provide one of these DHCP services on any VLAN interface to which you have assigned a *static* IP address:

- **DHCP server**—The module issues configurations (which are stored in a network pool) to stations in the VLAN. You can configure up to one network pool for each VLAN. You can also create host pools, each of which contains a fixed address for a single device. The module supports standard DHCP options, such as the IP addresses for a default router and Domain Name System (DNS) server. You can also define extended options and specify them for a pool.

- **DHCP relay**—The module forwards DHCP requests that arrive on the VLAN to an external DHCP server on a different VLAN.

With its DHCP capabilities, the Wireless Edge Services zl Module can support VLANs unique from those on your private, wired network. For example, your private network might use VLANs 1 to 23. You could establish a WLAN for mobile employees, customers, and guests; map the WLAN to VLAN 24; and terminate the VLAN on the module. (That is, you would not tag the module’s internal uplink port for VLAN 24 nor extend the VLAN throughout the network.)

You should ensure that the module can route the wireless traffic. Typically, you should also configure dynamic NAT in conjunction with DHCP. In the Ethernet network, the module then appears as the source for traffic from the module’s wireless DHCP clients. (See “NAT” on page 1-43.)

Security Features

As a network administrator, you must constantly consider how to secure your network, particularly as you add wireless access. The Wireless Edge Services zl Module supports a variety of security features both for wireless traffic and for the interface between the wireless and wired network.

Authentication Options for WLANs

A key function of the Wireless Edge Services zl Module is to establish settings for your network’s WLANs. One such setting is the method by which wireless stations authenticate themselves before associating to a WLAN.

Forcing stations to authenticate themselves protects your network from unauthorized users, securing both your organization’s data and that of wireless users. This security also protects wireless users from connecting to a rogue AP.
A Wireless Edge Services zl Module supports three types of authentication:

- 802.1X authentication
- Web-Auth
- RADIUS MAC authentication

Alternatively, the Wireless Edge Services zl Module can allow stations to connect to a WLAN without authenticating formally. In this case, an encryption key usually acts as a password.

The authentication types are implemented as part of a WLAN's settings. You can enable different types of authentication on different WLANs, but each WLAN can use only one of the three types of authentication.

However, you can also create MAC filters (MAC standard ACLs), which function as local MAC authentication. You configure these filters globally and then apply them to a WLAN. The filter is applied in addition to any other authentication you configure on that WLAN.

802.1X Authentication. 802.1X, an IEEE standard specifically developed to provide identity-based authentication for users, requires an authenticator to manage the exchange between a wireless station and an authentication server. The Wireless Edge Services zl Module acts as this authenticator. When a wireless user attempts to associate with a WLAN, the module blocks all traffic from the user's wireless station until the user authenticates itself to an authentication server (a RADIUS server).

With its internal RADIUS server, the Wireless Edge Services zl Module can also act as the authentication server.

802.1X relies on Extensible Authentication Protocol (EAP), which comes in several varieties designed by various product developers. Although the actual process varies according to the specific method, the basic process is outlined below:

1. A wireless station associates to the WLAN.
2. The Wireless Edge Services zl Module receives the station's traffic from the RP. As soon as the association becomes active, the module places the station in a shutdown status. The module issues an EAP challenge and refuses all traffic except EAP messages from the station.
3. The station and the authentication server authenticate each other (the exact process differs, depending on the EAP method they choose).

The Wireless Edge Services zl Module receives the EAP messages from the wireless station (via the RP) and repackages them as RADIUS messages for the RADIUS server. Conversely, the module extracts EAP messages for the wireless station from RADIUS messages from the server.

4. If the user sends the correct credentials (which may take various forms, including a digital certificate or a username and password), the RADIUS server sends an authentication acknowledgement.

5. If you have configured the WLAN to use encryption, the authentication process includes generating a per-session encryption key for WEP or a pairwise (per-user) master key (PMK) for WPA. The authentication server passes the key to the Wireless Edge Services zl Module.

Automatically generating secure encryption keys is one of the most vital components of 802.1X for wireless networks. For more information about encryption, see “Encryption Options for WLANs” on page 1-32.

6. If your network implements user-based controls—configured, for example, through ProCurve IDM—the RADIUS server sends dynamic settings—such as a VLAN assignment, ACLs, and rate limits—for the station.

**Note**

Remember: if you are using the Wireless Edge Services zl Module’s internal RADIUS server, the module acts as both the authenticator and the authentication server.

In short, 802.1X provides robust authentication as well as dynamic key management, and, if you want, support for dynamic, user-based settings.

**Web-Auth.** The Wireless Edge Services zl Module can also provide Web-Auth for stations that do not support 802.1X authentication. In this case, the module confines unauthenticated wireless users’ access to a list of allowed IP addresses. The module forces a user to authenticate itself by redirecting all nonapproved traffic to a login page on a Web server.

Because the Wireless Edge Services zl Module handles all background processes (such as forwarding requests to DHCP, RADIUS, and DNS servers), the allow list only needs to include the IP address of the Web server that stores the pages that guide the user through the authentication process.

You can even opt to maintain the Web pages on the Wireless Edge Services zl Module itself to secure your organization’s Web server. In this case, the allow list can be completely empty.
Figure 1-10 illustrates the Web-Auth process.

<table>
<thead>
<tr>
<th>SSID 1</th>
<th>WLAN 1</th>
<th>Web-Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID 2</td>
<td>WLAN 2</td>
<td>802.1x</td>
</tr>
</tbody>
</table>

1. User associates with WLAN 1 and enters Web-Auth state.
2. User opens Web browser and attempts to access a Web site.
3. User's HTTP packets are redirected to Web-Auth login page.
4. User enters username and password.
5. If login is successful, user enters authenticated state.
6. If login fails, user remains in unauthenticated state.
7. User disconnects from network services and returns to Web-Auth state.

After users authenticate, the Wireless Edge Services zl Module can control users' network access with dynamic ACLs stored in the external RADIUS server's database (perhaps configured with software such as ProCurve IDM). You can also control the VLAN associated with Web-Auth with manual ACLs.

The Wireless Edge Services zl Module grants users that fail to authenticate the same guest status that it grants unauthenticated users. If you want, you can add IP addresses to the approved list to provide limited resources to such users. For example, you could allow unauthenticated guests to access a Web page with information about your organization and other courtesy services.

Web-Auth is popular for wireless networks with many anonymous users who may or may not have client software that supports 802.1X. This form of authentication grants companies a degree of control over users' access while presenting users with an intuitive and easily navigable login interface. However, Web-Auth is not as secure as 802.1X.
You can add either WEP or WPA/WPA2 encryption to a WLAN that uses Web-Auth. Users must then know the encryption key in order to connect to the network and even reach the login page.

**MAC Authentication.** The Wireless Edge Services zl Module can also control which wireless stations connect to a WLAN according to their MAC, or hardware-based, addresses. This option is best suited for small networks and for devices without user interfaces.

The module supports two types of MAC authentication: RADIUS and local.

**RADIUS MAC Authentication.** If you enable MAC authentication on a WLAN, the Wireless Edge Services zl Module sends a request, which includes a station’s MAC address as both the username and password, to a RADIUS server. (See Figure 1-11.) The RADIUS request can be in the following formats:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

For information about configuring RADIUS MAC authentication, see Chapter 4: “Wireless Local Area Networks (WLANs).”

![Figure 1-11. RADIUS MAC Authentication](image)

**Local MAC Authentication.** RADIUS MAC authentication allows you to control stations centrally. Alternatively, you can control traffic locally with MAC standard ACLs. On the Wireless Edge Services zl Module, these ACLs are called filters and are configured separately from other ACLs.

You configure the following ACLs and associate them with WLANs:

- **Deny ACLs**—Stations are prevented from connecting to your network.
- **Allow ACLs**—Stations are permitted to connect to your network.
The module processes ACLs in order of index number, stopping when it first finds a match. It filters out any stations selected by a deny list before these stations associate with a particular WLAN. The module allows all stations either selected by an allow list or not selected by any list to associate. Whether the station can forward traffic in the WLAN depends on whether it completes any further authentication required by the WLAN.

For example, suppose you configure MAC authentication filters and apply them to a WLAN; you also enable 802.1X authentication on that WLAN. When a station attempts to connect to the WLAN, the module first checks the station’s MAC address. If the ACLs allow the station to associate to the WLAN, the module lets it proceed to authenticate using 802.1X.

The Wireless Edge Services zl Module can store and apply up to 1,000 ACLs. Any kind of encryption supported on the module is supported on a WLAN that uses local MAC authentication because these standards are configured entirely separately.

For information about configuring MAC ACLs, see Chapter 12: “Wireless Network Management.”

**Authenticating to a RADIUS Server.** Each of the authentication methods described in the sections above involve an authentication server. This server decides whether a station can connect to the network based on whether:

- the user provides the right login credentials
- the policies configured on the server allow wireless access at this time and location

The Wireless Edge Services zl Module supports authentication to an external RADIUS server or to its internal server.

**External RADIUS Server.** The Wireless Edge Services zl Module can contact an external RADIUS for these types of authentication:

- **MAC authentication**—The module can send either a PAP or a CHAP request to the external server, placing the station’s MAC address in both the username and password fields. You can configure the format in which the module sends the MAC address (that is, the type and placement of delimiters).

- **Web-Auth**—The module authenticates Web-Auth users to an external server using either PAP or CHAP requests. The module fills in the username and password fields from the information that a user enters into the Web-Auth login screen.
**Introduction**  
**ProCurve Wireless Edge Services zl Module**

- **802.1X with EAP**—The module acts as the 802.1X authenticator, and the external RADIUS server is the authentication server. The Wireless Edge Services module has been certified for these EAP methods:
  - EAP-Transport Layer Security (TLS)
  - EAP-Tunneled TLS (TTLS)
  - PEAP with Microsoft CHAP version 2 (MS-CHAP v2)
  - EAP-Subscriber Identity Module (SIM)
  - EAP-Generic Token Card (GTC)

**Note**

In 802.1X, the supplicant and the authentication server, not the authenticator, agree on the EAP method. Because the module simply passes EAP messages between the wireless station and the external server, rather than generating the messages itself, it should support any standard EAP method. The module has been certified those EAP method listed above.

For more information about EAP methods, see “EAP Methods” on page 1-31.

**Internal RADIUS Server.** The Wireless Edge Services zl Module’s internal RADIUS server can authenticate stations that connect to the module’s WLANs. The server can also respond to authentication requests from clients such as switches that enforce port authentication in the Ethernet network.

The internal RADIUS server supports these types of authentication:
- MAC authentication
- Web-Auth
- 802.1X with EAP:
  - EAP-TLS
  - EAP-TTLS with PAP
  - EAP-TTLS with MD5
  - PEAP with MS-CHAP v2

The internal RADIUS server can draw on one of two repositories for checking user credentials:
- **Local database**—The local database consists of user accounts and groups. A user account includes a username and password and, for guest accounts only, an expiration date and time. You assign a user to a group, which defines policies, including valid access times and VLAN assignment.
- **LDAP-compliant server**—The Wireless Edge Services zl Module can bind to an Lightweight Directory Access Protocol (LDAP)-compliant server. The LDAP-compliant server stores the login credentials, and you configure the module to bind to the server and perform searches for a user’s password and group. The group configuration in the module’s local database determines when wireless users can connect and the VLAN to which they are assigned.

**EAP Methods.** This section gives a brief overview of common EAP methods so that you can choose the method best for your environment.

EAP-TLS uses digital certificates and an automatic TLS handshake to authenticate both stations and servers. This method requires a full public key infrastructure (PKI).

EAP-TTLS and PEAP support wireless stations that do not use digital certificates. These EAP methods use the TLS handshake to create a secure tunnel over which the station can authenticate itself with another, less secure method. This inner method typically involves sending a username and password.

Wireless phones can use EAP-SIM to authenticate, automatically sending information stored on a smartcard rather than relying on a user to enter login credentials.

EAP-GTC is an early EAP method that requires users to enter information, usually read from a token card. Sometimes, however, the user simply enters a password.
Table 1-1 compares EAP methods and the support that the Wireless Edge Services zl Module provides for them.

### Table 1-1. EAP Methods and the Wireless Edge Services zl Module

<table>
<thead>
<tr>
<th>EAP Type</th>
<th>Requirement</th>
<th>Module Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>digital certificate on both the server and the wireless stations</td>
<td>authenticator or the authentication server</td>
</tr>
</tbody>
</table>
| EAP-TTLS with PAP or MD6 | • digital certificate on the server  
|                     | • user-entered name and password                                             | the authenticator or the authentication server |
| PEAP MS-CHAP v2     | • digital certificate on the server  
|                     | • user-entered name and password                                             | the authenticator or the authentication server |
| EAP-SIM             | Global System for Mobile communications (GSM) smartcard on the wireless station (phone) | the authenticator |
| EAP-GTC             | user-entered token card information or password                              | the authenticator |

EAP authentication also requires that the RADIUS server authenticate itself to wireless stations with a server certificate. For more information about how the Wireless Edge Services zl Module uses and acquires certificates, see “PKI and Digital Certificates” on page 1-45.

### Encryption Options for WLANs

A wireless network is an open medium. Anyone with a wireless network interface card (NIC) can intercept traffic and attempt to read it. Encryption, therefore, is required for any degree of security.

The Wireless Edge Services zl Module can enforce one of the following encryption standards on a WLAN:

- Wired Equivalent Privacy (WEP) with 64-bit or 128-bit keys
- Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Identity Protocol (TKIP)
- WPA2 with Advanced Encryption Standard (AES)
- WPA/WPA2 with both TKIP and AES (802.11i Mixed Mode)

A detailed analysis of encryption is beyond the scope of this guide. Briefly, however, the security of an encryption scheme often stands on the number of times an encryption key is reused. Each of the above standards attempts to create per-frame keys—that is a key that is used only one to encrypt a single frame.
WEP did not succeed at creating per-frame keys for several reasons that are beyond the scope of this overview to describe. You simply need to know that, in an enterprise setting, you should always use the more secure WPA or WPA2. WPA requires TKIP, a protocol that implements key mixing to successfully create per-frame keys. In addition to backward-compatibility support for TKIP, WPA2 requires support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) with AES—an extremely secure block cipher.

As was suggested throughout “Authentication Options for WLANs” on page 1-24, authentication is an important component of encryption. This is because 802.1X authentication provides a means for the Wireless Edge Services zl Module and the wireless devices to automatically receive an encryption key specific to their association.

Without 802.1X authentication, all wireless stations must use the same key. The key also acts as a password: unless the user enters the correct key, the station cannot successfully encrypt and forward data. For WPA/WPA2, the additional security provided by TKIP or AES offsets the lesser security of using a shared, manually configured encryption key. For WEP, however, a static key provides little real security, particularly in a busy, enterprise environment.
Table 1-2 lists the encryption options that are available with each authentication option.

**Table 1-2. Options for Authentication and Encryption on the Wireless Edge Services zl Module**

<table>
<thead>
<tr>
<th>Authentication Option</th>
<th>Encryption Options</th>
<th>Name of Security Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>• WEP with 64-bit or 128-bit keys</td>
<td>• dynamic WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2:</td>
<td>• WPA/WPA2 with 802.1X</td>
</tr>
<tr>
<td></td>
<td>– with TKIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with both TKIP and AES (802.11i Mixed Mode)</td>
<td></td>
</tr>
<tr>
<td>Web-Auth</td>
<td>• WEP with 64-bit or 128-bit keys</td>
<td>• static WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2:</td>
<td>• WPA/WPA2 with a preshared key (PSK)</td>
</tr>
<tr>
<td></td>
<td>– with TKIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with both TKIP and AES (802.11i Mixed Mode)</td>
<td></td>
</tr>
<tr>
<td>RADIUS MAC authentication</td>
<td>• WEP with 64-bit or 128-bit keys</td>
<td>• static WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2:</td>
<td>• WPA/WPA2-PSK</td>
</tr>
<tr>
<td></td>
<td>– with TKIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with both TKIP and AES (802.11i Mixed Mode)</td>
<td></td>
</tr>
<tr>
<td>MAC filters (comparable to local MAC authentication)</td>
<td>Depends on other authentication implemented on the WLAN</td>
<td>Depends on other authentication implemented on the WLAN</td>
</tr>
<tr>
<td>No authentication</td>
<td>• WEP with 64-bit or 128-bit keys</td>
<td>• static WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2:</td>
<td>• WPA/WPA2-PSK</td>
</tr>
<tr>
<td></td>
<td>– with TKIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with AES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– with both TKIP and AES (802.11i Mixed Mode)</td>
<td></td>
</tr>
</tbody>
</table>

**Intrusion Detection**

Even if an unauthorized wireless user is denied access to a WLAN, he or she can launch attacks. For example, he or she can flood RPs with probe requests or pose as another user and cause that user denial of service (DoS). You can implement a variety of attack checks on the Wireless Edge Services zl Module that guard against malicious attacks from any wireless user. For more information, see Chapter 12: “Wireless Network Management.”
Controlling Traffic with Policies

To this point, the overview of the Wireless Edge Services zl Module's security capabilities has focused on the security that module provides in the wireless network. However, in addition to managing which users connect to a WLAN (wireless authentication), the Wireless Edge Services zl Module also manages how users connect to the Ethernet network, controlling traffic so that each wireless user receives access to the appropriate services and resources. The module acts as the door between the wireless and wired networks; it can open the door to many different resources, depending on the policies it applies to wireless users’ traffic.

The module can apply policies that:
- it receives dynamically from a RADIUS server
- you configure manually

The following sections describe these options in more detail.

Controlling Traffic with User-Based Policies. As you know, a RADIUS server authenticates users who try to connect to your network. Using ProCurve IDM, you can configure the RADIUS server to associate additional settings with a particular user. When the user authenticates, the server sends these settings to the Wireless Edge Services zl Module, and the module applies them to traffic from that user.

Such settings are sometimes called user-based or identity-based because a user’s identity (rather than simply a MAC address or a switch port) links settings with traffic from a particular user. The settings are also called dynamic because you do not configure them permanently on the module; rather, the module receives them only when a particular user connects. In addition, the module can receive and apply different settings for different users or for the same user at different times.

The RADIUS server sends the user-based settings as HP ProCurve vendor-specific attributes in the message with which it accepts a user’s authentication. The Wireless Edge Services zl Module interprets these attributes and sets rules based on them. For the duration of the user’s association, the module controls the user’s traffic according to these rules.
The Wireless Edge Services zl Module can read these attributes from an external RADIUS server:
- VLAN assignment
- ACL
- rate limit, which applies to ingress traffic (traffic from the wireless station to the network)

Remember that the Wireless Edge Services zl Module can also act as a RADIUS server. The module supports only dynamic VLAN assignments on its internal RADIUS server.

Figure 1-12 shows how the user-based settings on the RADIUS server allow the Wireless Edge Services zl Module to assign users who connect to the same WLAN to different VLANs.

It does not matter how you actually configure these attributes on the RADIUS server. However, ProCurve IDM greatly simplifies the configuration process. Using ProCurve IDM, you create policies to control individual users' network access, depending on the time and location from which they connect. An IDM agent automatically configures the correct attributes on the RADIUS server. (For more information about ProCurve IDM, see the ProCurve Identity Driven Manager User's Guide. You can download this guide from http://www.procurve.com.)
If you are using your Wireless Edge Services zl Module’s internal RADIUS server, you can set this user-based policy: VLAN ID.

**Controlling Traffic Manually.** You can also control traffic according to manually created rules on the Wireless Edge Services zl Module; however, such policies are generally less flexible.

You can control these settings:

- **VLAN assignment**—When configuring VLAN assignments manually, you must assign an entire WLAN to the same VLAN. For example, suppose users A, B, and C connect to WLAN 1. User A is in the Marketing department, user B is in the Engineering department, and user C is a guest. With either an external or the module’s internal RADIUS server, you can configure the module to place each user in a different VLAN. If you manually configure the settings on the Wireless Edge Services zl Module, you must place all the users in the same VLAN, as shown in Figure 1-13.

![Figure 1-13. Assigning VLANs Manually](image)

For instructions on configuring the VLAN assignment, see Chapter 4: “Wireless Local Area Networks (WLANs).”

- **Filters (or ACLs)**—The Wireless Edge Services zl Module’s internal firewall supports a variety of options for ACLs, which are described in “ACLs” on page 1-40. Depending on the ACL type, you can control traffic based on source address, destination address, application, WLAN, 802.1p priority, and other criteria.

You cannot configure rate limits manually.
Wireless Edge Services zl Module Firewall

The section above introduced you to the idea of controlling traffic with policies. The Wireless Edge Services zl Module's firewall is one of the components that helps you to do so.

The module's firewall examines routed packets. It checks for and drops:

- packets with invalid TCP flags
- corrupted packets:
  - multicast source address
  - unknown IP option
  - IP TTL set to zero
  - IP fragment overflowing the packet (last fragment length creates a packet longer than 65,535 bytes)
  - IP fragment with a bad Length (non-last fragment length is not a multiple of 8)
  - IP fragment with the same ID as another fragment in that packet (fragment ID collision)
- packets symptomatic of these attacks:
  - LAND attack (a TCP SYN packet in which the destination IP address and port equal the source IP address and port)
  - Fragment death (fragment that overflows the valid packet length)
  - Traceroute attack (modified IP TTL value)
  - Xmas scan (all TCP flags set in TCP header)
  - TCP FIN scan
  - TCP NULL scan (no flags set in TCP header)

When the firewall drops a packet, the Wireless Edge Services zl Module creates a log with the name and time of the attack.

Enabling Attack Checking. The firewall is always on; however, it only affects packets that are routed from one VLAN interface to another VLAN interface. When the Wireless Edge Services zl Module re packages an 802.11 frame from a WLAN as an Ethernet frame in a VLAN, the module is acting as a bridge, not a router. The attack checks do not occur at this point. However, if the module then routes the traffic to a different VLAN, the firewall can check the traffic.
You should take these steps to ensure that a firewall screens traffic in between a WLAN and your private, wired network:

1. Map the WLAN to a VLAN ID that exists only on the Wireless Edge Services zl Module (or possibly on this module and other modules that support the same WLAN).

2. Enable routing on the Wireless Edge Services zl Module.

   The module should route all wireless traffic destined to the private network. You can add static routes to the module's route table, but the simplest configuration uses a single route through a default gateway. Choose a default gateway that knows how to reach all destinations to which wireless stations need access.

3. Assign the Wireless Edge Services zl Module an IP address on the VLAN created for the WLAN.

4. On this VLAN, configure the module's internal DHCP server to assign IP addresses to wireless stations. In the DHCP configuration, specify the module as the default router.

5. Configure NAT to translate the source addresses for wireless traffic to one of the module's IP addresses.

   You have created a unique VLAN for wireless stations, which is unknown to devices within the wired network. NAT allows the Wireless Edge Services zl Module to masquerade as the source of all wireless traffic, so devices in the wired network direct all return traffic for the wireless network to the module.

   For more information about NAT, see “NAT” on page 1-43 and Chapter 8: “Configuring Network Address Translation (NAT).”

Figure 1-14 illustrates this network design.
Introduction
ProCurve Wireless Edge Services zl Module

Figure 1-14. Setting up VLANs to Ensure the Firewall Checks Wireless Traffic

ACLs. In addition to screening traffic for signs of an attack, the Wireless Edge Services zl Module's firewall can enforce policies that you create. These policies are called ACLs, and they affect traffic inbound on an interface.

Note
IP ACLs applied to VLAN interfaces only affect traffic routed to another VLAN. ACLs applied to physical interfaces affect all inbound traffic.

You can create the following types of ACLs:
- MAC standard ACLs
- MAC extended ACLs
- standard IP ACLs
- extended IP ACLs

As discussed in “MAC Authentication” on page 1-28, MAC standard ACLs filter traffic according to the source MAC address. These ACLs act as authentication: rather than control which network services a user can access, MAC ACLs either allow or block traffic from a station entirely.
MAC extended ACLs, like MAC standard ACLs, filter traffic according to information in the Layer 2 header. However, the extended ACL provides many more options for filters, including destination MAC address, 802.1p priority value, and the type of encapsulated protocol. For example, you can permit IPv4 traffic but drop IPv6 traffic.

The IP ACLs operate at Layer 3. A standard IP ACL filters traffic according to source IP address only. An extended IP ACL, on the other hand, examines many fields in the Layer 3 IP header and even the Layer 4 TCP or UDP header. For example, an extended IP ACL could select traffic associated with a particular application by specifying the destination TCP or UDP port for that application.

Table 1-3 compares the various types of ACLs.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Standard IP ACLs</th>
<th>Extended IP ACLs</th>
<th>MAC Standard ACLs</th>
<th>MAC Extended ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operates at</td>
<td>Layer 3</td>
<td>Layer 3/4</td>
<td>Layer 2</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Filters traffic according to</td>
<td>source address</td>
<td>source address</td>
<td>source address</td>
<td>source address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination address</td>
<td></td>
<td>destination address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protocol</td>
<td></td>
<td>protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP or UDP source port or destination port</td>
<td></td>
<td>TCP or UDP source port or destination port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICMP type</td>
<td></td>
<td>ICMP type</td>
</tr>
<tr>
<td>Applies to traffic on</td>
<td></td>
<td>individual VLAN interface</td>
<td></td>
<td>individual VLAN interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical interface (uplink or downlink port)</td>
<td></td>
<td>physical interface (uplink or downlink port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical interface (uplink or downlink port)</td>
<td></td>
<td>physical interface (uplink or downlink port)</td>
</tr>
</tbody>
</table>

The Wireless Edge Services zl Module applies an ACL to traffic that arrives on a particular interface:

- You can apply one IP ACL to a VLAN interface. It affects traffic that arrives on the VLAN interface and is routed to another VLAN.

Traffic arrives on a VLAN interface in these two circumstances:

- The Wireless Edge Services zl Module maps a wireless frame to that VLAN.

In other words, the module decapsulates the frame received from a WLAN, removes the 802.11 header, and adds an Ethernet header with a tag for that VLAN. The VLAN assignment might originate in a static setting for the entire WLAN or from a dynamic assignment received from a RADIUS server.
Introduction
ProCurve Wireless Edge Services zl Module

- The Wireless Edge Services zl Module receives the traffic on its uplink port from the wireless services-enabled switch; the traffic is tagged for the VLAN interface.

You can apply one IP ACL and one MAC extended ACL to each physical interface.

The two physical interfaces are the internal uplink and downlink ports. The ACL applies to all traffic that arrives on the port in any VLAN. In addition to imposing other filters, an ACL applied to the downlink port can filter traffic according to WLAN.

To control traffic that arrives on the downlink port with a MAC extended ACL, the Wireless Edge Services zl Module examines the 802.11 header and the Ethernet header after the packet is bridged. For traffic that arrives on the uplink port, the MAC extended ACL applies to the Ethernet header.

Figure 1-15 shows where ACLs affect traffic. For more information about ACLs, see Chapter 7: “Access Control Lists (ACLs).”

Figure 1-15. Applying ACLs to Interfaces
NAT. NAT, another function the Wireless Edge Services Zl Module’s firewall offers, modifies addresses in packets’ IP headers. The module supports NAT on both source addresses and destination addresses.

The Wireless Edge Services Zl Module has the following capabilities:

- **Dynamic source NAT with port mapping**—The module translates multiple source addresses to a single new address, which is one of the module’s own IP addresses. Although every NATed packet has the same new source address, the module assigns each session a different source port. The module then maintains a table that maps each source port to the correct original address, allowing the module to forward return traffic to its destination.

- **Static source NAT with optional port translation**—The module translates a single source IP address to a single new address.

  Typically, the address after translation is an IP address that is assigned to the Wireless Edge Services Zl Module. However, you can use a different IP address as long as it is not assigned to another device. If you choose not to use one of the module’s IP addresses, you must configure proxy ARP so that the module can respond to ARP requests for the NATed IP address.

  You can optionally configure the module to translate the packet’s source port to a new port.

- **Static destination NAT with port forwarding and optional port translation**—The module translates packets destined to a specific IP address (typically one of the module’s own) to a new IP address. It then forwards the traffic toward the new destination.

  Port forwarding allows the module to differentiate between traffic sent to the same IP address but different ports. For example, port forwarding can translate a packet sent to its public IP address on the HTTP port (80) to one IP address but translate a packet sent to the FTP port (21) to a different address. Port forwarding allows multiple servers to share the same public IP address.

  Port translation, an additional option, allows the Wireless Edge Services Zl Module to translate the destination port as well as the destination IP address. For example, the module can receive an HTTP packet on port 80 and change its destination to a Web server that uses the private port 55000.

You can learn more about these capabilities, including how to enable them, in Chapter 8: “Configuring Network Address Translation (NAT).” The section below gives some examples of when to use NAT.
Uses for NAT. Typically, NAT works at the interface between two networks controlled by separate entities. For example, you are probably familiar with how NAT functions on the Internet. The NAT device sits between your private network and the Internet. It intercepts packets sent from the private network to the Internet, changing all private source addresses to a single public IP address that is known on the Internet. If hosts on the Internet need to access a device in your private network, such as a Web server, the NAT device performs destination NAT in the other direction, translating traffic destined for the publicly known IP address to the correct private IP address.

The Wireless Edge Services zl Module performs NAT in much the same way, and you can use the module to ready traffic for transmission on the Internet. Other typical uses include:

- isolating wireless and wired traffic and preserving IP addresses

  You should guard the threshold between the wireless and wired network rigorously. As mentioned before, one of the best ways to protect the wired network is to create VLANs specifically for wireless traffic. The module can handle all necessary functions for those VLANs, including DHCP services and routing.

  The module should also perform dynamic source NAT on addresses in the VLAN for wireless users, translating all wireless stations’ IP addresses to its own IP address on the wired network. This step ensures that, even though the VLAN for wireless users does not exist in the wired network, return traffic finds its way to the module and back onto the wireless network.

  Another benefit of using dynamic source NAT on wireless traffic is that the wireless stations do not consume IP addresses in the wired network. They all share a single IP address on the wired network—the IP address of the Wireless Edge Services zl Module.

- concealing IP addresses in the private, wired network from wireless users

  You can configure the Wireless Edge Services zl Module to translate the source IP addresses of traffic that originates on your private, wired network. To allow access to specific private servers, you must also configure destination NAT, which translates the IP address advertised in the wireless network back to the private address on the wired network.

- relaying traffic destined for a particular server to a different server

  For example, wireless stations might send requests to one server on the Internet, but you want to force the stations to communicate with a different server. In this case, you configure static destination NAT to translate packets destined to the first server to the server of your choice.
PKI and Digital Certificates

The Wireless Edge Services zl Module’s security capabilities often require it to authenticate itself with a digital certificate and the data it sends with a digital signature.

Digital signatures, created by a public-private key pair, authenticate data. To create the digital signature, a key pair relies on asymmetric encryption, which means that data encrypted by a private key is decrypted by the corresponding public key. A host “signs” data by encrypting it with its private key—something only that host can do because only it knows the private key. Other hosts verify the signature by decrypting the signature with the public key, which is distributed freely.

A digital certificate distributes the public key, tying it to a particular host’s identity, which can be presented as an LDAP distinguished name, a hostname, or an IP address. Typically, a trusted third-party, called the certificate authority (CA), signs and issues certificates. A less secure option is a self-signed certificate, which is issued by the host itself.

Remember that verifying a signature requires a public key in a digital certificate. To verify the CA’s signature, a host must have the CA’s certificate. The CA’s certificate is signed either by itself or by another CA, higher in the PKI hierarchy. The root CA is the top of the PKI hierarchy and trusted implicitly; the root CA’s certificate is self-signed.

A set of certificates from the host’s own certificate up to the root CAs is grouped together as a trustpoint. The Wireless Edge Services zl Module supports up to six trustpoints, each of which can store one of the following sets of certificates:

- **One self-signed certificate**—No CA certificate is required because the module is the root of the trustpoint.
- **One root CA certificate, one server certificate issued by that CA, and one certificate revocation list (CRL)**

The advantage of a trustpoint that terminates in a root CA is, of course, that a host is more likely to trust the module’s certificate when it is signed by a well-known CA.

To obtain a CA-signed certificate, the module generates a certificate request, which you transfer from the module and submit to the CA. The Wireless Edge Services zl Module supports:

- Privacy Enhanced Mail (PEM)-formatted certificates
- Distinguished Encoding Rules (DER)-formatted certificates
You can load these certificates to the module from an FTP server, a TFTP server, or the local disk of the management station.

Before creating a certificate or certificate request, the Wireless Edge Services zl Module must generate a public/private key pair. The module can create Rivest-Shamir-Adleman (RSA) keys of between 1024 and 2048 bytes. Each certificate can use a unique key pair, or multiple certificates can share a key pair.

The Wireless Edge Services zl Module uses certificates for several purposes:

- **HTTPS access**—The module’s server certificate authenticates the module to your Web browser.
- **RADIUS authentication services**—802.1X authentication with EAP requires mutual authentication. In other words, the module’s internal RADIUS server must send a server certificate and authenticate to supplicants.
- **Autokey authentication for secure Network Time Protocol (NTP)**—The module sends its certificate to the secure NTP server to authenticate itself and generate keys to secure NTP exchanges.

Because the Wireless Edge Services zl Module can store multiple trustpoints, you can select different certificates for different functions.

**Traffic Management and QoS**

In the past, users often treated wireless connections as a supplement to other network connections. Now, users demand more and more from wireless connections, increasing congestion and decreasing QoS.

Compounding the problem, users have begun to demand the same applications to which they have become accustomed on Ethernet connections. As multimedia applications become more common in wireless networks, maintaining a high QoS for such time-sensitive, bandwidth-intensive traffic becomes a priority. Voice-over-WLAN (VoWLAN) wireless phones further complicate the situation with yet another type of traffic that requires special handling.

A wireless network, which uses the shared medium of radio signals, functions differently from a switched Ethernet network. On a wireless network, collisions can occur, bandwidth can be reduced, and latency can be high. A wireless QoS solution must address these issues.
The Wireless Edge Services zl Module manages wireless traffic with several QoS mechanisms, ensuring that each type of traffic receives the necessary level of service. The module supports the following QoS protocols, which you can enable on a WLAN-to-WLAN basis:

- SpectraLink Voice Priority (SVP)
- priority queuing based on WMM or on a WLAN classification

These protocols improve QoS in the wireless network. You can also configure the module to mark traffic outbound to voice stations for high priority. Called Voice prioritization, this feature improves the QoS for traffic destined to wireless stations, as the traffic travels through both the Ethernet network and the wireless network.

Finally, the Wireless Edge Services zl Module can implement weighted fair queueing (WFQ) on traffic destined from the module to RPs.

Figure 1-16 illustrates which traffic is affected by each QoS mechanism.
This chapter will discuss these features at a high level; to learn how to configure them, see Chapter 4: “Wireless Local Area Networks (WLANs).”

SVP

SVP maintains a high QoS in the wireless network, specifically for VoWLAN devices that are SVP-capable. SVP is implemented in wireless phone handsets, wireless APs, and SpectraLink servers. This IEEE 802.11-compliant mechanism minimizes latency for voice traffic by providing priority queues reserved for voice packets and by increasing the probability that all voice packets are transmitted in a predictable and timely manner.

If your network includes a SpectraLink server and SVP-capable phones, you should enable SVP in the WLAN that includes these phones. RPs then recognize SVP-encapsulated frames and handle them accordingly.

WMM

WMM is a more comprehensive QoS solution because it can provide differentiated handling for any type of traffic based on its priority. Like 802.1p and Differentiated Services (DiffServ) in Ethernet networks, WMM divides traffic into multiple priority queues and then assigns different settings to each queue. Although the types of settings dictated by the protocols are of course different (as the shared wireless medium is different from the switched Ethernet medium), the goal is the same: higher throughput for high priority traffic, as well as lower latency for time-sensitive traffic.

The Wireless Edge Services zl Module can implement WMM on both downstream and upstream wireless traffic. To implement WMM on downstream wireless traffic, the module sends settings for priority queues as part of a radio’s configuration. To implement WMM on upstream wireless traffic, the module configures RPs to send priority queue settings to wireless stations in a particular WLAN.

You must enable WMM on a WLAN if you want RPs to prioritize downstream traffic according to priority value. Enabling WMM also allows WMM-capable wireless stations to prioritize upstream wireless traffic. By default, devices prioritize traffic according to 802.1p priority. However, you can configure them to use DiffServ values instead.

Figure 1-17 illustrates how the Wireless Edge Services zl Module can configure RPs and wireless stations to prioritize mission-critical and VoWLAN traffic.
WLAN Classification

WMM allows RPs to queue frames according to priority marking. Alternatively, RPs can place all traffic that is destined to stations associated with a particular WLAN in the same queue. The four queues are the same as the four access categories (ACs) for WMM (Voice, Video, Best Effort, and Background), and the RPs use the same parameters for transmitting traffic in those queues that they would use for WMM. The only difference is that traffic is queued statically according to WLAN instead of automatically according to priority marking.

Voice Prioritization

Voice prioritization improves QoS for traffic destined to VoWLAN devices. When you enable this feature in a WLAN, RPs monitor frames received from stations in that WLAN. When a voice frame is detected, the Wireless Edge Services zl Module marks all traffic destined to the source of that frame for priority handling.

Ethernet devices between the Wireless Edge Services zl Module and the RP and the RP itself place return traffic to the VoWLAN device in a high-priority queue. Thus, voice prioritization can improve QoS for voice traffic in both the Ethernet and the wireless networks.
WFQ

The Wireless Edge Services zl Module queues traffic outbound to RPs according to the RP and the WLAN to which it is destined. Each different WLAN on each different RP has its own queue.

Management Capabilities and sFlow

You can manage the ProCurve Wireless Edge Service zl Module through either a command line interface (CLI) or its intuitive Web browser interface. Access to the Web browser interface is controlled through the highly secure Simple Network Management Protocol version 3 (SNMP v3).

You can also manage the Wireless Edge Services zl Module entirely through an SNMP solution such as PCM Plus.

In addition to managing the module’s software and configuration, the SNMP server can also analyze the wireless traffic processed by the module. The Wireless Edge Services zl Module acts as an sFlow agent, sampling wireless traffic and forwarding the samples to the SNMP server or other sFlow collector. The module can also poll RP radios for overall traffic statistics and submit the results to the sFlow collector. Through packet sampling and counter polling, sFlow creates a highly accurate picture of network traffic—useful for security auditing, traffic management, or network troubleshooting—without consuming undue resources.

RP Licensing

Each Wireless Edge Services zl Module (J9051A) includes an RP license, allowing it to adopt and manage up to 12 RPs. This nonremovable RP license ships with the module.

Note

Because an RP can include two built-in radios, the Wireless Edge Services zl Module can manage up to twice as many radios as it can adopt RPs. With the default RP license, the module can manage up to 24 radios.

If you connect a thirteenth RP to the wireless services-enabled switch, the module does not adopt it. The module can, however, adopt the RP if you disconnect one of the other RPs: the module does not bind a license to a particular set of RPs.

For the same reason, you can move the module to a different wireless services-enabled switch, and it continues functioning as before. It simply adopts the RPs that connect to the new wireless services-enabled switch. (Modules also retain licenses if you move them to a different slot in the same switch.)
You can purchase two types of additive licenses:

- a license which allows the Wireless Edge Services zl Module to adopt 12 additional RPs
- a license which allows the Wireless Edge Services zl Module to adopt 48 additional RPs

You can install any combination of these licenses. The Wireless Edge Service zl Module can adopt a maximum of 156 radios.

For networks that require between 12 and 48 RPs, purchase additive 12 RP Licenses.

For networks that required between 48 and 156 radios, it is generally recommended that you purchase the 48 RP Licenses.

Table 1-4 shows the licenses you should buy to support a particular number of RPs.

Table 1-4. RP Licenses and the Number of RPs Supported

<table>
<thead>
<tr>
<th>Products</th>
<th>Maximum Number of RPs</th>
<th>Maximum Number of Radios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td>Wireless Services Module 12 RP License</td>
<td>36</td>
<td>72</td>
</tr>
<tr>
<td>2 Wireless Services Module 12 RP Licenses</td>
<td>48</td>
<td>96</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>60</td>
<td>120</td>
</tr>
<tr>
<td>1 Wireless Services Module 48 RP License</td>
<td>108</td>
<td>216</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>156</td>
<td>312</td>
</tr>
</tbody>
</table>

You install additive licenses on a particular module, and only that module can adopt the additional RPs. However, you can uninstall additive licenses and then install them on a different module.
For example, suppose you install an additive 48 RP License on a Wireless Edge Services zl Module so that it can adopt 60 RPs. Later, you decide that a different module should support additional RPs. You uninstall the additive license from the first module and install it on the second. In other words, if you need to move RPs within your network, you can move RP licenses instead of moving an entire module.

**Note**

You can move only *additive* licenses. You can *never* remove a module’s original license for 12 RPs and install it on another module.
Radio Ports

Because the RPs are a critical component of the wireless network—establishing the actual radio signal and transmitting wireless traffic to and from stations—you should understand how these RPs function.

The Wireless Edge Services zl Module can manage the following ProCurve RPs:

- **RP 210**—includes one 802.11bg radio. The radio has two omnidirectional diversity antennas.
- **RP 220**—includes two radios, one 802.11a and one 802.11bg. Each radio has two omnidirectional diversity antennas.
- **RP 230**—includes two radios, one 802.11a and one 802.11bg. This RP is designed for use with external antennas.

Using their radios and Ethernet interfaces, these IEEE 802.11-compliant RPs enable wireless stations to connect to a WLAN and eventually to your Ethernet network.

**Note**

This guide will generally use the term RP instead of AP, even when discussing general concepts that apply to both, to remind you that you connect RPs to the Wireless Edge Services zl Module.

These devices are “thin” APs, which ProCurve Networking refers to as RPs to distinguish them from its “thick” APs. Unlike APs, the RPs themselves provide little intelligence. Instead, the RPs rely on the Wireless Edge Services zl Module for the intelligence required to provide advanced services and customized access for wireless users.

You can think of an RP as a remote radio on the Wireless Edge Services zl Module. For example, an RP receives 802.11 frames from wireless stations, encapsulates them in Ethernet headers, and forwards them to the Wireless Edge Services zl Module; the module handles functions associated with a standalone AP, such as generating 802.11 frames, encrypting traffic, filtering traffic, and tagging traffic for a specific VLAN.

The advantage of such a deployment—coordinated RPs managed by a module installed in a switch—is that the wireless network can be controlled efficiently for consistent and transparent network access for all users. In addition, you can configure multiple RPs through the Wireless Edge Services zl Module instead of using separate management interfaces to configure each one.
802.11 Overview

802.11 is the IEEE standard for wireless networks. It specifies Physical Layer standards such as radio channel frequencies and the modulation techniques used to encode data. At the Data Link Layer, the standard also specifies the format for 802.11 frames.

At its most fundamental level, an 802.11 network can be defined as a set of devices that communicates over the same medium. The area in which the devices can detect each other's signals is sometimes called a wireless cell.

More broadly, an 802.11 network, or WLAN, is a set of devices (typically, stations and RPs) that share a network name.

For the purposes of understanding how to configure your Wireless Edge Services zl Module, some important 802.11 concepts are:

- Physical Layer standards
- 802.11 frames
- Basic service set (BSS)
- Basic service set identifier (BSSID)
- Extended service set (ESS)
- Service set identifier (SSID)

Physical Layer Standards

The ProCurve Wireless Edge Services zl Module and ProCurve RPs support these Physical Layer standards:

- 802.11a
- 802.11b
- 802.11g
- 802.11h
- 802.11a

802.11a. 802.11a defines the Physical Layer for wireless networks in the 5.0 GHz range. Each wireless cell operates on a certain subfrequency, or channel, within this range. None of these channels overlap—that is, interfere with each other. The exact channels differ from region to region; setting the country code on Wireless Edge Services zl Module allows the module OS to present you with the correct options when you configure radio settings.
The 802.11a standard enables data rates from 6.0 Mbps to 54 Mbps, depending on the quality of the signal level. Overhead and competition for the shared medium often lowers actual throughput to about half the theoretical data rate.

The second radio on the RP 220 and on the RP 230 supports 802.11a.

**802.11b.** This standard defines the Physical Layer for wireless networks that operate in the 2.4 GHz band—one of the radio bands available to any private entity.

This band includes channels 1 to 14, some of which, however, are not allowed in certain regions. The channels overlap, each creating noise in the five channels on either side. Non-overlapping channels include:

- 1, 6, and 11
- 1, 7, and 13

802.11b enables data rates between 1 Mbps and 11.5 Mbps, although overhead decreases the actual throughput by at least half.

Although 802.11g is replacing 802.11b, some older stations still support only 802.11b. The RP 210's single radio and the first radio on the RP 220 and the RP 230 support 802.11b.

**802.11g.** 802.11g operates in the 2.4 GHz range like 802.11b. However, it enables the higher data rates of 802.11a—between 6.0 Mbps and 54 Mbps (although, again, overhead decreases the actual throughput).

The RP 210's single radio and the first radio on the RP 220 and the RP 230 also support 802.11g. 802.11g is backward compatible with 802.11b, so the radio can support both standards at once. This guide refers to the RP radios that support 802.11b and 802.11g as 802.11bg radios.

By default, an RP's 802.11 bg radio supports both 802.11b and 802.11g stations. You can remove support for 802.11b stations by requiring 802.11g's short preamble and removing the 802.11b rates for the radio's basic rate set. See Chapter 3: “Radio Port Configuration” for more information.

**802.11h.** 802.11h consists of two mechanisms: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). DFS enables RPs to dynamically change channel if they detect interference on a channel. RPs use TPC to lower their power, and that of associated stations, and minimize interference.
Many countries require support for 802.11h as a condition to using certain 802.11a channels. The countries operate military radar on those channels; with 802.11h, the private radios share the channels without interfering with the military.

The second radio on the RP 220 and on the RP 230 supports 802.11a.

802.11 Frames

In addition to Physical Layer standards, 802.11 defines Data Link Layer standards. 802.11 frame types include:

- control frames, which wireless devices use to reserve the shared medium
- management frames, which regulate communications between stations and RPs and include:
  - beacon frames, which the RP radio uses to announce itself to wireless stations and which will be discussed in more detail in “Beaconing” on page 1-61
  - authentication frames, which wireless devices use to ensure that they are connecting to the correct peer
  - association frames, which stations use to negotiate the wireless connection to an RP

A station cannot send or receive data until it associates to an RP.

- data frames, which encapsulate all the higher layer packets the wireless connection is intended to carry (for example, a data frame might include an HTTP request for a Web page)

BSS

A BSS is the set of wireless stations controlled by a single coordination function as well as the RP to which they connect. In other words, the BSS consists of all stations that share the same medium (the radio signal broadcast by an RP) to transmit and receive data. (See Figure 1-18.)
A BSS operates in infrastructure mode, which means that instead of communicating with each other, wireless stations communicate with an RP. This is the typical mode for a wireless network used to grant mobile users access to an Ethernet network, as well as the mode in which the ProCurve RPs operate. (See Figure 1-19.)
A wireless station must send all traffic to its RP. However, the RP can then forward the traffic to another station in the BSS. For tighter security, you can block these inter-station communications entirely, or you can force them to pass through the Wireless Edge Services zl Module, where ACLs can be applied. See “Controlling Inter-Station Traffic” on page 4-63 of Chapter 4: “Wireless Local Area Networks (WLANs).”

Figure 1-19. Infrastructure Mode

**BSSID**

The BSSID is the RP’s MAC address in a BSS. (See Figure 1-18.) Wireless stations in a BSS address all frames to the BSSID.

**ESS**

An ESS is a set of BSSs that share a common network name, or SSID. An ESS may consist of many RPs, and on the Physical Layer each of these RPs manages a different shared medium. However, logically all of the RPs and the stations they support are part of the same network, identified by the same SSID. The WLAN configured with this SSID defines all options for the ESS.

In contemporary networks, it is often more useful to talk about an ESS than a BSS because users may roam from RP to RP. Each RP may support a different BSS, but all share the same SSID, as shown in Figure 1-20. In fact, at the logical layer, all BSSs in an ESS appear as the same BSS to a wireless station.
Similarly, when configuring the Wireless Edge Services zl Module, you are often more interested in the WLAN to which users connect than in the particular RP to which a user connects at any given moment.

**SSID Versus BSSID**

As indicated above, the SSID identifies a group of BSSs that make up a single WLAN. All frames transmitted in a WLAN are marked with this SSID. Wireless media can be very busy, and wireless devices limit the number of superfluous frames that they must process by accepting only frames marked with the SSID of their WLAN.
It is important to understand the relationship between SSIDs and BSSIDs. An SSID identifies a WLAN; the two are connected with a one-to-one correspondence. As a MAC address, a BSSID identifies an RP in that WLAN—one of the perhaps many RPs that offer wireless stations a connection to that WLAN.

Like switches that can carry traffic for multiple VLANs, most RPs, including the ProCurve RPs, can support multiple WLANs, each of which is identified by its own SSID.

An RP can identify itself with a unique BSSID in each WLAN. This provides the greatest flexibility in configuring the WLAN. The RP can also carry traffic for multiple WLANs on the same BSSID. The SSIDs for these WLANs are said to “share” the BSSID.

Each ProCurve RP 210 provides four separate BSSIDs. The ProCurve 220 and 230, which include two built-in radios, provide eight BSSIDs, four on each radio. Up to four SSIDs can share each BSSID, which means that each RP radio can support up to 16 WLANs. In Figure 1-21, SSID A (WLAN 1) and SSID E (WLAN 5) share BSSID 1 on each RP radio.

![Diagram of SSID and BSSID on ProCurve RPs](image-url)
Introduction
Radio Ports

The two radios on a single RP generally support the same WLANs, as shown in Table 1-5. However, using advanced mode configuration, you can enable different WLANs on an RP's two built-in radios; in this case, a single RP with two radios can support up to 32 WLANs. Using advanced mode configuration raises several concerns that are discussed in Chapter 4: "Wireless Local Area Networks (WLANs)."

Note

Although, a single RP can support up to 32 WLANs, the Wireless Edge Services zl Module can support up to 256. You must use advanced mode configuration to enable different WLANs on RPs.

Table 1-5.  BSSIDs and WLANs on the ProCurve RPs

<table>
<thead>
<tr>
<th>ProCurve RP</th>
<th>BSSID</th>
<th>WLANs (Normal Mode)</th>
<th>WLANs (Advanced Mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>210</td>
<td>4</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>220</td>
<td>8 (4 on each radio)</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>230</td>
<td>8 (4 on each radio)</td>
<td>16</td>
<td>32</td>
</tr>
</tbody>
</table>

Beaconing

An RP broadcasts beacon frames to announce its presence to wireless stations. In an open system, a beacon includes the SSID for a WLAN to which the RP offers a connection, as well as other information about the WLAN such as:

- the authentication and encryption method
- a timestamp for synchronization
- supported data rates and parameters for signaling frequencies
- the interval at which stations should expect beacons
- the delivery traffic indication message (DTIM), which informs power-saving stations whether they must “wake up” to receive buffered packets
- priority queue settings if WMM is used

In a closed system, beacons include all this information except the SSID, which stations must send in a probe request before they can associate to the WLAN.

The destination address for a beacon is the broadcast address. The source address is the BSSID on which the RP carries traffic for the WLAN.
If the RP supports multiple WLANs, it may send different beacons, each containing a different SSID. However, the RP can transmit only as many different beacon frames as it has BSSIDs. This means that even if a ProCurve RP supports more than four WLANs, it can advertise only the first four.

For example, WLAN 1 and WLAN 5 have been assigned to the same BSSID. The RP advertises the SSID for WLAN 1 in the beacon frame from that BSSID, but not the SSID for WLAN 5. However, if a wireless station sends a probe request for WLAN 5’s SSID, then the RP responds, and the station can associate. In other words, WLAN 1 operates in open system, and WLAN 5 operates in closed system.

**Note**

By default, ProCurve RPs beacon the first WLAN assigned to a BSSID; however, you can configure that WLAN to operate in closed system instead. You cannot configure a WLAN with an index number higher than four to operate in open system (unless you use advanced mode configuration to assign that WLAN as the primary WLAN). For more information about configuring open and closed system operation, see Chapter 4: “Wireless Local Area Networks (WLANs).”

**RP Modes**

The ProCurve RPs typically act in master mode, the default mode for an AP. Of course, because the RPs are part of a coordinated solution, the Wireless Edge Services zl Module controls the RPs’ functions.

You can also configure an RP radio to act in detector mode.

**Master Mode**

As mentioned earlier, BSSs and ESSs operate in infrastructure mode: wireless stations must communicate through their RP. In this mode, 802.11 requires that wireless stations and RPs function differently. The wireless stations act in managed mode, and the RPs in master mode. All communications must proceed between the master and the managed stations or between a managed station and the master.

You should understand the basic functions that the RP, as the master, fulfills:

- It sends beacon frames to:
  - announce its presence
  - advertise the WLANs that it supports
  - perform other network control functions, such as synchronizing the time
It receives authentication requests, which the Wireless Edge Services zl Module forwards to the authentication server.

It receives association requests from wireless stations, which it forwards to the Wireless Edge Services zl Module for response.

It receives data traffic from associated wireless stations and forwards this traffic to an upstream Ethernet device, or if permitted, to other wireless stations.

It forwards return traffic to associated wireless stations.

Masters communicate with managed stations; they do not communicate with each other. In other words, one RP does not send traffic to another RP, but simply transits traffic from wireless stations toward the Wireless Edge Services zl Module and from the module back to wireless stations.

The Wireless Edge Services zl Module collects traffic from one or more RPs. It is this module's role to process this traffic, respond to it, apply appropriate controls to it, and forward it in the correct uplink VLAN in the Ethernet network.

The module also acts as the authenticator, managing responses to stations' authentication requests and forwarding users' credentials to a RADIUS server.

Detector Mode

Typically, ProCurve RPs function as masters within one or more WLANs. However, you can also assign an RP the role of detector: such an RP scans for other APs in the vicinity.

More precisely, you assign an RP radio the role of detector. For example, a dual-radio RP could use one radio to support wireless stations and one to detect APs.

The detector is dedicated to scanning for unauthorized APs, which can threaten the security of your network. Unauthorized APs fall into two types:

- APs placed by unauthorized personnel without malicious intent.
  
  For example, employees might introduce APs so that they can connect to the network more conveniently. Although the employees may not mean any harm, if these APs are not secured, those who do mean harm can exploit the vulnerability.

- APs placed by hackers with malicious intent.
  
  Hackers can use rogue APs to lure users into sending them their passwords and other sensitive information. They can also hijack your network devices for illegal activities, opening your organization up to legal sanctions.
You can configure two types of detectors to search for these unauthorized APs:

- single-channel detector
- dedicated detector

The single-channel detector listens passively for beacons from APs. It listens only on its own radio channel and can simultaneously respond to association requests from wireless stations.

The dedicated detector, on the other hand, does not respond to association requests from wireless stations. Instead, the dedicated detector sends probes on each channel:

- used by its 802.11 mode
- allowed by the regulatory rules in its country

For instructions on configuring a radio as a detector, see Chapter 12: “Wireless Network Management.”

Configuring the ProCurve RPs

The RPs 210, 220, and 230 do not include a management interface. You configure these devices by configuring the Wireless Edge Services zl Module, which automatically deploys configurations to adopted RPs.

For example, if you want to specify the country code so that an RP can activate its radio, you must do so from the Wireless Edge Services zl Module. If you want RPs to support a WLAN, then you configure and enable that WLAN on the Wireless Edge Services zl Module. The Wireless Edge Services zl Module deploys the WLAN configuration to all adopted RPs, so you can quickly configure a consistent wireless service set throughout your entire network.

A radio configuration includes settings such as:

- **Country code**—The country code programs the radio to use channels and transmission powers according to your country’s regulatory restrictions.

- **Channel**—You can set a channel manually, or you can specify a method such as automatic channel select (ACS) that radios use to choose their own channel.

- **Power**—The power determines the radio’s signal strength. You might lower this power when using external antennas or placing RPs close to each other.

- **Data rate sets**—On 802.11bg radios, the data rate set determines whether the radio supports both 802.11b and 802.11g stations or only 802.11g stations.
Advanced radio settings—You will learn more about these options in Chapter 3: “Radio Port Configuration.”

WLAN assignment—When you enable a WLAN, the Wireless Edge Services zl Module automatically configures radios to support that WLAN. It creates a radio configuration that specifies which SSIDs should be assigned to which of the radio’s BSSIDs.

Note

If you use advanced mode configuration, then you must manually specify the WLAN assignment for a radio configuration.

The module deploys configurations in two ways:

- It deploys a radio adoption default configuration to any newly adopted RP radio.
- It deploys override configurations to targeted radios.

Therefore, you can configure radio settings in two ways: for all RP radios or for particular radios.

The Wireless Edge Services zl Module handles all WLAN settings. Indeed, one of the advantages of the Wireless Edge Services zl Module is that you can more quickly and easily establish a WLAN throughout an entire wireless network. (If necessary, you can use advanced mode configuration to disable a WLAN on a particular RP. See Chapter 4: “Wireless Local Area Networks (WLANs).”)

Note

Do not confuse the module's configuration with the RPs’ configurations. You configure settings on the module, many, but not all of which, it pushes down to RPs.

Radio Adoption Default Configurations

The Wireless Edge Services zl Module stores two radio adoption default configurations, one for 802.11a radios and one for 802.11 bg radios. In this way, each type of radio receives the correct channel, data rate sets, and other settings that may differ according to the 802.11 mode.

When a new RP is adopted, the module sends it the default configuration for its radio type. (If the RP has two radios, the module sends both configurations.)

The factory default configuration for the Wireless Edge Services zl Module already includes the two radio adoption default configurations, with the settings shown in Table 1-6. Note, however, that the configurations do not yet include the country code, which you must set before the module can deploy them.
Table 1-6. Factory Default Settings for Radio Adoption Default Configurations

<table>
<thead>
<tr>
<th>Setting</th>
<th>802.11a</th>
<th>802.11bg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placement</td>
<td>Indoors</td>
<td>Indoors</td>
</tr>
<tr>
<td>Channel</td>
<td>Random</td>
<td>Random</td>
</tr>
<tr>
<td>Power</td>
<td>Depends on country code</td>
<td>Depends on country code</td>
</tr>
<tr>
<td>Rate settings (in Mbps)</td>
<td>Basic: 6, 12, 24</td>
<td>Basic: 1, 2, 5.5, 11</td>
</tr>
<tr>
<td></td>
<td>Supported: 6, 9, 12, 18, 24, 36, 48, 54</td>
<td>Supported: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>Antenna mode</td>
<td>Diversity</td>
<td>Diversity</td>
</tr>
<tr>
<td>Maximum stations</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>RTS threshold (bytes)</td>
<td>2346</td>
<td>2346</td>
</tr>
<tr>
<td>Beacon interval (microseconds)</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>DTIM period (beacons)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Self healing offset</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

In the Web browser interface, you change these configurations from the Network Setup > Radio Adoption Defaults screen, as described in Chapter 3: “Radio Port Configuration.” You can then save these settings as customized radio adoption default configurations.

If you make a change to the radio adoption default configuration, the change only takes effect for newly adopted RPs.

The default configuration does not include WLAN assignments until you manually enable one or more WLANs. With normal configuration, the radio adoption default configuration always takes the settings shown in Table 1-7. The module redeploy the new WLAN assignments every time that you enable or disable a WLAN.
Table 1-7. Radio Adoption Default Configuration WLAN Assignment

<table>
<thead>
<tr>
<th>Setting</th>
<th>802.11a / 802.11bg</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID 1</td>
<td>SSIDs for: WLAN 1 (5, 9, 13)</td>
</tr>
<tr>
<td>BSSID 2</td>
<td>SSIDs for: WLAN 2 (6, 10, 14)</td>
</tr>
<tr>
<td>BSSID 3</td>
<td>SSIDs for: WLAN 3 (7, 11, 15)</td>
</tr>
<tr>
<td>BSSID 4</td>
<td>SSIDs for: WLAN 4 (8, 12, 16)</td>
</tr>
</tbody>
</table>

You can use advanced mode configuration to change these settings. See Chapter 4: “Wireless Local Area Networks (WLANs).”

Specific Radio Configurations

The radio adoption default configuration acts as a template for all adopted RP radios. However, many situations could require different settings for different RP radios. For example, you might install an external antenna on an RP, so you must configure a different antenna mode and power for it. You might want a radio in one area to support only the higher data rates of 802.11g, but a radio in another area, which includes 802.11b stations, to operate in mixed mode. Or, you might want to dedicate a single RP as a detector.

In such circumstances, you can configure settings that apply only to a particular radio or radios. The module then deploys this new configuration to the targeted radios.

Note

You can target an RP radio for override settings only if the RP has been detected by the Wireless Edge Services zl Module, although the RP does not actually have to be adopted. When the RP is adopted, the module sends the override configuration to its radio, rather than the radio adoption default configuration. A radio configured before the RP is adopted is said to have a static index type. Radios adopted with the default configuration have a dynamic index type.
You configure settings for particular radios from the **Network Setup > Radio** screens, as described in Chapter 3: “Radio Port Configuration.” The Wireless Edge Services zl Module still automatically manages WLAN assignments for these radios (unless you are using advanced mode configuration).

**Note**

The Wireless Edge Services zl Module associates the radio’s MAC address with the override configuration, so it persists even if the RP is powered down.

Communications Between an RP and the Wireless Edge Services zl Module: Layer 2 and Layer 3 Adoption

The Wireless Edge Services zl Module must communicate with RPs in order to control the wireless network. It must:

- adopt RPs
- deploy configurations to RPs, including radio settings, WLAN assignments, and WLAN settings
- forward traffic that is part of wireless users’ sessions to and from RPs
- collect information from RPs

A module communicates with all of its adopted RPs. An RP is adopted when the module identifies it and assumes responsibility for managing it.

When first powered up, an RP transmits three types of messages continuously until it is adopted:

- **LLDP messages**—signal the RP’s presence to a Wireless Edge Services zl Module. You can customize the LLDP name for individual RPs or for all RPs adopted by a module.
- **Hello messages**—signal the RP’s presence and desire to be adopted. The hellos, which are Layer 2 broadcasts, ensure that the Wireless Edge Services zl Module detects the RP even if intervening switches do not support LLDP.
- **802.1X EAP messages**—authenticate the RP to the network (see “802.1X Client” on page 1-74 for more information).

The Radio Port VLAN must be properly established in order for the discovery messages to reach the module. (See “Communicating with RPs: Radio Port VLANs” on page 1-8 or the *Getting Started Guide* for the ProCurve Wireless Edge Services zl Module.)
If you must place your RP on a different subnetwork from the Radio Port VLAN, the messages listed above fail to receive a response from the Wireless Edge Services zl Module. The RP initiates Layer 3 adoption, sending these messages:

- **DHCP messages**—request an IP address and other options such as a default gateway, a DNS server address, a domain name, and private option 189 (which specifies up to three IP addresses for Wireless Edge Services zl Modules).
Introduction
Radio Ports

- **DNS requests**—request the IP address for the Wireless Edge Services zl Module. If the RP does not receive option 189 from the DHCP server, it uses DNS to discover the module’s IP address. At its factory settings, the RP requests the IP address for this hostname: PROCURVE-WESM. The RP also adds the domain suffix that it received in the DHCP configuration. For example:

  PROCURVE-WESM.procurve.com

  If your Wireless Edge Services zl Module uses a customized hostname, you must first adopt the RP at Layer 2. After a module adopts the RP, you can change the hostname for which the RP sends the request. You can then install the RP in its final location, and the RP can find the module with the customized hostname.

- **Hello messages targeted to the module’s IP address**—request that the Wireless Edge Services zl Module adopt the RP. The RP is adopted on the VLAN on which the module receives the message, which is usually one of the module’s uplink VLANs. (If so, do not tag this VLAN on the module’s downlink port: the uplink and downlink ports must never carry the same VLANs.) Remember that because the RP is on a different subnetwork than the module, the RP’s DHCP configuration must include a default gateway that can route the RP’s messages to the module.

  Figure 1-23 shows the messages that an RP sends as part of Layer 3 adoption.
Figure 1-23. Layer 3 Adoption
When a Wireless Edge Services zl Module receives an adoption request from an unadopted RP—whether as a broadcast or as a targeted message—the module must decide whether or not to adopt the RP.

You can configure the module to automatically adopt any identified, nonconfigured RP. The simple plug-in installation makes this option ideal, as long as your organization secures access to its network devices. In a less secure environment, you should configure the module to adopt only those RPs for which you manually specify the MAC address. (You can also use port authentication to secure your network. See “802.1X Client” on page 1-74.)

After adopting the RP, the module deploys the radio adoption default configuration to it, and the RP can begin functioning in your network, as shown in Figure 1-22.
Managing RPs in a Self-Healing Network

A Wireless Edge Services zl Module collects a variety of information from managed RPs. For example, RPs configured as detectors report information about neighboring APs. The module then processes this information into lists of authorized and unauthorized APs, according to rules that you configure.
The Wireless Edge Services zl Module also collects information about the wireless network in order to improve its functioning. For example, if you enable interference avoidance, the module has RPs change their channel when they report excessive congestion.

Intrusion detection is one useful self-healing feature. The Wireless Edge Services zl Module can also implement neighbor recovery and create a highly availability, self-healing network. That is, when one RP fails, nearby RPs automatically come to the aid of that RP’s stations by raising their transmit power, among other actions. For more information on network self-healing capabilities, see Chapter 12: “Wireless Network Management.”

**802.1X Client**

A secure network often enforces port authentication such as 802.1X: a device must prove that it is legitimate before it can even connect to the network. The danger posed by a rogue RP connecting to your network is minimized by the fact that the RP must accept the settings configured on your Wireless Edge Services zl Module. However, it is a good idea to enforce 802.1X authentication on all physically accessible switch ports, and if you connect your RPs to such ports, they must be able to authenticate themselves to the network.

The RPs 210, 220, and 230 include an 802.1X client for such authentication. Using Message Digest 5 (MD5) authentication, the client automatically sends the RP’s credentials when the RP connects to a network device that requires port authentication. The switch to which the RP connects forwards the credentials to an authentication server and, if they are correct, allows the RP to join the network.

The authentication server may store a VLAN setting for the RP and sends this VLAN setting to the switch after the RP authenticates. Such dynamic configuration of the Radio Port VLAN can replace auto-provisioning on the wireless services-enabled switch or manual configuration on an infrastructure switch. (For more information about configuring Radio Port VLANs, see “Communicating with RPs: Radio Port VLANs” on page 1-8.)

The default username and password on all ProCurve 200 Series RPs are admin and procurve, respectively.

ProCurve Networking suggests that you change these settings, using a Wireless Edge Services zl Module to load new credentials on your organization’s RPs. You can then move these RPs to their final locations and be sure that they can authenticate and connect to your network. (To learn how to configure RPs’ 802.1X username and password, see Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)
RP Deployment Requirements

This section provides a brief overview of features on the ProCurve RPs that affect their deployment. For information about installing your RPs, refer to the appropriate *Installation and Getting Started Guide*.

Power over Ethernet (PoE)

PoE, based on the IEEE 802.3af standard, defines a mechanism by which a device receives power over the Ethernet cable on which it also sends and receives data.

ProCurve RPs 210, 220, and 230 must be powered by PoE. The RPs operate at 48 V and typically draw about 7 W of power.

An RP can connect to:
- a 10/100 Ethernet port on a PoE module in your wireless services-enabled switch
- a 10/100 Ethernet port on an 802.3af-compatible PoE switch, such as a ProCurve 2600-PWR
- an 802.3af-compatible PoE injector

The source can be up to 100 meters away.

You should use a CAT 5 cable for the connection. The devices use LLDP-MED to automatically communicate power requirements to the power source.

Antennas

The ProCurve RPs 210 and 230 have internal omnidirectional antennas, which can provide up to 20 decibel milliwatts (dBm) of power. The actual maximum power allowed in your region may vary.

You cannot install external antennas on the RPs 210 and 230.

The ProCurve RP 220, on the other hand, requires an external antenna. For more information about purchasing and installing antennas, refer to the manuals for the RP 220, available at [http://www.procurve.com](http://www.procurve.com).
Redundancy Groups

A good network design builds in redundancy so that, in the unlikely event of a hardware or link failure, users continue to access the resources that they need. To provide redundancy for your wireless network, you can create a redundancy group using various combinations of the following two modules:

- the Wireless Edge Services zl Module (J9001A)
- the Redundant Wireless Services zl Module (J9003A)

Because new members of a redundancy group add failover capabilities, processing power, and throughput, *but not licenses*, the most typical design includes a single primary module and one or more redundant modules. In addition to enabling high-availability, a redundancy group can serve these functions:

- **adding capacity**—You can configure the redundant modules to be active at all times, not only when the primary module fails. In this case, the modules load balance the groups’ RPs between them. Each module adds 400 Mbps of throughput, which might be important in a busy network.

- **providing seamless Layer 2 roaming for Web-Auth**—See “Roaming Between RPs on Different Wireless Edge Services zl Modules at Layer 2” on page 1-82 for more information about this feature.

**Redundant Wireless Services zl Module**

The Redundant Wireless Services zl Module (J9003A) is designed primarily to provide cost-effective failover capabilities. The redundant module provides the same capabilities as the Wireless Edge Services zl Module, or primary module, with one exception: the redundant module does not include any RP licenses, and you cannot add licenses to it. Instead, the redundant module is authorized to use the primary module’s licenses in certain situations, which are discussed later in this section.

To enable a redundant module to back up one or more primary modules that are installed in the same or in different wireless services-enabled switches, you must configure the modules as part of a redundancy group. The redundant module can then use a primary module’s RP licenses to adopt RPs in various circumstances (which depend on the redundant module’s operation mode as described later in this section).
Rules of Redundancy Groups

A redundancy group consists of up to 12 members; each member is either a primary module or a redundant module. Up to two modules can be installed in the same wireless services-enabled switch.

Within the redundancy group, you can combine primary and redundant modules in any proportion. For example, you could have two primary modules and one redundant module; or you could group three primary modules and four redundant modules. However, because only primary modules have RP licenses, the group must include at least one primary module.

When designing a redundancy group, you must consider RP licenses. A redundancy group shares RP licenses. Any member of the group can draw on the group’s licenses to adopt RPs (although the member’s operation mode determines when the member can actually use the RP licenses).

The total number of RPs that a redundancy group can adopt is set by the group authorization level, which matches the authorization level of the single group member with the greatest number of licenses. Members’ licenses are not added together.

For this reason, it is recommended that a redundancy group be based on a single primary module. If you want to add more modules to the group, add another redundant module rather than another primary module.

For example, suppose that a group includes these members:

- one Wireless Edge Services zl Module with the default license (supporting 12 RPs) and one additive license (supporting 48 RPs)
- one Wireless Edge Services zl Module with the default license (supporting 12 RPs)
- one Redundant Wireless Services zl Module

This redundancy group has two RP licenses and a group authorization level for 60 RPs. The second primary module did not contribute its licenses, so you could add the same capabilities by adding a second redundant module.

The following group is the recommended group:

- one Wireless Edge Services zl Module with the default license and optional additive licenses (supporting a maximum total of 156 RPs)
- one or more Redundant Wireless Services zl Modules
Redundancy Group Operation Modes

Group members can operate in either active mode or standby mode. The type of module (primary or redundant) has no relation to the operation mode. You can place a primary module in standby mode, or more typically, you can place a redundant module in active mode. An active redundant module adds capacity by loading balancing RPs with other members of the group. (Remember it does not add capacity by increasing the number of RPs that can be adopted.)

An active member can adopt RPs at any time. If a group has more than one active member, together the active members can adopt as many RPs as allowed by the group authorization level (see “Rules of Redundancy Groups” on page 1-77.)

Like active members, standby members adopt RPs using any available group RP licenses. However, a standby member can adopt RPs only when:

- it does not receive heartbeats from the active member for too long a period
- the active member fails to adopt an RP

Thus, when necessary, one of the standby members can assume the active module's services, and wireless services continue after a minimum of delay.

Table 1-8 describes some of the situations in which a standby member adopts RPs.

**Table 1-8. Situations in Which a Standby Member Adopts RPs**

<table>
<thead>
<tr>
<th>Situation</th>
<th>Possible Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The standby member does not receive heartbeats from any one of the active members.</td>
<td>• The active member has failed.</td>
</tr>
<tr>
<td></td>
<td>• The wireless services-enabled switch in which the active member is installed has failed.</td>
</tr>
<tr>
<td></td>
<td>• A failed network connection has isolated the active member from the rest of the network.</td>
</tr>
<tr>
<td>All active members fail to adopt an RP.</td>
<td>• The active member’s internal downlink port has not been tagged for the Radio Port VLAN.</td>
</tr>
<tr>
<td></td>
<td>• The network infrastructure does not support the Radio Port VLAN on all interfaces between the RP and the active member.</td>
</tr>
<tr>
<td></td>
<td>• The active member is explicitly prohibited from adopting the RP.</td>
</tr>
</tbody>
</table>

Figure 1-25 illustrates a situation in which a standby member adopts RPs.
To provide consistent service, the standby member continues to support the RPs even after the active member comes back up.

Figure 1-25. Redundancy Module Adopting RPs
Remember that standby members support all the same services as the active members, so you must configure the same wireless settings on all members of a redundancy group. A simple way to ensure successful failover is to upload one module's configuration onto each other module, edit the configuration with module-specific settings (such as IP address and redundancy group settings), and save the edited configurations.

A special feature of the Wireless Edge Services zl Module CLI gives you another option. After establishing a redundancy group, you can access the redundancy group configuration mode context through the CLI of one of the members of the group. Any configurations entered from this mode context are pushed to all members of the group. You can also create a text file offline and copy the file into the CLI in the redundancy group configuration mode context. The text file can include individual settings for a particular module and settings that apply to all members of the group.

For instructions on configuring redundancy groups, see Chapter 10: “Redundancy Groups.”

**Note**

You can configure multiple modules as active members of the group. Because only one module adopts any given RP, the modules balance RPs among them as described in Chapter 10: “Redundancy Groups.”
Layer 2 and Layer 3 Roaming Between RPs and Modules

One of the principle attractions of wireless networking is the mobility that it offers users, and users often want to roam further than the range of a single radio. The 802.11 standard gives guidelines for roaming between the coverage areas, or cells, provided by two APs (or RPs), but leaves the implementation largely to the makers of wireless network interface cards (NICs).

Typically, a station monitors the signal strength of beacons from its AP. When the signal fades below a certain level, the station looks for another AP that supports the same SSID (WLAN) but has a stronger signal. The station then disassociates from the first AP and associates to the second.

For roaming, you must consider the speed of the roam and also whether, during and after the roam, the station can preserve its IP address and active sessions.

The actual process of reassociating is very fast, but other requirements for connecting to a WLAN can slow roaming. For example, an AP might require users to authenticate to the network with 802.1X. Without special provisions, the AP does not realize that the user has already completed this authentication with another AP. To speed up roaming, developers design ways to get the information necessary for connecting a station to an AP before the station needs to roam to that AP:

- APs can communicate necessary information to each other.
- Wireless stations can complete some association and authentication requirements before they actually roam.

The Wireless Edge Services zl Module supports many of these mechanisms. In addition, by its very nature as a controller of coordinated RPs, the module enables fast roaming between its own RPs.

Roaming Between RPs on a Single Wireless Edge Services zl Module

ProCurve Networking’s coordinated AP solution facilitates fast and seamless roaming between wireless cells. A central device, the Wireless Edge Services zl Module, controls all security settings and associations with wireless stations. The module generates and encrypts 802.11 frames and monitors a station’s authentication state.
In other words, the module functions much like a single, high-capability AP with many remote radios (the RPs). Therefore, when a station disassociates from one RP and reassociates with another RP adopted by the same module, the module already has in place the association, the authentication, and the encryption keys. The roam is fast and seamless.

The Wireless Edge Services zl Module also supports these 802.11i mechanisms for speeding up roaming in a WLAN that requires WPA/WPA2 with 802.1X:

- **Pairwise Master Key (PMK) caching**—enables fast roaming between RPs.

  WPA's TKIP (and WPA2's CCMP) derive encryption keys from a unique PMK for each association. This key is necessary for the station and the module to communicate. PMK caching allows the module to store a station's PMK after the station disassociates with an RP so that the key is still in place if the station then associates with a new RP.

- **Opportunistic key caching**—facilitates fast roaming to a new RP.

  The station attempts to use the same PMK that it used for one RP with another. As long as the same module has adopted both of the RPs, the PMK works.

No matter which security options you have enabled on a WLAN, a station can quickly roam (under 50 milliseconds) between two RPs adopted by the same module.

### Roaming Between RPs on Different Wireless Edge Services zl Modules at Layer 2

The same factors that affect roaming between APs (outlined in “Layer 2 and Layer 3 Roaming Between RPs and Modules” on page 1-81) apply to roaming between RPs adopted by different Wireless Edge Services zl Modules. Without special provisions, the two modules operate as separate entities, each forcing the user to complete all necessary steps to connect. In some cases, the roam still occurs quickly and seamlessly, but in other cases it is slowed by authentication requirements.
However, Wireless Edge Services zl Modules supports these mechanisms to facilitate and speed roaming between RPs adopted by different modules:

- **PMK caching**—enables fast roaming back to a module in a WLAN that requires WPA/WPA2 with 802.1X.

  A station disassociates from one of the module’s RPs and moves to an RP on a different module. As far as the first module knows, the station has left the WLAN. However, the module stores the station’s PMK. If the station returns to an RP on the first module, the key is ready, and the station can quickly connect.

- **Pre-authentication**—enables fast roaming for the first time to a module in a WLAN that requires WPA/WPA2 with 802.1X.

  PMK caching speeds roaming only if the Wireless Edge Services zl Module already has a PMK for the station. To create this PMK, the station must complete 802.1X authentication. Traditionally, 802.1X authentication occurs only when the station actually associates to one of the module’s RPs. To speed roaming, the station can complete 802.1X authentication to a module in advance before roaming. The module caches the PMK until the station actually roams to it.

- **Redundancy groups**—enables fast and seamless roaming between modules in a WLAN that requires Web-Auth.

  The Wireless Edge Services zl Modules that compose a redundancy group exchange various messages. Some of these messages can include Web-Auth usernames and passwords. When a user enters his or her username and password into a Web-Auth login screen, the module enforcing Web-Auth retrieves these login credentials and submits them to a RADIUS server. The module also sends the credentials to all other members of the redundancy group. The other members submit the credentials to the RADIUS server and log in the user. When the user's station roams to an RP on a new module, the module has already authorized it to forward traffic, so the roam is fast and seamless.

---

**Note**

Pre-authentication functions only between two Wireless Edge Services zl Modules that are on the same VLAN. In fact, roaming between modules on different VLANs requires special configurations discussed in the next section.

For more information about these mechanisms, see Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility” and Chapter 4: “Wireless Local Area Networks (WLANs).”
Roaming Between RPs on Different Wireless Edge Services zl Modules at Layer 3

Roaming always occurs within a WLAN—that is, a station can roam only to another RP if that RP supports the same SSID. Otherwise, the station does not roam; it connects to a new network.

For the roaming described in the previous sections, the roaming station’s traffic arrives in the same VLAN when it is bridged into the Ethernet network. This allows the station to keep the same IP address and maintain active sessions. Roaming between two wireless cells but within the same VLAN on the wired side is called radio frequency (RF), or Layer 2, roaming.

Whenever possible, you would configure all of your modules to support the same VLAN for the same WLAN, and all roams would be at Layer 2. However, two Wireless Edge Services zl Modules separated by a router must forward wireless traffic into different VLANs, complicating the roaming process. When a station roams to an RP adopted by a different module, the station’s IP address is no longer valid, and the station loses its active sessions.

Wireless Edge Services zl Modules use network, or Layer 3, roaming to solve this problem. Figure 1-26 illustrates a network that requires Layer 3 roaming. The module on the left places wireless stations in WLAN A in VLAN 1 while the module on the right places stations in WLAN A in VLAN 20.
Introduction

Layer 2 and Layer 3 Roaming Between RPs and Modules

Figure 1-26. Network Requiring Layer 3 Roaming

Note

It is important that the difference in subnetwork be reflected in different VLAN IDs because Layer 3 roaming relies on a changing VLAN ID to detect a Layer 3 roam. In other words, the two modules in Figure 1-26, which are in different subnetworks, correctly place WLAN A traffic on different VLANs. If both used the same VLAN ID, the modules would treat roaming between their RPs as Layer 2 roaming and the roaming would not be seamless.

To implement Layer 3 roaming, Wireless Edge Services zl Modules perform these functions:

- **Establish a Layer 3 mobility domain**—A domain can include up to 12 modules, or peers, each of which can support up to 500 stations. Every station has a home module (HM) and a current module (CM). The HM is on the same VLAN as the station, and the station is currently associated to the CM; the two modules might be the same device.
Introduction
Layer 2 and Layer 3 Roaming Between RPs and Modules

- **When necessary, tunnel traffic back to a station’s HM**—Every module in the Layer 3 roaming domain establishes a tunnel to every other module. A module tunnels traffic only when necessary, which is when a station that has an HM on a different VLAN roams to the module. If a station that has an HM on the same VLAN roams to the module, the module simply becomes the station’s new HM. This provisions eliminates unnecessary and inefficient tunneling.

Wireless Edge Services zl Modules’ Layer 3 roaming capabilities provide seamless roaming (sessions maintained) between RPs on different modules regardless of the security options on the WLAN. However, fast roaming at Layer 3 is not supported except when modules implement a redundancy group and Web-Auth. For more information about roaming, see Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility.”
# Configuring the ProCurve Wireless Edge Services zl Module

## Contents

Management Interfaces  ...................................................... 2-5

The Web Browser Interface ................................................... 2-5
  - Determining the Dynamic IP Address or Assigning a Static Address  ........................................ 2-6
  - Accessing the Web Browser Interface ..................................... 2-9
  - Logging In to the Web Browser Interface  ................................ 2-11
  - Overview of the Web Browser Interface  .................................... 2-12
  - Applying or Saving Changes ................................................ 2-12
  - Logging Out or Refreshing the Screen .................................... 2-14
  - Accessing the Online Help .................................................. 2-14
  - Using Filtering Options .......................................................... 2-16

CLI ................................................................. 2-21
  - Accessing the Switch CLI Through a Serial Session  ............... 2-21
  - Accessing the Switch CLI Through a Telnet or SSH Session  .......... 2-22
  - Accessing the Wireless-Services Context ................................ 2-22
  - Navigating the CLI ........................................................... 2-22
  - Saving Changes to the startup-config .................................... 2-23
  - CLI Commands ................................................................. 2-23

Security ............................................................. 2-24
  - SSH Access ................................................................. 2-24
  - HTTPS Access .............................................................. 2-24
  - SNMP Support ............................................................... 2-24

2
Configuring the ProCurve Wireless Edge Services zl Module

Contents

Controlling Management Access to the Module ....................... 2-27
   Enabling HTTP and HTTPS Access to the Module ............. 2-27
   Choosing SNMP Versions ...................................... 2-29
   Setting Up the Internal FTP Server ........................... 2-32
   Changing the Password for the Default SNMP v3
      Users (Operator or Manager) .............................. 2-35
   Configuring Web-Users .................................... 2-40

Logging In to the Module as a WebUser Administrator ............ 2-49
   Creating Guest Accounts on the Local RADIUS Database ... 2-50
   Viewing and Deleting Guest Accounts ....................... 2-53
   Printing Records of Guest Accounts ........................ 2-55

Radio Port Adoption ........................................... 2-57
   Network Requirements for Layer 2 Adoption ................. 2-58
      Auto-Provisioning on the Wireless Services-Enabled Switch 2-58
      Attaching RPs to Infrastructure Switches ................ 2-59
   Network Requirements for Layer 3 Adoption ................. 2-62
      Enabling Layer 3 Adoption Through DHCP Option 189 ..... 2-65
      Enabling Layer 3 Adoption Through DNS Lookup .......... 2-67
      Verifying Layer 3 Adoption ................................ 2-69

Automatic or Manual Adoption of RPs .............................. 2-70
   Controlling Which Wireless Edge Services zl Module Adopts
      Particular RPs—Adoption Preference ID ................... 2-76
   802.1X Authentication for RPs ................................ 2-78
      Configuring 802.1X Authentication for RPs .............. 2-79

System Maintenance ............................................ 2-81
   Software Images ........................................... 2-81
      Viewing the Software Images .............................. 2-82
      Selecting the Software Image That Is Used to Reboot .... 2-83
      Changing the Image Failover Setting .................... 2-83
      Manually Updating the Software Image ................... 2-85
### Contents

- Configuration Files ........................................... 2-86
- Viewing Configuration Files ............................... 2-87
- Transferring, or Copying, Files ......................... 2-89
- Transferring Configuration Files from an FTP or TFTP Server to the Wireless Edge Services zl Module .......... 2-89
- Transferring Configuration Files from the Wireless Edge Services zl Module to Another Destination .................. 2-91
- Managing the Directory Structure and Browsing for Files ........................................ 2-95
- Deleting a Configuration File ............................. 2-97
- Returning the Startup-Config File to Factory Default Settings ........................................ 2-98
- Update Server .............................................. 2-98
- Checking the Software Image File ......................... 2-99
- Checking the Configuration File ......................... 2-99
- Avoiding Problems in Using the Update Server .......... 2-100
- Configuring the Update Server Settings .................. 2-104
- Password Encryption ........................................ 2-105
- SNMP Traps and Error Reporting ......................... 2-109
- SNMP Communities ....................................... 2-109
  - Modifying SNMP v2 Communities ....................... 2-110
- SNMP Statistics ........................................ 2-110
- SNMP Traps .............................................. 2-111
  - Enabling SNMP Traps .................................. 2-113
  - Disabling SNMP Traps .................................. 2-115
- Setting Thresholds ....................................... 2-116
- Sending Traps to an SNMP Receiver ...................... 2-117
- Radio Port Licenses .................................... 2-122
  - Installing or Uninstalling Licenses on a Wireless Edge Services zl Module ......................... 2-127
  - Registering on the My ProCurve Web Portal ........ 2-127
  - Understanding the Numbers: IDs and Keys .......... 2-128
- Installing RP Licenses ................................ 2-128
- Removing RP Licenses .................................. 2-132
- Redundancy Groups and RP Licensing .................. 2-135
- Setting System Information—Name, Time, and Country Code .... 2-136
Configuring the ProCurve Wireless Edge Services zl Module

Contents

Enabling Secure Network Time Protocol (NTP) .................................................................. 2-138
Secure NTP Overview ................................................................................................. 2-138
  NTP Modes and Communications ............................................................................ 2-139
  NTP Hierarchy ......................................................................................................... 2-139
  Secure NTP Enhancements ..................................................................................... 2-141
Configuring a Secure NTP Server .............................................................................. 2-142
  Configuring Secure NTP Options ............................................................................ 2-144
  Applying ACLs to NTP Services ............................................................................. 2-146
  Configuring Authentication for Secure NTP .......................................................... 2-148
  Configuring NTP Neighbors .................................................................................... 2-152
  Configuring the Wireless Edge Services zl Module as a Broadcast Server .......... 2-155
Viewing NTP Associations and Status ...................................................................... 2-158
Viewing Secure NTP Status ....................................................................................... 2-163
Digital Certificates .................................................................................................... 2-166
  Overview ................................................................................................................ 2-166
  Configuring Digital Certificates ............................................................................ 2-167
  Using the Certificates Wizard ................................................................................. 2-170
    Creating Certificates .............................................................................................. 2-171
    Uploading a Certificate to the Module .................................................................. 2-181
    Deleting Trustpoints, Certificates, and Keys ......................................................... 2-184
  Uploading a CRL to a Trustpoint ............................................................................. 2-187
  Transferring Trustpoints ......................................................................................... 2-187
    Transferring Trustpoints from the Wireless Edge Services zl Module to a Server . 2-188
    Transferring Trustpoints from a Server to the Wireless Edge Services zl Module . 2-189
Certificate Keys .......................................................................................................... 2-191
  Creating a Key ......................................................................................................... 2-191
  Transferring Keys .................................................................................................... 2-193
Management Interfaces

To configure and manage the ProCurve Wireless Edge Services zl Module, you can use one of the following management interfaces:

- **Web browser interface**—Accessed through a Web browser, this intuitive interface provides comprehensive information to help you manage and monitor your company's wireless services. The menus and online help guide you through configuration steps.

- **Command line interface (CLI)**—Available through a serial, Telnet, or Secure Shell (SSH) session, the CLI provides a complete set of commands to configure, manage, and troubleshoot your wireless services.

- **Simple Network Management Protocol (SNMP) applications**—SNMP applications allow you to manage your company's wireless services in the context of other network services. By default, the Wireless Edge Services zl Module supports SNMP v1, v2, and v3. As a result, you can use SNMP applications such as ProCurve Manager (PCM) Plus and ProCurve Mobility Manager (PMM) to manage your wireless services. (For more information about PCM Plus and PMM, visit ProCurve Networking's Web site at [http://www.procurve.com](http://www.procurve.com).)

Because the Web browser interface simplifies both management and configuration tasks, this guide focuses on using the Web browser interface.

The Web Browser Interface

To access the Web browser interface for the ProCurve Wireless Edge Services zl Module, your workstation must be running the Java Virtual Machine (JVM), which enables the Web browser to run Java applets. If your workstation is not running the JVM and you attempt to open the module's Web browser interface, the workstation will automatically try to access the Internet and download the JVM.

In addition to running JVM, the workstation that is running the Web browser must be able to reach the Wireless Edge Services zl Module's IP address.
Determining the Dynamic IP Address or Assigning a Static Address

Initially, you must access the Wireless Edge Services zl Module through the CLI of the wireless services-enabled switch zl—either to determine the IP address that is assigned to the module through a Dynamic Host Configuration Protocol (DHCP) server or to assign the module a static IP address.

By default, the module is configured to receive an IP address through a DHCP server. If you keep this default setting, you can simply access the CLI and determine the IP address dynamically assigned to the module. You can then use this IP address to access the Web browser interface and manage the module.

Alternatively, you can assign the module a static IP address (again through the CLI).

Access the Wireless Edge Services zl Module CLI. To access the Wireless Edge Services zl Module CLI, you must first access the CLI for the wireless services-enabled switch. You can use one of the following access methods:

- Serial session
- Telnet session
- SSH session

If you are connecting to the wireless services-enabled switch through a serial session, use the serial cable (5184-1894) that was shipped with the switch. Then run terminal session software such as Tera Term or HyperTerminal on your workstation, setting the following parameters for the session:

- Baud Rate = 9600
- Parity = None
- Data Bits = 8
- Stop Bits = 1
- Flow Control = None

If prompted for a password, enter the password for either the manager or the operator user on the wireless services-enabled switch.

Move to the wireless-services context by entering:

```
ProCurve# wireless-services <slot letter>
```
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Replace `<slot letter>` with the letter for the chassis slot in which the Wireless Edge Services zl Module is installed. For example, if the module is installed in chassis slot C, you would enter:

```
ProCurve# wireless-services c
```

You access the Wireless Edge Services zl Module CLI with the same rights (either manager or operator) that you have to the switch CLI. For example, when you enter `wireless-services <slot letter>` command from the switch enable mode context, you also enter the module enable mode context:

```
ProCurve(wireless-services-C)#
```

**Determine the IP Address Assigned by the DHCP Server.** If the Wireless Edge Services zl Module receives an IP address through a DHCP server, enter:

```
ProCurve(wireless-services-C)# show ip interface
```

The IP address and default gateway assigned to the default management interface is listed.

**Assign a Static IP Address.** If you want to assign a static IP address to the Wireless Edge Services zl Module, move to the global configuration context and enter the following commands:

```
ProCurve(wireless-services-C)# configure [terminal]
ProCurve(wireless-services-C) (config)# interface vlan1
ProCurve(wireless-services-C) (config-if)# ip address <A.B.C.D>/<prefix length>
```

Replace `<A.B.C.D>` with the IP address that you want to assign the Wireless Edge Services zl Module. Replace `<prefix length>` with the Classless Inter-Domain Routing (CIDR) notation. Do not include a space between the IP address and the prefix length.

**Specify a Default Gateway.** You should also configure a default gateway for the Wireless Services zl Module. The module directs all traffic destined to a different subnetwork to the gateway device, which routes the traffic.

To specify a default gateway for the Wireless Edge Services zl Module, exit to the global configuration context and enter:

**Syntax:** `ip default-gateway <A.B.C.D>`

Replace `<A.B.C.D>` with the IP address of the default gateway.
The command saves to the running-config as a default route in which the gateway IP address is the IP address of the next hop. For example, you enter:

```
ProCurve(wireless-services-C) (config)# ip default-gateway 10.1.10.1
```

The running-config displays:

```
ip route 0.0.0.0/0 10.1.10.1
```

**Note**

Be careful when you change the default gateway IP address. The Wireless Edge Services zl Module allows you to set more than one default gateway (and default route). However, only the gateway configured first is active. Therefore, you cannot change the gateway by simply re-entering the `ip default-gateway` command. Instead first delete the old gateway; then specify the new gateway. For example:

```
ProCurve(wireless-services-C) (config)# no ip default-gateway 10.1.10.1
ProCurve(wireless-services-C) (config)# ip default-gateway 10.1.12.1
```

Failure to follow this procedure can cause your module to lose connectivity.

**Set the Management VLAN Interface.** The example commands above assign an IP address to VLAN 1, the module’s default management interface. Your network might use a different management VLAN. In that case, you must assign the IP address to the VLAN you use and configure that VLAN as the management interface.

For example, in a network that defines VLAN 2 as the management VLAN, you would enter these commands from the global configuration mode context:

```
ProCurve(wireless-services-C) (config)# interface vlan2
ProCurve(wireless-services-C) (config-if)# ip address <A.B.C.D>/<prefix length>
ProCurve(wireless-services-C) (config-if)# management
```
Enable Secure Management. Secure management forces managers to access the Wireless Edge Services zl Module at the IP address configured on the management VLAN.

For example, you configure VLAN 2 as the management VLAN, and the module's IP address on VLAN 2 is 10.1.2.30. The module also has an IP address on VLAN 4, 10.1.4.30. By default, you can enter either IP address in your Web browser and access the module's Web browser interface. However, if you enable secure management, you must enter 10.1.2.30 in your Web browser.

Enter this command from the global configuration mode context to enable secure management:

```
ProCurve(wireless-services-C) (config)# management secure
```

Secure management filters management traffic according to the destination address only. In other words, in the example above, secure management forces you to manage the Wireless Edge Services zl Module through its IP address on VLAN 2. However, your management station could be on VLAN 4 and its traffic routed to VLAN 2. To restrict management access to devices in the management VLAN only, you must configure ACLs on the module's uplink port, on routing devices in your network, or on both.

Accessing the Web Browser Interface

You can access the Web browser interface in one of two ways:

- Enter the IP address (or hostname) assigned to the Wireless Edge Services zl Module as the URL in your Web browser
- Access the Web browser interface for the wireless services-enabled switch

Entering the IP Address in a Web Browser. Once you know the IP address assigned to the Wireless Edge Services zl Module, enter that address as the URL in your Web browser. For example, if you assigned the Wireless Edge Services zl Module the IP address 192.168.5.20, you would enter `http://192.168.5.20` as the URL in your Web browser. (On a module that has multiple IP addresses, you can enter any address, or—if you have enabled secure management—only the address on the management VLAN.)

The first time that you access the Web browser interface, a Security-Warning screen may be displayed, including the following warning: “The application’s signature is invalid. Do you want to run the applications?” Click the Run button to continue.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Accessing the Web Browser Interface for the Wireless Services-Enabled Switch. You can also access the module’s Web browser interface from the Web browser interface for the wireless services-enabled switch. (Like the module’s Web browser interface, the switch’s Web browser interface uses Java applets.) To access the switch’s Web browser interface, enter the IP address for the management interface as the URL in your Web browser. For example, if the management interface has the IP address 192.168.5.1, you would enter http://192.168.5.1.

Like other modules installed in the wireless services-enabled switch, the Wireless Edge Services zl Module is displayed on the switch graphic displayed on the Device View screen. To access this screen, click Configuration > Device View. (See Figure 2-1.)

![Figure 2-1. The Web Browser Interface for the Wireless Services-Enabled Switch](image)

To access the Web browser interface for the Wireless Edge Services zl Module, click the link for the module, as shown in Figure 2-1.
Logging In to the Web Browser Interface

Whichever way you attempt to access the Web browser interface, you are prompted to enter a username and password. (See Figure 2-2.)

![Figure 2-2. Logging In to the Module's Web Browser Interface](image)

In the **Username** field, enter **manager**, and in the **Password** field, enter the default password **procurve**. (The Wireless Edge Services zl Module also supports the operator user. For more information, see "Default SNMP v3 Users—Manager and Operator" on page 2-26.)

**Note**

To protect your network, ProCurve Networking strongly recommends that you immediately change the password for the manager and operator users. (See “Changing the Password for the Default SNMP v3 Users (Operator or Manager)” on page 2-35.)
Overview of the Web Browser Interface

The Web browser interface includes a navigation bar on the left. (See Figure 2-3.) Using this navigation bar, you can access:

- Information screens that help you manage and troubleshoot your wireless services
- Configuration screens that allow you to tailor wireless services for your particular environment

Figure 2-3. Example of a Configuration Screen

Applying or Saving Changes

When you use the Web browser interface to configure the Wireless Edge Services zl Module, these changes may affect two configuration files, depending on whether you apply or save changes:

- **startup-config**—When you save changes, these changes become part of the startup-config file, which is stored in non-volatile RAM (NVRAM) on the module's internal flash. When the Wireless Edge Services zl Module is rebooted, all of the configurations that are contained in the startup-config file are retained. During the reboot process, the module initializes the designated boot image software and then loads the startup-config.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

- **running-config**—When the Wireless Edge Services zl Module loads the startup-config, all the configurations become part of the running-config, which is held in RAM. When you make and apply configuration changes in the Web browser interface, these changes become part of the running-config as well. Unless you save the changes that you apply to the running-config, these changes are *not* retained when the Wireless Edge Services zl Module is rebooted.

**Applying Changes to the running-config.** You can make and apply configuration changes to the running-config in different ways:

- **Apply** button—On some configuration screens, you make configuration changes and then click the **Apply** button.
- **Enable** button—In some instances, you enable functionality by clicking the **Enable** button. To deactivate the functionality, you click the **Disable** button.
- **OK** button in **Add** or **Edit** screens—To add information or edit configurations, you click the **Add** or **Edit** button, make configuration changes on the screen that is displayed, and then click the **OK** button. (In some cases you can delete specific configurations by clicking the **Delete** button.)

After you enter changes in a configuration screen but *before* you click one of these buttons, you have the option of backing out, or deleting, the changes. To back out changes not yet applied to the running-config, click the **Revert** button. (See Figure 2-4.)

**Saving Changes to the startup-config.** To save configuration changes to the startup-config and ensure that they are not lost when the Wireless Edge Services zl Module is reloaded, you must click the **Save** link at the top of the screen. (See Figure 2-4.)

If you are using the CLI, you must enter the **write memory** command to save changes to the startup-config file. When you enter this command, you must be in the wireless-services context. (For more information, see “CLI” on page 2-21.)
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Figure 2-4. Applying or Saving Changes

Logging Out or Refreshing the Screen

In addition to the Save link, the Web browser interface includes three links at the top of the screen:

- **Refresh**—updates the screen with current information
- **Logoff**—ends this management session

**Note**

Refreshing the screen too often can cause the refresh to fail. Simply refresh the browser again to rectify the problem.

Accessing the Online Help

Both information and configuration screens include a Help button, which allows you to access the online help. (See Figure 2-5.)
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Figure 2-5. Help Navigator Screen

From the Help Navigator screen, you can select one of the following tabs:

- **Content**—The Content tab provides a list of available topics. You simply double click a topic to view the Help information.

- **Search**—The Search tab allows you to enter keywords or boolean expressions to find all the information about a specific topic. When the results of the search are listed, select one of the topics and click the Open button to view the Help information.

The Wireless Edge Services zl Module (Module) uses the following SNMP community names: public, private, and trap. You can modify the public and private communities, but you cannot modify the trap community. Each community name is assigned an access control, which determines the operations an SNMP server can complete on the Module:

- **Read-only**—The SNMP server can retrieve information from the Module.
- **Read-write**—The SNMP server can retrieve information and modify the configuration settings.

By default, the public and trap communities have read-only access, and the private community has read-write access.

The SNMP Access v1/v2c screen is used to
Using Filtering Options

Filtering allows you to limit the amount of data displayed on a configuration screen by narrowing the criteria that is displayed. You can use the filtering options on certain configuration screens in order to list items that meet certain criteria. Screens that can be filtered contain a **Show Filtering Options** link, as shown in the example in Figure 2-6.

![Figure 2-6. Configuration Screen with Show Filtering Options Link](image-url)
Configuring the ProCurve Wireless Edge Services zl Module

Management Interfaces

Filters affect the display. The filter selects rows according to values in columns. For example, you can filter the Network Setup > WLANs screen to display rows only for those WLANs that list Web-Auth in the Authentication column.

Click the Show Filtering Options link to begin creating a filter.

![Filtering Options Example](image)

From the drop-down menus on the left, you select against which columns the filter matches items. For example, you can choose index and create a filter that displays only WLANs that list certain numbers in the Index column.

A filter can include:

- **A single criterion**—Leave the fields next to the second drop-down menu blank.
- **Two criteria**—You can choose different column names from the drop-down menus—for example, to filter according to encryption type and enabled status. Or you can choose the same column name—for example to show WLANs using either of two authentication methods.
When you select two criteria, you must use Boolean operators to link the two:
- **AND**—Only rows that match both criteria display.
- **OR**—Rows that match either or both criteria display.

In the fields to the right of the drop-down menus (see Figure 2-7 on page 2-17), you create the actual filter. The format for the filter depends on the type of column:
- **Match operators**—for columns that include a string.
  
  In the field on the right, you enter the string that must be included in the specified column. For example, if **Encryption** was selected from the drop-down menu on the left, you could enter TKIP. The string match is case sensitive.

  You also select, from a drop-down menu in the middle, the degree to which the string in a column must match the string in the filter. You can choose:
  - **contain**—The column must contain the specified string, but can also include other characters.
  - **exactly match**—The column must include only the specified string.
  - **start with**—The string in the column must start with the specified string, but can include characters after the string.
  - **end with**—The string in the column must end with the specified string, but can include characters before the string.
- **True or false**—for columns that have either a green check mark or red X. You choose whether the filter selects items for which the criteria is **True** (the column has a green check mark) or **False** (the column has a red X).
- **From and to fields**—for columns that list numbers, such as index numbers. The range is inclusive—that is, the filter matches the number in the **From** field, the number in the **to** field, or any number between the two.

To use the filtering options on a screen that can be filtered, complete the following steps:

1. On the screen, click **Show Filtering Options**.

   A **Filter Options** section is displayed on the screen, similar to the example shown in Figure 2-8.
2. In the Filter Options section, on the first line, use the first drop-down menu to select the criterion for the filter. The drop-down menu includes the name of every column in the screen.

In the example in Figure 2-8, you can select from Index, Enabled, SSID, and so on.

3. Specify the match criteria for the first criterion, as follows:
   - If the selected column contains strings, use the next drop-down menu to select contains, exactly matches, starts with, or ends with. This setting determines the degree to which the string in a column must match the specified string.

   Then, in the adjacent field, enter the string to be matched. The string match is case sensitive.

   - If the selected column displays check marks and Xs, select either True (check mark) or False (X).

   - If the selected column displays numeric values, enter the range of values in the From and to fields. The range is inclusive. For a single value, enter the value in the From field only.
4. If you are also filtering for a second criterion, on the second line, use the drop-down menu to select the Boolean operator for linking the two criteria:
   - **AND**—to list items that meet the criteria on both lines
   - **OR**—to list items that meet the criteria on either line

   The OR operator is not an “exclusive OR” operator; it will list items that meet the criteria on either or both lines.

5. If you are also filtering for a second criterion, on the remainder of the second line, complete steps 2 and 3 for this criterion.

   For example, in the **Network Setup > Radio** screen you could filter for all adopted radios of the 802.11bg type. You choose **Type** that contains “bg” for the first criterion and, for the second criterion, **Adopted is True**. Since you only want to see radios that meet both criteria, you select **AND** as the operator.

![Network Setup > Radio Screen](image)

**Figure 2-9. Filtering Options Radios Example**

---

2-20
6. After you set the filter criteria, click the **Filter Entire Table** button. Only the tunnels that match the filter are now listed on the screen. If you want, you can refine your filter criteria and click the **Filter Entire Table** button again.

**Note**

Throughout the Wireless Edge Services zl Module interface (whether or not you are using filtering), you can sort data lines by clicking on the respective column headings. For example, on the screen shown in Figure 2-8, you can click on the **SSID** column heading to sort the data alphabetically by the SSID name. Click the heading once to sort the column in ascending order (an up-arrow is displayed), and then click the heading again to sort the column in descending order (a down-arrow is displayed). Click the heading a third time to return the column to its original sort order (the arrow will no longer be displayed).

7. When you are finished viewing the filtered results, click the **Turn Off Filtering** button in order for all tunnels to be listed on the screen.

To hide the filtering options on the screen, click the **Hide Filtering Options** link. Although the filter itself is hidden, the screen continues to display only the rows that match the filter. To turn off filtering, click the **Show Filtering Options** link and then click the **Turn Off Filtering** button.

**CLI**

You access the Wireless Edge Services zl Module CLI through the CLI for the wireless services-enabled switch. You can access the switch CLI through:

- serial session
- Telnet session
- SSH session

**Accessing the Switch CLI Through a Serial Session**

If you use a serial session to connect to the wireless services-enabled switch, use the serial cable (5184-1894) that was shipped with the switch. Then run terminal session software such as Tera Term or HyperTerminal on your workstation, setting the following parameters for the session:

- Baud Rate = 9600
- Parity = None
- Data Bits = 8
- Stop Bits = 1
- Flow Control = None
When you are prompted for a password, enter the password for the manager user on the wireless services-enabled switch.

Accessing the Switch CLI Through a Telnet or SSH Session

You can also use a Telnet or SSH application to access the CLI for the wireless services-enabled switch. For instructions on establishing a Telnet or SSH session, see the management and configuration guide for your switch.

Accessing the Wireless-Services Context

To begin configuring the Wireless Edge Services zl Module, you must move to the wireless-services context in the switch CLI. In essence, the wireless-services context is a subset of the switch CLI.

To access the wireless-services context, enter this command, either from the basic, enable, or global configuration mode context:

```
ProCurve# wireless-services <slot letter>
```

Replace `<slot letter>` with the letter for the chassis slot in which the Wireless Edge Services zl Module is installed. For example, if the module is installed in slot C, you would enter:

```
ProCurve# wireless-services c
```

The CLI prompt shows that you are in the wireless-services context. You access the context with the same rights that you had in the switch CLI:

```
ProCurve(wireless-services-C)#
```

If you had only operator rights to the switch CLI, you would enter the command from the switch basic mode context and access the module’s basic mode context:

```
ProCurve> wireless-services c
ProCurve(wireless-services-C)>
```

Navigating the CLI

The wireless-services context allows you to configure and manage the Wireless Edge Services zl Module. The wireless-services context is organized into the same contexts used in the switch CLI. When you first access the wireless-services context, you are at the enable context, which is identified by the `#` symbol that follows the “(wireless-services-C)” portion of the prompt.
From the enable context, you can enter `show` commands to view information about the Wireless Edge Services zl Module, and you can perform some operations such as erasing the startup-config file and copying configuration files to and from the module.

To make configuration changes, however, you must move to the global configuration context. From the global configuration context, you can enter commands to change settings, or you can access other contexts that allow you to change settings.

To move to the global configuration context for wireless services, enter:

```
ProCurve(wireless-services-C)# configure terminal
```

Again, the CLI prompt shows your new context:

```
ProCurve(wireless-services-C) (config)#
```

To view the commands available at any context, you can use a question mark:

```
ProCurve(wireless-services-C) (config)# ?
```

You can also use the question mark to view the options available for specific commands:

```
ProCurve(wireless-services-C) (config)# ip ?
```

### Saving Changes to the startup-config

When you make configuration changes to the Wireless Edge Services zl Module, you must enter the `write memory` command to save these changes to the module’s startup-config. When you enter this command, you must be in the wireless-services context:

```
ProCurve(wireless-services-C)# write memory
```

If you exit the wireless-services context and enter the `write memory` command in the CLI for the wireless services-enabled switch, the configuration changes for the Wireless Edge Services zl Module are *not* saved to its startup-config file.

### CLI Commands

See Appendix A: “ProCurve Wireless Edge Services zl Module Command Line Reference” for a list of CLI commands for the Wireless Edge Services zl Module and their descriptions.
Security

In addition to supporting the latest security standards for wireless communications, the Wireless Edge Services zl Module allows you to secure management access. To protect communications between the Wireless Edge Services zl Module and your management workstation, the module supports secure hypertext transfer protocol (HTTPS) over Secure Socket Layer (SSL), and SNMP v3. Management users and their related passwords are also controlled through SNMP v3. You can also use SSH to access the module CLI indirectly.

SSH Access

If you want to access the Wireless Edge Services zl Module CLI from a remote location, consider using SSH to access the wireless services-enabled switch CLI and, through the switch CLI, the module’s. Although you can use Telnet to access the switch CLI (and through it the module CLI), Telnet is not secure from eavesdropping. The SSH protocol, on the other hand, generates public keys to encrypt all the data exchanged between the module and your management workstation. Further, SSH ensures that data traveling over the network arrives unaltered.

HTTPS Access

By default, the Wireless Edge Services zl Module supports both HTTP and HTTPS. When you use HTTPS to access the module’s Web browser interface, the connection between your management workstation and the Wireless Edge Services zl Module is secure. Communications between your workstation and the module are encrypted.

Note

You cannot modify the port numbers for HTTP and HTTPS.

SNMP Support

The Wireless Edge Services zl Module supports SNMP v1/v2c, allowing SNMP servers that know the correct community names either complete read-write or read-only access to the module.

The module also supports SNMP v3, a more secure—and flexible—way of controlling the users and SNMP servers allowed management privileges to the Wireless Edge Services zl Module.
SNMP v3 encrypts management communications. For example, SNMP v3 support secures messages between the Java applet running the Web browser interface and your management workstation even when you use HTTP, rather than HTTPS.

**SNMP Communities.** SNMP v1/v2c uses communities to control various types of management access. In order for an SNMP v1/v2c server to access the SNMP agent running on a device such as the Wireless Edge Services zl Module, the server must know at least one of the community names configured on the device. Each community name is assigned an access control: read-only or read-write. The access control assigned to the community determines the operations that an SNMP server can complete on the Wireless Edge Services zl Module.

A server that knows a device's read-only community name can view, but not alter, settings and other information stored on that device. For example, you might want a particular SNMP server to only monitor traffic on the device. An SNMP server that knows a device’s read-write community name can change its configuration in addition to viewing information about it.

The Wireless Edge Services zl Module uses the following community names:

- public
- private
- trap

By default, the public and trap communities have read-only access, and the private community has read-write access.

For more information on configuring communities, see “SNMP Communities” on page 2-109. For more information on setting up traps, see “Enabling SNMP Traps” on page 2-113.

You can also control management access and traps with SNMP v3, as described in the next section.

**SNMP v3 Users.** The management users for the Wireless Edge Services zl Module are controlled through SNMP v3.

SNMP v3 allows you to create multiple users with different levels of access. For example, instead of configuring a community name on an SNMP v3 server, you can configure it with its own username, password, and management privileges.
In addition, SNMP v3 secures communications between the user and the managed device, transforming the traffic with an encryption algorithm, an authentication algorithm, or both.

**Default SNMP v3 Users—Manager and Operator.** There are two default users:

- **Manager**—The manager has read-write access, which means the manager can configure settings and view information.
- **Operator**—The operator has read-only access, which means the operator can only view information. When a user accesses the Web browser interface using the operator name and password, buttons (such as **Apply** or **Edit**) that allow you to make configuration changes are unusable. (These buttons are dimmed or missing from the screen, as shown in Figure 2-10.)

There is also an trap user, which allows access to SNMP v3 traps sent by the module.

---

**Figure 2-10. Web Browser Interface (Operator Access)**

---
The operator user is particularly useful if you want to assign a new IT staff member the task of monitoring certain module functions; however, you do not want this IT staff member to change the existing configuration. In this case, you could give this IT staff member the password for the operator user but reserve the manager user password for only senior-level IT staff.

To learn how to add new SNMP v3 users, see “Configuring Web-Users” on page 2-40.

Controlling Management Access to the Module

This section teaches you how to control Web management access to the Wireless Edge Services zl Module. It explains how to:

- enable and disable HTTP and HTTPS access
- configure the internal FTP server
- choose SNMP versions
- change passwords for the default SNMP v3 users (manager and operator)
- create new Web-Users—users allowed to access the module’s Web browser interface with various privileges

Enabling HTTP and HTTPS Access to the Module

As described in “Security” on page 2-24, the Wireless Edge Services zl Module includes an HTTP server and an HTTPS server, which run the module’s Web browser interface. (Access to the interface is controlled by SNMP v3.)

- By default, both servers are enabled. You can disable either or both of these servers. (Of course, if you disable both, you will only be able to configure the module through the CLI.)

Follow these steps to enable and disable HTTP and HTTPS:

2. Uncheck the Enable HTTP box to disable insecure HTTP access to the Wireless Edge Services zl Module. Check the box to re-enable this server.

3. Uncheck the Enable HTTPS box to disable HTTPS access to the Wireless Edge Services zl Module. Check the box to re-enable this server.

4. From the HTTPS Trustpoint drop-down menu, select the trustpoint with the server certificate for the module’s HTTP server.

When an HTTPS client and server negotiate a connection, the server submits its digital certificate to the client to prove its identity. The HTTPS client must trust the entity that signed the certificate.

The Wireless Edge Services zl Module can store up to six trustpoints, each of which can contain a self-signed certificate or a certificate signed by a certificate authority (CA).
By default, the HTTPS server submits the self-signed certificate in the default-trustpoint. The HTTPS Trustpoint drop-down menu includes this trustpoint and any other trustpoint configured on the module.

The drop-menu also includes the **Create New Certificate** option. Select this option to open the Certificates Wizard, which guides you through the process of creating or installing a certificate. For more information about digital certificates and the Certificates Wizard, see “Digital Certificates” on page 2-166.

5. Click the **Apply** button.

**Note**

By default, users can reach the Wireless Edge Services zl Module’s Web browser interface at any IP address configured on the module. Secure management forces the module to open sessions only with users that destine their traffic to the module’s management VLAN IP address.

To enable this option, check the **Secure Management (or Management VLAN only)** box in the Management > Web Access Control screen. Then click the **Apply** button.

Choosing SNMP Versions

As described in “SNMP Support” on page 2-24, the Wireless Edge Services zl Module supports both SNMP v2 and SNMP v3. By default, both versions are enabled. You can disable either version.

For example, you might disable SNMP v2 to avoid sending management data in plaintext. Before disabling SNMP v2, make sure that your SNMP server supports SNMP v3 and that it knows the username and password for an SNMP v3 user configured on the module.

Take care when disabling SNMP v3: because this protocol controls communications between management stations and the Java applet, disabling SNMP v3 disables all access to the Web browser interface. You must then configure the module through the CLI. To re-enable Web access, enter this global configuration mode command: `snmp-server manager v3`.

To enable and disable either (or both) SNMP versions, as well as to configure various other options, follow these steps:

1. Select **Management > Web Access Control**.
2. Uncheck the **Enable SNMP v2** box to disable SNMP v2 access to the Wireless Edge Services zl Module. Check the box to re-enable such access.

3. Uncheck the **Enable SNMP v3** box to disable SNMP v3 access to the Wireless Edge Services zl Module.

   A screen is displayed, warning you that disabling SNMP v3 locks you out of the Web browser interface.
If you are sure that you want to disable SNMP v3 and Web access, click the Yes button. You have one more chance to change your mind: you must click the Apply button in the Management > Web Access Control screen to actually disable the server.

4. Configure other SNMP options:
   a. In the Retries field, enter the number of times that the Wireless Edge Services zl Module should re-attempt to send an SNMP message that times out.
      The default value is 3.
   b. In the Timeout field, specify, in seconds, how long the module should wait before timing out an SNMP message.
      The default value is 10 seconds.

5. Click the Apply button.

Choosing SNMP versions is only one step to configuring SNMP:
   ■ See “Configuring Web-Users” on page 2-40 to learn how to create SNMP v3 users.
   ■ See “SNMP Traps and Error Reporting” on page 2-109 to learn how to set up SNMP traps and configure SNMP communities.
Setting Up the Internal FTP Server

The Wireless Edge Services zl Module includes an FTP server, which can send files stored in the module's flash memory to FTP clients. For example, you could upload a configuration file directly from one module to another—eliminating the middle step of transferring the file to an external FTP server.

The FTP server has these properties:

- **Port**—The server listens on the standard FTP port, 21. You cannot alter the port number.
- **Username**—The default username is “ftpuser” and cannot be altered.
- **Password**—The FTP client must submit the correct password to receive the requested file.
- **Root directory**—The Wireless Edge Services zl Module searches this directory for requested files. You can specify the module's entire flash memory or a directory within the flash.

By default, the FTP server is disabled.

Follow these steps to set up the internal server:

1. Select **Management > Web Access Control**.
2. Check the **Enable FTP** box.
3. In the **Password** box, enter a string, which can include alphanumeric and special characters.

4. In the **Root Dir** field, specify the name of the directory with the files that clients will request.

   For example, enter `flash/`. The module searches for files in the flash directory. If the file is stored in a directory within flash, the client must request the file with the correct extension.

   You can click the **Browse** button to search for a different directory to specify as the root or to create a new directory. See the steps below for more information on this option.

5. Click the **Apply** button.
To use the browse button to select the root directory, follow these steps:

1. Click the Browse button next to the Root Dir field. The Select Directory file screen is displayed.

   This screen displays three buttons, one for each of the Wireless Edge Services zl Module's three file systems:
   - **system**: stores the running-config
   - **nvram**: stores the startup-config
   - **flash**: stores a variety of files

2. Click one of the buttons at the top of the screen to choose the file system in which the directory is located.

   When you first open the screen, **flash** is selected.

   The section at the left of the screen lists directories within this file system. For example, at factory settings, flash memory includes the four folders shown in Figure 2-59.

---

**Figure 2-15. Select Directory file Screen**
3. In the left section, select the directory in which the Wireless Edge Services zl Module searches for requested files.
   Click the directory once to choose the directory. Its name is displayed in the field at the bottom of the screen.
   Click the directory twice to view and select subdirectories within that directory. To return to the original directory, click [up one level], which is displayed in the left section with the subdirectories.

4. Alternatively, create a new directory (in the flash memory only).
   a. Click the New Folder button. The New Folder screen is displayed.

   ![New Folder Screen](image)

   Figure 2-16. New Folder Screen

   b. Name the directory, or folder, and click the OK button.
   c. Your new folder is displayed in the left section of the Select Directory file screen. Select this folder.

5. The path to the directory you have selected is displayed in the field at the bottom of the screen. Click the OK button.

   The path to the selected directory is displayed in the Root Dir field of the Management > Web Access Control screen. Finish configuring other options and click the Apply button.

Changing the Password for the Default SNMP v3 Users (Operator or Manager)

The Wireless Edge Services zl Module ships with the default passwords listed in Table 2-1.
Table 2-1. Default Passwords for the Operator and Manager Users

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>operator</td>
</tr>
<tr>
<td>manager</td>
<td>procurve</td>
</tr>
</tbody>
</table>

To protect your network, you should change the passwords for both users. Because the usernames and passwords are managed through SNMP v3, you must select a password that meets SNMP v3 standards: the password must be at least eight characters.

The password does not only authenticate the user. The password also functions as the key for the following algorithms which secure SNMP v3 communications:

- Hash Message Authentication Code-Message Digest 5 (HMAC-MD5), a hash algorithm that ensures data integrity
- Cipher Block Chaining-Data Encryption Standard (CBC-DES), an encryption algorithm that ensures data privacy

You can change the passwords either through the SNMP v3 settings or through the Web-User settings. The most recent configuration takes precedence.

Changing Passwords for Default Users Through SNMP v3. To change the passwords through the SNMP v3 settings, complete these steps:

1. Select Management > SNMP Access and click the V3 tab.
2. Select the username that you want to modify, and then click the **Edit** button. The **Edit SNMPV3** screen is displayed.
3. In the **Old Password** field, enter the current password.

4. In the **New Password** and **Confirm Password** fields, enter the new password.

5. Click the **OK** button.

If you change the password for the manager user, you are logged out of the Web browser interface and must enter the new password in order to log back in to the interface.
Changing Passwords for the Default Users Through Web-User Settings. To change the passwords for the manager or operator user through their Web-User settings, follow these steps:


![Image of Management > Web Users](image)

**Figure 2-19. Default Users in the Management > Web-Users > Local Users Screen**

2. Select the user for which you want to change the password.

3. Click the Edit button. The Edit User screen is displayed.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Figure 2-20. Editing a Web-User

4. In the Password and Confirm Password fields, enter a new password between 8 and 32 characters. The password can include spaces and special characters.

5. Click the OK button.

6. Click the Save link to copy these changes to the Wireless Edge Services zl Module’s startup-config.

Configuring Web-Users

By default, the Wireless Edge Services zl Module has two SNMP v3 user accounts: manager and operator. You can add more users allowed to access the Wireless Edge Services zl Module’s Web browser interface.

Note

Rights to the module CLI are determined by rights to the wireless services-enabled switch CLI. You must access the module CLI through the switch CLI, and you are granted the same rights that you had in the switch CLI.

The Wireless Edge Services module can authenticate these users against a local list of users, or you can have a RADIUS server authenticate the users.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

By default, the module uses its local list to authenticate the users.

**Web-User Roles.** You can select one or more of six roles for a user:

- **Monitor**—read-only rights (the default account, operator, has this role):
  - view settings and statistics, including detailed information
  - export statistics and other device information

- **HelpDesk Manager**—read-only rights and the ability to collect troubleshooting information:
  - view settings and statistics, including detailed information
  - export statistics and other device information
  - configure logging (Management > System Logging screens)
  - transfer core and panic snapshots (Troubleshooting screens)

- **Network Administrator**—read-write rights to most of the Wireless Edge Services zl Module's capabilities:
  - view settings and statistics, including detailed information
  - export statistics and other device information
  - complete any task in the Network Setup screens, including:
    - add, delete, and edit VLAN interfaces
    - configure Internet Protocol settings (such as routes)
    - configure radio and radio adoption default settings
    - add, delete, and edit WLANs
    - set up redundancy and Layer 3 mobility groups
    - configure DHCP services
    - configure the internal RADIUS server
  - complete most tasks in the Security screens, including:
    - create MAC filters
    - add and delete ACLs and apply them to interfaces (not editing existing ACLs)
    - configure dynamic NAT
  - complete all tasks in the Special screens, except configure sFlow

- **System Administrator**—read-only rights and rights to management tasks:
  - view settings and statistics, including detailed information
  - export statistics and other device information
  - complete limited tasks in the Network Setup screens:
    - add, delete, and edit VLAN interfaces
    - configure Internet Protocol settings (such as routes)
Configuring the ProCurve Wireless Edge Services zl Module

Management Interfaces

- complete any task in the Management screens, including:
  - control access to the Web browser interface, including adding and editing Web-users
  - configure the Update Server
  - manage configuration files and software images
  - install licenses
  - add digital certificates
  - configure SNMP and system logging

- set up secure NTP (Special > Secure NTP screens)

- **WebUser Administrator**—add guest user accounts to the Wireless Edge Services zl Module’s internal RADIUS database. The database must already include at least one guest group.

- **SuperUser**—complete read-write access to the module. The default user account, manager, has this role. A SuperUser can complete any task that any other type of user can complete.

You can assign a user more than one role. For example, you could make a user both a HelpDesk Manager and a System Administrator. However, the WebUser Administrator can only play that single role.

**Adding a Web-User to the Local List.** Follow these steps to add a Web-User:


   Initially, the screen lists the two default SNMPv3 users. If you select a user, the user's roles display in the Privileges section.
2. Click the **Add** button. The **Add User** screen is displayed.
3. In the **User Name** field, enter a string between 1 and 28 characters. You can include spaces and special characters.

4. In the **Password** and **Confirm Password** fields, enter a password between 8 and 32 characters. The password can include spaces and special characters.

5. Check the boxes in the **Associated Roles** section to assign one or more roles to this user.

   See the discussion above for more information on the privileges associated with each role.

6. Click the **OK** button.

7. Click the **Save** link to copy these changes to the Wireless Edge Services zl Module’s startup-config.

**Configuring Authentication for Web-Users.** Instead of (or in addition to) using the local list to authenticate users, you can use a RADIUS server. If the RADIUS server authenticates a user, that user has the rights configured on the RADIUS database.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Make sure that the configuration on the RADIUS server meets these requirements:

- The user's password is at least 8 characters.

  SNMP v3 requires a password of at least this length. Your RADIUS server, however, may or may not enforce such a requirement. (For example, the Wireless Edge Services zl Module's internal server does not.) Check the accounts for users that need management access to the module and, if necessary, set a new password of the correct length.

- The RADIUS server supports vendor specific attributes (VSAs).

  For the RADIUS server to properly authorize the management user, you must set two VSAs in the policy that the RADIUS server uses to authenticate the user. Table 2-2 shows the proper values for the “HP-Management-Protocol” and the “HP-Management-Role” attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Length</th>
<th>Vendor ID</th>
<th>Vendor Type</th>
<th>Vendor Length</th>
<th>Format</th>
<th>Vendor Value</th>
</tr>
</thead>
</table>
| HP-Management-Protocol | 26   | 12     | 11 (HP)   | 4           | (HP-Management-Protocol) | 6   | Decimal | • 6 = HTTP  
|                    |      |        |           |             |               |                | 7 = HTTPS        |
| HP-Management-Role     | 26   | 12     | 11 (HP-Management-Role) | 1  | (HP-Management-Role) | 6   | Decimal | • 1 = SuperUser
|                      |      |        |           |             |               |                | 2 = Monitor      |
|                      |      |        |           |             |               |                | 16 = HelpDesk Manager |
|                      |      |        |           |             |               |                | 17 = Network Administrator |
|                      |      |        |           |             |               |                | 18 = System Administrator |
|                      |      |        |           |             |               |                | 19 = WebUser Administrator |

If the server does not send the proper VSAs, the user receives the monitor role (read-only) to the Web browser interface.

The module's internal server does not support VSAs, so you should use the local server only to authenticate users that require read-only access.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Note

If you do not correctly configure the RADIUS server, you can lock yourself out of the Wireless Edge Services zl Module Web browser interface.

To fix the problem, access the module CLI through the wireless services-enabled switch. Enter this global configuration mode command to have the module authenticate Web-Users against its local list:

Syntax: aaa authentication login default local

Then configure at least one user in the local list:

Syntax: username <username> password <password>

The password must be between 8 and 32 characters.

Then assign the user rights sufficient to correct the problem. For example:

Syntax: username <username> privilege superuser

Follow these steps to choose how users authenticate when they attempt to access the Wireless Edge Services zl Module's Web browser interface:

2. Click the Authentication tab.
3. Choose the primary authentication method from the **Preferred method** drop-down menu.
   
   You can choose **local** (which is the list of local users configured on the **Local Users** tab) or **radius**.

4. If you want to use both authentication methods, chose the other method from the **Alternate method** drop-down menu.
   
   If the preferred method fails, the alternate is attempted. Note that “fails” means that the authentication service is unavailable, not that the user’s authentication attempt fails.
5. Optionally, check the **If authentication services are unavailable, allow read-only access** box.

   All users are granted read-only (monitor) access when the selected authentication services are unavailable.

   If you do not check the box and authentication services become unavailable, users will have no access to the Web browser interface at all. (They must access the module CLI from the wireless services-enabled switch CLI.)

6. Click the **Apply** button.

7. If you have selected RADIUS for either authentication method, you must specify the RADIUS server:

   a. Click the **Add** button. The Add RADIUS Server screen is displayed.

   ![Add RADIUS Server Screen](image)

   **Figure 2-24. Specifying the RADIUS Server To Authenticate Web-Users**

   b. Specify the server's IP address in the **Radius Server IP Address** field.

   The Wireless Edge Services zl Module attempts to contact RADIUS servers in the order that you add them. Be careful to specify your preferred server first.
c. Enter your server’s port in the **Radius Server Port** field.
   Typically, enter 1812. The valid range is from 0 to 65535.

d. In the next field, specify the number of times that the module attempts to connect the RADIUS server if it does not receive a reply.
   For example, if you enter 3, the module attempts to reach the RADIUS server four times, at the most. It then considers the authentication service unavailable. The valid range is from 0 to 100.

e. In the next field, specify how long the module waits for a reply from the RADIUS server before retrying (or, on the final retry, declaring the authentication service unavailable).
   The timeout value is in seconds; specify a number from 1 to 1000.

f. In the next field, enter the shared secret.
   This string must match the secret specified for the Wireless Edge Services zl Module in the list of clients on the RADIUS server.

g. Click the **OK** button.

8. Click the **Save** link to copy these changes to the Wireless Edge Services zl Module's startup-config.

---

**Logging In to the Module as a WebUser Administrator**

WebUser Administrators, with their very limited rights, access a single screen, from which they can manage guest accounts on the local RADIUS database.

---

**Note**

A guest account is a temporary user account, and the user must belong to a guest group.

Before the WebUser Administrator can add guests accounts, a user with Network Administrator or SuperUser privileges must create a guest group on the local RADIUS database.

For more information about the Wireless Edge Services zl Module's internal RADIUS server, see Chapter 11: “RADIUS Server.”

---

To log in as a WebUser administrator, access the Wireless Edge Services zl Module's Login screen, and enter the username and password for a user with this role.

The screen illustrated in Figure 2-28 is displayed.
Configuring the ProCurve Wireless Edge Services Z1 Module
Management Interfaces

Figure 2-25. Guest Registration Screen

From this screen, the WebUser Administrator can:

- create guest accounts
- view all guest accounts
- delete guest accounts
- print records for the guest accounts added during the current management session

Creating Guest Accounts on the Local RADIUS Database

Follow these steps to add a guest user account:

1. Log in as the WebUser Administrator and access the Guest Registration screen.
Guest Registration

Use this page to register guests and grant them temporary access to your company's network, to the internet, or allow them entry to only specific areas on your wireless network.

2. Enter the username in the **User Name** field.

   The username can be up to 64 characters and can include alphanumeric and special characters.

   Alternatively, click the **Create** button to have the Wireless Edge Services zl Module OS automatically generate a random username.

3. In the **Password** field, enter the user's password.

   The password can be up to 21 characters and can include alphanumeric and special characters.

   Again, you can click the **Create** button, and the module automatically generates a random password.
4. In the **User Group** drop-down menu, select the name of a guest group policy. The group policy determines the days of the week and the times of day at which the user is allowed to access the network. The group policy can also dictate a dynamic VLAN assignment. (However, dynamic assignment must be enabled on the WLAN to which the guest connects for this setting to take effect.)

The WebUser Administrator cannot create groups. Before the WebUser Administrator creates guest user accounts, someone must log into the Wireless Edge Services zl Module with SuperUser or Network Administrator rights, and create at least one guest group.

5. Guest accounts are temporary. Specify the period of validity in the **Access Period** section:

   a. In the **Start Date & Time** field, choose when the account becomes active.

   Enter the date in this format, in which MM is the number of the month, DD is the date, and YYYY is the year:

   MM/DD/YYYY

   After the date, enter a hyphen (-) and the time in this format, in which HH is the hour in the 24-hour clock and MM is the minutes:

   HH:MM

   For example, enter:

   02/17/2007-08:00

   By default, the account’s start date and time is the current time.

   b. Specify the date and time at which the account expires (that is, the user can no longer connect) in one of two ways:

   – Enter an exact date and time in the **Expiry Date & Time** field.

   Use the same format as for the **Start Date and Time** field. Of course, the expiry time must be later than the start time.
Configuring the ProCurve Wireless Edge Services zl Module
Management Interfaces

Specify how long the account remains active from the **Access Periods** drop-down menu.
You can choose a length from one to six days. You can also choose one to three weeks or one to three months.
The Wireless Edge Services zl Module OS automatically sets the expiry date and time based on start date and time and the specified period of validity.
The Wireless Edge Services zl Module automatically clears out expired accounts every 24 hours. In the meantime, however, no one can use the expired account to connect.

6. Click the **Submit** button.
7. The interface asks you to confirm the creation of the account. Click the **Yes** button.

At any time before you submit the guest account, you can click the **Clear** button to erase the settings.

When you are finished managing the guest accounts, click the **Logoff** link. You do not need to take any further step to save your changes to the startup-config. Clicking the **Submit** button and confirming the creation of the account commits automatically does so.

**Viewing and Deleting Guest Accounts**

The WebUser Administrator can also view guest accounts already configured on the Wireless Edge Services zl Module’s local RADIUS database. And he or she can delete these accounts.

Follow these steps:

1. Log in as the WebUser Administrator and access the **Guest Registration** screen.
2. Click the **View/Delete Guests** tab.
3. The screen displays a list of all guest user accounts and the start and end time for these accounts. When you select an account, the Assigned Groups section displays the group of which the user is a member.

4. To delete a user, select the user and click the Delete button.

5. A screen is displayed, informing you that the RADIUS server must restart in order to implement the change. Click the Yes button to confirm the restart. (The server will become very briefly unavailable.)

When you are finished managing the guest accounts, click the Logoff link. You do not need to take any further step to save your changes to the startup-config.
Printing Records of Guest Accounts

You can also print records of guest accounts. A record includes:

- the username
- the password (in plaintext)
- the time and date at which the account starts and expires

You can only print accounts created during the current management session. This requirement protects guest users’ passwords. Even if an unauthorized person gains access as a WebUser Administrator, he or she cannot view and print passwords for existing accounts.

1. Log in as the WebUser Administrator and access the **Guest Registration** screen.
2. Click the Print link at the top of the screen. The Print screen is displayed. If you have not yet created a guest account, you receive an error message. You must click the Submit button before you can print the record of an account.

![Print Screen]

Figure 2-29. Printing a User Record

3. From the drop-down menu, choose the username for the account that you want to print.

The account information is displayed below.

4. Click the Print button.

An application on your management station, which must be connected to a printer, opens and guides you through printing the document.

You are then returned to the Guest Registration page. When you are finished managing the guest accounts, click the Logoff link.
Radio Port Adoption

By default, the Wireless Edge Services zl Module automatically adopts radio ports (RPs) that it detects on the network. For more security, you can disable automatic RP adoption and configure the module to adopt only those RPs for which you manually enter the Media Access Control (MAC) address.

The module can adopt RPs that are in the Radio Port VLAN (Layer 2 adoption) or in a different VLAN across a subnetwork boundary (Layer 3 adoption). Figure 2-30 illustrates when to use each type of adoption. In either case, your network must meet certain requirements in order for the module to detect the RP.

Figure 2-30. Layer 2 Versus Layer 3 Adoption
Network Requirements for Layer 2 Adoption

Before the Wireless Edge Services zl Module can adopt an RP that is connected to your network, the module must detect that RP. Detection is dependent upon network connectivity: all the network interfaces between the module and the RP must be correctly configured to carry traffic in the Radio Port VLAN.

- The Wireless Edge Services zl Module’s downlink port must be a tagged member of the Radio Port VLAN (by default, VLAN 2100).
- The switch port that connects to the RP must be an untagged member of the Radio Port VLAN.
- Each switch interface that carries traffic between the RP and the module must be either a tagged or untagged member of the Radio Port VLAN, as your network requires.

For example, you may attach the RPs to a Power over Ethernet (PoE) compatible infrastructure switch, which is connected, in turn, to the wireless services-enabled switch. The uplink port on the infrastructure switch must be able to carry traffic from the Radio Port VLAN. If the uplink port is carrying traffic from other VLANs, you must make that port a tagged member of the Radio Port VLAN.

Auto-Provisioning on the Wireless Services-Enabled Switch

The wireless-enabled switch automatically creates a default Radio Port VLAN—VLAN 2100—when you install the Wireless Edge Services zl Module in the Switch 5400zl or Switch 8200zl chassis. If VLAN 2100 is already being used, the wireless services-enabled switch uses the next available VLAN.

In addition to creating the default Radio Port VLAN, the wireless services-enabled switch automatically configures the module’s downlink port as a tagged member of VLAN 2100. The downlink port handles the traffic sent to and from RPs.

If you attach RPs to a PoE module that is installed in the wireless services-enabled switch, the switch automatically configures each RP’s switch port as an untagged member of the default Radio Port VLAN. (Because the RP does not support 802.1Q, it must be an untagged member of the Radio Port VLAN.)

When the appropriate VLAN memberships are established, the RPs can transmit traffic to the Wireless Edge Services zl Module, and the module can, in turn, detect the RPs. (See Figure 2-31.) (For more information about the communications between the RPs and the wireless services-enabled switch, see Chapter 1: “Introduction.”)
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Adoption

Figure 2-31. RPs Attached to the Wireless Services-Enabled Switch Are Automatically Assigned to a Radio Port VLAN

Attaching RPs to Infrastructure Switches

If you connect an RP to an infrastructure switch, rather than to the wireless services-enabled switch, the VLAN memberships are not automatically created on the infrastructure switch. Instead, you must manually create the Radio Port VLAN on the infrastructure switch and then add each RP’s switch port as an untagged member of that VLAN.

To allow RP traffic to be transmitted between the infrastructure switch and the wireless services-enabled switch, you must make the ports that connect the switches members of the Radio Port VLAN, which is VLAN 2100 by default. Typically, you will make these ports tagged members of the Radio Port VLAN, because they must also carry traffic for other VLANs such as the management VLAN. (See Figure 2-32.) However, if the downlink ports on both switches carry only traffic from the Radio Port VLAN, you can make these ports untagged members of the Radio Port VLAN.
Instead of using the default Radio Port VLAN, you can use any VLAN in your network—even a VLAN that is used to transmit wired traffic. In this case, you must manually tag the downlink port for this VLAN and configure other switch ports for this VLAN as described above. In Figure 2-33, for example, the network administrator used VLAN 300 for traffic transmitted to and from one of the RPs.
**Note** Generally, you should simply assign RPs to the default Radio Port VLAN ID (2100). Assigning RPs to a VLAN also used in your Ethernet network can introduce problems because you must never tag both the uplink and the downlink port for the same VLAN. Such a configuration would cause the Wireless Edge Services zl Module to ignore the downlink port.

![Diagram of Wireless Services-Enabled Switch and Infrastructure Switch](image)

**Figure 2-33. Manually Creating Radio Port VLANs**

For more information about Radio Port VLANs, see Chapter 1: “Introduction.”
Note

You might also need to perform some configuration tasks on the wireless services-enabled switch, such as raising the maximum number of VLANs. For help on completing configuration tasks on the wireless services-enabled switch, refer to the appropriate guide for the zl switch:

- **ProCurve Series 6200yl Switches, 5400zl Switches, and 3500yl Switches Management and Configuration Guide**
- **ProCurve Series 6200yl Switches, 5400zl Switches, and 3500yl Switches Advanced Traffic Management Guide**

Network Requirements for Layer 3 Adoption

As discussed in “Network Requirements for Layer 2 Adoption” on page 2-58, RPs can be adopted at Layer 2 as long as you attach them to an infrastructure switch that is in the same VLAN (Layer 2 domain) as the wireless services-enabled switch. The messages that the RPs send to become adopted, which are Layer 2 broadcasts, can reach the Wireless Edge Services zl Module.

Sometimes, however, you may want to attach RPs to switches that are on a different subnetwork than the Wireless Services zl Module, requiring a Layer 3 device, such as a router, to establish communications. In this case, Layer 3 adoption is required. Figure 2-34 shows several RPs that require Layer 3 adoption.
An RP first attempts to be adopted at Layer 2. If Layer 2 adoption fails, the RP initiates Layer 3 adoption. The RP sends a DHCP request so that it can begin to communicate at Layer 3.

After receiving an IP address, the RP attempts to contact the Wireless Edge Services zl Module at Layer 3. The RP can discover the module's IP address either through a special DHCP option (option 189) or through Domain Name System (DNS).

To be adopted at Layer 3, an RP requires:

- its own IP address and the IP address of a default gateway
  
  The RP receives both its IP addresses through DHCP. (Because the RP is on a different subnetwork than the Wireless Edge Services zl Module, the RP requires the default gateway to route its adoption messages to the module.)

- the IP address of the Wireless Edge Services zl Module
  
  The RP can learn this address in one of two ways:
  - receiving the address in option 189 of a DHCP configuration
  - looking up the address through DNS
Configuring the ProCurve Wireless Edge Services zl Module

Radio Port Adoption

- the correct bootloader code

The bootloader code allows the RP to request a DHCP configuration and contact the Wireless Edge Services zl Module at Layer 3. If the RP did not ship with this code, it must first be adopted at Layer 2 by a Wireless Edge Services zl Module.

The instructions for enabling Layer 3 adoption explain how to determine your RP's bootloader code version and, if necessary, update the code.

**Note**

This guide refers to the process of adopting and configuring an RP before installing it in its final location as *pre-adoption*.

In addition to ensuring that your RP meets the requirements for Layer 3 adoption, you must ensure that your network meets the following requirements:

- DHCP server that sends one of these two configurations to the RP:
  - an IP address, a default gateway address, and option 189, which includes the IP address of up to three Wireless Edge Services zl Modules
  - an IP address, a default gateway address, a domain suffix, and a DNS server address

- router that acts as the default gateway for the RP and can reach the Wireless Edge Services zl Module

- any necessary IP helper addresses on infrastructure devices so that the RP can reach the DHCP server

- the internal uplink port on the Wireless Edge Services zl Module tagged for the VLAN on which the module has its IP address

**Note**

Do not tag the downlink port for this VLAN. (The two internal ports of Wireless Edge Services zl Module must never be tagged for the same VLAN.) The RP can be adopted on the uplink port.

- a PoE device to provide the RP with power

- optionally, a DNS server that maps the name that the RP knows for the Wireless Edge Services zl Module to the module’s IP address (required only if you select the DNS strategy)
  - By default, the RP sends a DNS request for this name:
    
    PROCURVE-WESM
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Adoption

The RP appends the domain suffix that it received through DHCP. For example:

PROCURVE-WESM.procurve.com

- You can change the name that the RP looks up. However, this option requires you to pre-adopt the RP at Layer 2.

Note

If a firewall separates your RPs from your Wireless Edge Services zl Module, you must ensure that this firewall allows the RPs adoption messages. The RPs send these messages on UDP port 24576; do not filter this port.

The next sections describe in more detail the two strategies for enabling Layer 3 adoption of RPs.

Enabling Layer 3 Adoption Through DHCP Option 189

Using DHCP option 189 to adopt RPs at Layer 3 has these advantages:

- By specifying the IP addresses of up to three Wireless Edge Services zl Modules, you ensure high availability. If one module happens to be down, the RP can be adopted by another module.

- Even if your Wireless Edge Services zl Modules use custom hostnames, you do not have to pre-adopt RPs. The RPs receive the modules' IP addresses directly in option 189, so they do not need to send DNS requests.

However, this strategy does require some extra setup: you must define the private option 189 on your server and you must add the option to the DHCP configuration that the RP will receive. Refer to your DHCP server's documentation for instructions on adding private options. You must set up the option so that its code is 189 and its value type is string.

Complete these steps to enable Layer 3 adoption:

1. Ensure that the RP has the proper bootloader code.

   If the RP has the old boot code, you must have the Wireless Edge Services zl Module pre-adopt the RP at Layer 2. As part of the adoption process, this module will automatically update the RP's bootloader code, as you can check in the Device Information > Radio Adoption Statistics screen (see Figure 2-35).

   The code automatically updates.
Radio Port Adoption

With the new bootloader code, the RP can complete Layer 3 adoption. You can now install the RP in its final location, and as long as you set up other requirements described below, the RP will be adopted at Layer 3.

2. On your DHCP server, you can create a fixed configuration specifically for the RP, or you can add option 189 to a pool already configured for other stations.

You can easily allow the RP to use the same pool as other stations. The DHCP server does not send the 189 option unless the device requests it.

If, however, for whatever reason, you want to create a fixed configuration for the RP, you should specify the RP’s Ethernet MAC address as the client ID. You can find this MAC address on the undercarriage of an RP 210 or 230 or the top face of an RP 220.

**Figure 2-35. Checking an RP’s Bootloader Code Through the Module’s Web Browser Interface**

With the new bootloader code, the RP can complete Layer 3 adoption. You can now install the RP in its final location, and as long as you set up other requirements described below, the RP will be adopted at Layer 3.
3. Whichever type of configuration you choose for the RP, add option 189 to the configuration. For the option's value, specify up to three IP addresses of Wireless Edge Services zl Modules. Separate the addresses with spaces. For example:

   10.4.1.30 10.4.1.40 10.4.2.35

4. Ensure that all necessary helper addresses are in place in your network infrastructure so that the RP's DHCP request can reach the server.

5. Ensure that the RP's default gateway can reach the IP addresses specified in option 189.

6. The Wireless Edge Services zl Module's internal uplink port must be tagged for the VLAN on which RPs messages arrive—that is, the VLAN on which the module has the IP address specified in option 189. The module's uplink port is probably already tagged for this VLAN. If so, the RP is adopted without further configuration.

7. Install the RP in its final location, connecting it to a PoE device.

### Enabling Layer 3 Adoption Through DNS Lookup

The DNS strategy has the advantage that the RP can receive a DHCP configuration that is probably already in place on your network's DHCP server. In fact, the RP might be able to connect to the network and immediately be adopted at Layer 3. However, for this to occur, your DNS server must map the default DNS name known by RPs to the Wireless Edge Services zl Module's IP address. If you have changed the module's DNS name, you must pre-adopt the RPs and configure the module to push down the new DNS name to them (explained in step 4 on page 2-68).

Follow these steps to enable Layer 3 adoption:

1. Ensure that the RP has the proper bootloader code.

   If the RP has the old boot code, you must have the Wireless Edge Services zl Module pre-adopt the RP at Layer 2. As part of the adoption process, this module will automatically update the RP's bootloader code, as you can check in the Device Information > Radio Adoption Statistics screen (see Figure 2-35).

   The code automatically updates.
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Adoption

Figure 2-36. Checking an RP’s Bootloader Code Through the Module’s Web Browser Interface

With the new bootloader code, the RP can complete Layer 3 adoption. You can now install the RP in its final location, and as long as you set up other requirements described below, the RP will be adopted at Layer 3.

2. Verify that your DHCP server has a configuration that the RPs can use:
   • IP address in the RPs’ subnetwork
   • IP address of a default gateway
   • IP address of a DNS server
   • typically, a default domain name

3. Check the configuration of your network’s DNS server, if necessary adding an entry that maps the Wireless Edge Services zl Module’s hostname to its IP address.

4. If you choose a different name for your module than the default name known by the RPs, you must configure the new name on the RPs:
   a. Have the module adopt the RPs at Layer 2.
b. Access the module CLI and enter these commands:

   ProCurve(wireless-services-C)# configure
   ProCurve(wireless-services-C)(config)# wireless
   ProCurve(wireless-services-C)(config-wireless)# radio dns-name <name> [XX:XX:XX:XX:XX:XX]

   Replace <name> with the name specified for the module on the DNS server. The name can be up to 127 characters. Enclose the string with quotation marks (" ") if you want to include spaces in the name: for example, you might enter the following: “Company XYZ Module”

   The RP requests a DNS lookup of this name as part of Layer 3 adoption. The exact request is the name that you enter followed by the domain name suffix that the RP receives from the DHCP server.

   Optionally, specify the MAC address of a single RP to have the module send the DNS name to that RP only. Otherwise, the module sends the name to all RPs adopted at that time. These RPs, if they later must perform Layer 3 adoption, will send the new name in requests to the DNS server.

   The radio dns-name command pushes the name to RPs as a one-time event. If an RP is adopted after you enter the command, you must enter it again to affect that RP.

5. Ensure that all necessary IP helper addresses are in place in your network infrastructure so that the RP’s DHCP request can reach the server.

6. Ensure that the RP’s default gateway can reach the IP addresses known by the DNS server.

7. The Wireless Edge Services zl Module’s internal uplink port must be tagged for the VLAN on which RPs messages arrive—that is, the VLAN on which the module has the IP address specified on the DNS.

   The module’s uplink port is probably already tagged for this VLAN. If so, the RP is adopted without further configuration.

8. Install the RP in its final location, connecting it to a PoE device.

Verifying Layer 3 Adoption

To verify that an RP has been adopted at Layer 3, select Device Information > Radio Adoption Statistics.
Configuring the ProCurve Wireless Edge Services zl Module

Radio Port Adoption

Figure 2-37. Verifying Layer 3 Adoption in the Device Information > Radio Adoption Statistics

The screen should list the Layer 3 RP just as it lists other RPs. However, the IP Address field shows the Layer 3 RP's IP address. (This field shows N/A for Layer 2 RPs.)

Note

The IP address is for informational purposes only. For example, you can ping the RP at this address, but you cannot attempt to access or manage the RP.

Automatic or Manual Adoption of RPs

Once an RP can transmit traffic to the Wireless Edge Services zl Module, the module can detect and adopt it. Automatic adoption simplifies deployment, especially if your network includes many RPs. After the Wireless Edge Services zl Module adopts an RP, it sends the radio adoption default configuration to it. You can then customize settings for certain RPs. (To learn how to configure RP settings, see Chapter 3: “Radio Port Configuration.”)
There is one possible drawback to automatically adopting RPs, however. The Wireless Edge Services zl Module could potentially adopt an unauthorized RP. This unauthorized RP would be treated exactly as an authorized RP, receiving settings for your network’s WLANs and sending traffic into the Ethernet network.

If you can tightly control your wireless services-enabled switch and all infrastructure switches, you can prevent someone from attaching a rogue RP to the network and adding access to your wireless services in authorized areas. If you are worried about rogue RPs, you can manually adopt RPs.

Although manually adopting RPs can tighten security, it also requires more administrative effort. You must determine the best option for your particular network environment.

You can also use a combination of methods. For example, install and automatically adopt some RPs. Then enable manual adoption and manually add the remaining RPs. The RPs that you previously adopted automatically remain adopted.

**Note**

If you create a redundancy group and decide to disable automatic RP adoption, you should ensure that you disable automatic RP adoption on both the Wireless Edge Services zl Module and the Redundant Wireless Services zl Module. Otherwise, the Redundant Wireless Services zl Module will automatically adopt RPs. For more information about configuring redundancy groups, see Chapter 10: “Redundancy Groups.”
Configuring Manual Adoption for RPs

To manually adopt RPs, you must edit the global settings for RPs. Complete these steps:

1. Select **Network Setup > Radio** and click the **Configuration** tab.

2. Click the **Global Settings** button. The **Global** screen is displayed.
Configuring the ProCurve Wireless Edge Services zl Module

Radio Port Adoption

Figure 2-39. Network Setup > Radio > Global Settings Screen

3. Uncheck the **Adopt unconfigured radios automatically** box.

4. Click the **OK** button to apply the change to the running-config.

5. Find the MAC address of the RPs that you want to manually adopt by selecting **Device Information > Radio Adoption Statistics** and clicking the **Unadopted** tab. The unadopted RPs and their MAC addresses are listed on this screen.

6. Select the unadopted RP that you want to adopt.
   
   You can skip this step if you want to adopt an RP that the Wireless Edge Services zl Module cannot yet detect.
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Adoption

Device Information > Radio Adoption Statistics

<table>
<thead>
<tr>
<th>Adopted RP</th>
<th>Unadopted RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>MAC Address</td>
</tr>
<tr>
<td>3</td>
<td>10-14-02-A0-3B-E3</td>
</tr>
</tbody>
</table>

Number of unadopted RPs: 1

Adopt Export

Figure 2-40. Device Information > Radio Adoption Statistics Screen

7. Click the Adopt button at the bottom of the screen. The Add Radio screen is displayed.

Add Radio

RP MAC Address: 00-14-02-A0-3B-E3

Radio Settings:

- 802.11b Radio Index
- 802.11bg Radio Index

Status:

OK Cancel Help

Figure 2-41. Add Radio Screen
8. If you selected an unadopted RP before clicking the Add button, the RP MAC Address field displays the MAC address of that RP. Otherwise, enter the RP's Ethernet MAC address.

9. In the Radio Settings section, check the boxes for the radio types that you want—802.11a or 802.11bg (or both).

10. For each radio type that you select, in the corresponding Radio Index field, enter a number to identify this RP.

   Do not enter a radio index number already used on this Wireless Edge Services zl Module.

11. Click the OK button.

   You can also manually add a radio from the Network Setup > Radio screen. Follow these steps:


   Note that the screen informs you that automatic adoption is disabled. You must manually add radios.

---

![Network Setup > Radio Screen (Manual Adoption)](image)

**Figure 2-42.** Network Setup > Radio Screen (Manual Adoption)
2. In the **RP MAC Address** field, enter the MAC address for the RP’s Ethernet interface.

3. In the **Radio Settings** section, check the boxes for the radio types that you want—**802.11a** or **802.11bg** (or both).

4. For each radio type that you select, in the corresponding **Radio Index** field, enter a number to identify this RP.

5. Click the **OK** button. The RP’s radios are added to the **Network Setup > Radio** screen, but it takes a few seconds for the green check mark to be displayed in the **Adopted** field.

**Controlling Which Wireless Edge Services zl Module Adopts Particular RPs—Adoption Preference ID**

Your Wireless LAN System can include multiple Wireless Edge Services zl Modules. In this case, you might want to control which modules adopts which RPs.

Adoption preference IDs control the adoption process.

Each module should have its own adoption preference ID. Set this ID by clicking the **Global Settings** button in the **Network Setup > Radio > Configuration** screen. Then enter a value from 1 to 65535 in the **Module Adoption Preference ID** field.

As an RP attempts to become adopted, modules defer the RP to the module that has the same ID as the RP. (However, should no module have a matching ID, the RP eventually becomes adopted by any module in the system.)
You set an RP’s ID by selecting one of its radios in the **Network Setup > Radio > Configuration** screen and clicking the **Edit** button.

Then enter a value from 1 to 65535 in the **Adoption Preference ID** field. Match the ID that you set for the Wireless Edge Services zl Module that should adopt this RP.

Remember: RPs do not store their own radio configurations; they receive them from a Wireless Edge Services zl Module. Therefore, you must create radio configurations for each RP on each module, and you must set the correct adoption preference IDs in these radio configurations. This allows the RP to receive the correct ID no matter which module first detects its adoption messages.

For example, if your system includes two modules and 70 RPs, you must create the same radio configurations for all 70 RPs on both modules. And on both modules, you would set some RP radios to the first module’s adoption preference ID and some RP radios to the second module’s ID.
You can create a radio configuration manually by clicking the **Add** button in the **Network Setup > Radio > Configuration** screen and entering the RP’s Ethernet MAC address. You can then edit the configuration and set the adoption preference ID to match the module that should adopt that RP.

For a more efficient alternative, have one module pre-adopt all RPs and edit the radio configurations on that module. Then copy those configuration to other modules in the Wireless LAN System.

For more information on configuring adoption preference IDs, see “Setting up Adoption Preference IDs to Control RP Adoption” on page 10-24 of Chapter 10: “Redundancy Groups.” These instructions focus on the special case of multiple Wireless Edge Services zl Modules and Redundant Wireless Services zl Modules that form a redundancy group; however, they also apply to modules that are not in a redundancy group, but are part of the same Wireless LAN System.

### 802.1X Authentication for RPs

To prevent rogue RPs from being adopted, you can also enforce 802.1X authentication on your network switch ports. The ProCurve RPs 210, 220, and 230 include an 802.1X client so that they can connect to ports that enforce such authentication. Using MD5 authentication, the client automatically sends the RP’s credentials when the RP connects to a network device. The switch to which the RP connects forwards the credentials to an authentication server and, if the credentials are correct, allows the RP to join the network.

The authentication server may store a VLAN setting for the RP, which it sends to the switch after the RP authenticates. Such dynamic configuration of the Radio Port VLAN can replace auto-provisioning on the wireless services-enabled switch or manual configuration on an infrastructure switch. (See “Communicating with RPs: Radio Port VLANs” on page 1-8 of Chapter 1: “Introduction” for more information about configuring Radio Port VLANs.)

---

**Note**

When you implement 802.1X on a port, auto-provisioning is disabled on that port. You must either manually set the port to the correct VLAN for the RP or configure the VLAN assignment on the RADIUS server.

However, the wireless services-enabled switch can continue to implement auto provisioning on ports that do not enforce 802.1X.
The default username and password on all ProCurve 200 Series RPs are admin and procurve.

ProCurve Networking suggests that you use pre-adoption to change these settings, using a Wireless Edge Services zl Module to load new credentials on your organization’s RPs. You can then move these RPs to their final locations and be sure that only these RPs can connect to your network.

Configuring 802.1X Authentication for RPs

To configure 802.1X authentication for RPs, complete these steps:

1. Select **Network Setup > Radio > Configuration**.
2. Click the **Global Settings** button. The **Global** screen is displayed.

   ![Figure 2-45. Radio Global Settings Screen](image)

3. Click the **Configure Port Authentication** button. The **Configure Port Authentication screen** is displayed.
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Adoption

4. Configure a username and password.
   - Check the Use Default Values box to use the default username and password:
     - username: admin
     - password: procurve
   - Or, in the Username and Password fields, enter the username and password that you want to use.

5. Click the OK button, and then click the OK button on the Global screen.

**Note**

The Wireless Edge Services zl Module pushes the username and password to the RPs as a one time occurrence. You must complete these steps again to configure the username and password on an RP that is adopted later.

6. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.
System Maintenance

The Web browser interface allows you to manage:

■ software images
■ configuration files
■ SNMP support
■ password encryption

Software Images

The Wireless Edge Services zl Module maintains two software images:

■ primary
■ secondary

Typically, the primary image loads when the Wireless Edge Services zl Module is rebooted. However, you can configure the module to reboot with either the primary or the secondary image.

The two images provide failover capabilities in the event that one software image becomes corrupted. If a software image fails to initialize completely during two consecutive reboots, the Wireless Edge Services zl Module automatically boots with the other image.

Having two images also simplifies the update process. For example, you can boot the Wireless Edge Services zl Module with the secondary image and then update the primary image. Likewise, you can boot the module with the primary image and update the secondary image. After you upgrade the software and reboot the module, the module, by default, loads the upgraded image.

ProCurve Networking uses the following naming convention for software image files:

\texttt{WT.xx.yy}

The \texttt{xx} is replaced with numbers that indicate a major release of the software image. The \texttt{yy} is replaced with numbers that indicate a minor release of the software.
Viewing the Software Images

To view the version of the primary and secondary images, access the **Management > System Maint.—Software** screen. (See Figure 2-47.)

<table>
<thead>
<tr>
<th>Image</th>
<th>Version</th>
<th>Current Boot</th>
<th>Next Boot</th>
<th>Exit Time</th>
<th>Install Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>WS-1.0.27953</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary</td>
<td>WS-1.0.27953</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2-47. Management > System Maint.—Software Screen**

The **Management > System Maint.—Software** screen includes the following fields:

- **Image**—This field indicates whether the image is the primary or secondary image.
- **Version**—This field displays the version number of the image file.
- **Current Boot**—This field indicates whether or not the image was used the last time that the Wireless Edge Services zl Module was rebooted. A green check mark indicates that the image was used; a red x indicates that the image was not used.
- **Next Boot**—This field determines whether the software image will be used to boot the Wireless Edge Services zl Module the next time the module is reloaded. A green check mark indicates that the image will be used; a red x indicates that the image will not be used.
Configuring the ProCurve Wireless Edge Services zl Module

System Maintenance

- **Built Time**—This field reports the date and time that this software image was created.
- **Install Time**—This field reports the date and time that this software image was updated on the Wireless Edge Services zl Module.

Selecting the Software Image That Is Used to Reboot

You can specify which software image the Wireless Edge Services zl Module will use the next time it is rebooted—the primary or the secondary. Complete these steps:

1. Select **Management > System Maint.— Software**.
2. Select the software image that the Wireless Edge Services zl Module should use to boot. For example, if you want the module to boot with the secondary image, select that image.
3. Click the **Edit** button at the bottom of the screen.

![Figure 2-48. Update Software Image Dialog Box](image)

4. Check the **Use this software on next reboot** box, and then click the **OK** button.
5. Click the **Save** link at the top of the Web browser interface to save this change to the startup-config.

Changing the Image Failover Setting

When the Wireless Edge Services zl Module reboots, it attempts to initialize the software image that you have selected for the next reboot. If this attempt fails, the module tries one more time to initialize the software image. If this second consecutive attempt fails, by default the module automatically reboots using the other software image.
If you do not want the Wireless Edge Services zl Module to automatically reboot using the other image, you can disable this failover capability. Complete these steps:

1. Select **Management > System Maint.—Software**.

   ![Figure 2-49. Management > System Maint.—Software Screen](image-url)

   **Management > System Maint. - Software**

   - **Image Failover is enabled**
   - **Use Global Settings to disable it**

   **Show Filtering Options**

<table>
<thead>
<tr>
<th>Image</th>
<th>Version</th>
<th>Current Boot</th>
<th>Next Boot</th>
<th>Built Time</th>
<th>Install Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>W5.1.0.27331</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary</td>
<td>W5.1.0.27331</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   **Filtering is disabled**

   ![Figure 2-50. Global Settings Screen for Software](image-url)

2. Click the **Global Settings** button at the bottom of the screen. The **Software Global Settings** screen is displayed.

   ![Figure 2-50. Global Settings Screen for Software](image-url)
3. Uncheck the **Enable Image Failover** box, and then click the **OK** button. The change is applied to the running-config.

4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

### Manually Updating the Software Image

ProCurve Networking periodically updates the software image for the Wireless Edge Services zl Module. You can configure the module to automatically contact an Update Server and download the new image when the module is rebooted, or you can manually update the image. (To configure settings for automatic updates, see “Update Server” on page 2-98.)

To manually update an image, complete these steps:

1. Select **Management > System Maint.—Software**.

2. Click the **Upgrade Software** button at the bottom of the screen. The **Update** screen is displayed.

   The software image that you upload will automatically copy to the image not currently in use.

3. In the **From** field, accept the default setting, **Server**.

4. In the **File** field, enter the name of the new image file.
5. In the **Using** field, use the drop-down menu to select **FTP** or **TFTP**, depending on the type of server that you have.

6. In the **Port** field, if needed, change the port number for your FTP or TFTP server. In most cases, the defaults (port 21 for FTP, port 69 for TFTP) should apply to your server.

7. In the **IP Address** field, enter the IP address of the FTP or TFTP server.

8. If you are using an FTP server, enter the login credentials for that server.
   a. In the **User ID** field, enter the username.
   b. In the **Password** field, enter the password for this username.

9. In the **Path** field, enter the path where the new image file is saved. If you are using an FTP server and the image file is saved at the server's root level, enter a period followed by a slash (/). If the image file resides at a different level on the FTP server, enter the complete path. (If you are using a TFTP server, this field may not be required.)

10. Click the **Do Upgrade** button.

**Configuration Files**

The Wireless Edge Services zl Module ships with a factory default startup-config file. Factory default settings include:
- support for HTTP and HTTPS
- support for SNMP v1, v2, and v3
- DHCP-assigned IP address for the default management interface (VLAN 1)

As you configure the Wireless Edge Services zl Module and save changes, these changes are saved to the startup-config. From the Web browser interface, you can view the commands included in the startup-config file, or you can return the startup-config file to factory default settings.

For backup purposes, you can save the startup-config file to:
- FTP server
- TFTP server
- workstation's hard disk

In addition, you can save multiple configuration files and store them in the module's internal flash. As Table 2-3 shows, configuration files are stored in two locations in the module's internal flash.
Table 2-3. Configuration Files Stored in Internal Flash

<table>
<thead>
<tr>
<th>Name of Configuration File</th>
<th>Location in Internal Flash</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>NVRAM</td>
</tr>
<tr>
<td>other configuration files</td>
<td>flash</td>
</tr>
</tbody>
</table>

Viewing Configuration Files

To view a configuration file, select **Management > System Maint.—Config Files**. As shown in Figure 2-52, this screen displays the following information about each configuration file saved in flash:

- **Name**
- **Size (Bytes)**
- **Created**—date and time when the file was created
- **Modified**—date and time when the file was last changed

![Management > System Maint. - Config Files](image)

Figure 2-52. Management > System Maint.—Config Files
To view the contents of a configuration file, select the file and click the View button at the bottom of the screen. For example, you might want to view the startup-config file. (See Figure 2-53.)

![Figure 2-53. Viewing the Contents of the startup-config](image)

Click the Refresh button to update the information displayed in the screen.

Click the Close button to return to the Management > System Maint.—Config Files screen.
Transferring, or Copying, Files

The Web browser interface allows you to transfer, or copy, configuration files. You simply specify a source and a destination for the transfer. Valid selections are listed in Table 2-4:

<table>
<thead>
<tr>
<th>From (Source)</th>
<th>To (Destination)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server—either an FTP or TFTP server</td>
<td>Wireless Edge Services zl Module</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module</td>
<td>• Wireless Edge Services zl Module</td>
</tr>
<tr>
<td></td>
<td>• Local disk</td>
</tr>
<tr>
<td></td>
<td>• Server—either an FTP or TFTP server</td>
</tr>
</tbody>
</table>

When you select a source, the Web browser interface displays the fields that are needed to copy a configuration file from that source. Likewise, when you select a destination, the Web browser interface displays the fields that are needed to copy a file to that destination. For example, to copy a file from a TFTP server, you must specify fields such as the IP address and the name of the file.

Transferring Configuration Files from an FTP or TFTP Server to the Wireless Edge Services zl Module

To upload a configuration file from an FTP or TFTP server to the Wireless Edge Services zl Module, complete these steps:

1. Select **Management > System Maint.—Config Files**.
2. Click the **Transfer Files** button at the bottom of the screen. The **Transfer** screen is displayed. (See Figure 2-54.)
3. In the Source section, specify the source as an FTP or TFTP server:
   a. In the From field, use the drop-down menu to select Server.
   b. In the File field, enter the name of the configuration file.
   c. In the Using field, use the drop-down menu to select either FTP or TFTP.
   d. In the Port field, if needed, change the port number for your FTP or TFTP server. In most cases, the defaults (port 21 for FTP, port 69 for TFTP) should apply to your server.
   e. In the IP Address field, enter the IP address of the FTP or TFTP server.
   f. If you are using an FTP server, enter the login credentials.
      i. In the User ID field, enter the username for the FTP server.
      ii. In the Password field, enter the password for this username.
   g. In the Path field, enter the path where the configuration file is saved on the server.

   If you are using an FTP server and the configuration file is saved at the server's root level, enter a period followed by a slash (./). If the configuration file resides at a different level on the FTP server, enter the complete path. If you are using a TFTP server, this field may not be required. However, enter the path if the file is stored in a subdirectory on the TFTP server.
4. In the Target section, specify the destination as the Wireless Edge Services zl Module:
   a. In the To field, use the drop-down menu to select **Wireless Services Module**.
   b. In the File field, enter the name that you want to give to the configuration file.

5. Click the Transfer button. In the Status section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

Transferring Configuration Files from the Wireless Edge Services zl Module to Another Destination

You can copy a configuration file from the Wireless Edge Services zl Module to the module itself, an FTP server, a TFTP server, or the hard disk of your workstation. Complete these steps:

1. Select **Management > System Maint.—Config Files**.

2. In the Source section, specify the source as the Wireless Edge Services zl Module:
   a. In the Source section, in the From field, use the drop-down menu to select **Wireless Services Module**.

   
   ![Figure 2-55. Management > System Maint.—Config Files > Transfer Screen](image)

   b. In the File field, use the drop-down menu to select the file that you want to copy.
3. In the **Target** section, specify the destination. Choose a destination from the **To** drop-down menu:

- **Wireless Services Module**—copy the file to another location on the module
- **Server**—copy the file to an external FTP or TFTP server
- **Local Disk**—copy the file to the workstation on which you are running the Web browser

The **Target** fields below change depending on the target type. The following three sections give you guidelines for filling in the necessary information.

**Copying a File to the Wireless Edge Services zl Module.** You can copy a file on the Wireless Edge Services zl Module to an new location on the module. For example, you might want to copy a logo used for Web-Auth on one WLAN to another WLAN. Follow these steps:

1. Complete steps 1 to 3 in “Transferring Configuration Files from the Wireless Edge Services zl Module to Another Destination” on page 2-91.

2. In the **File** field, enter the name that you want to give to the configuration file.

   The filename should include the path for the location in the module's memory to which you want to save the file.

3. You can use the Browse button to search the module's directory and even create a new folder for the file. See “Managing the Directory Structure and Browsing for Files” on page 2-95 for more information.

4. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.
Figure 2-56. Transferring a File to a New Location on the Module

At any point during the transfer, you can click the **Abort** button to cancel the process.

After you have finished transferring files, click the **Close** button.

**Copying a File to an External Server.** Follow these steps to upload a file to an external FTP or TFTP server:

1. Complete steps 1 to 3 in “Transferring Configuration Files from the Wireless Edge Services zl Module to Another Destination” on page 2-91.
2. In the **File** field, enter the name of the configuration file.
3. In the **Using** field, use the drop-down menu to select either **FTP** or **TFTP**.
4. In the **Port** field, if needed, change the port number for your FTP or TFTP server. In most cases, the defaults (port 21 for FTP, port 69 for TFTP) should apply to your server.
5. In the **IP Address** field, enter the IP address of the FTP or TFTP server.
6. If you are using an FTP server, enter a username in the **User ID** field and enter the password in the **Password** field.
7. In the **Path** field, enter the path where the configuration is saved on the server. (Depending on your server, this field may not be required.)

For some FTP servers, you might need to enter / even if the file is stored in server's default directory.
8. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

At any point during the transfer, you can click the **Abort** button to cancel the process.

After you have finished transferring files, click the **Close** button.

**Copying a File to the Local Disk.** To specify the local hard disk as the destination, follow these steps:

1. Complete steps 1 to 3 in “Transferring Configuration Files from the Wireless Edge Services zl Module to Another Destination” on page 2-91.
2. In the **File** field, enter the name that you want to give to the file.
3. Use the **Browse** button to select the directory in which you want to store this configuration file. See “Managing the Directory Structure and Browsing for Files” on page 2-95 for more information.

---

![Figure 2-57. Transferring a File to the Local Disk](image)

4. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

At any point during the transfer, you can click the **Abort** button to cancel the process.

After you have finished transferring files, click the **Close** button.
Managing the Directory Structure and Browsing for Files

The Browse button appears when choosing where to download files to the Wireless Edge Services zl Module.

Figure 2-58. Browse Button

To use the browse button to search and manage the Wireless Edge Services zl Module's directory structure, follow these steps:

1. In the Target section, click the Browse button next to the File field. The Select Config file screen is displayed.

   This screen displays three buttons, one for each of the Wireless Edge Services zl Module's three file systems:
   - system:
   - nvram:
   - flash:

2. Click one of the buttons at the top of the screen to choose the file system to which to save the file.

   When you first open the screen, flash: is selected.

   The section at the left of the screen lists directories, or folders, within this file system. For example, at factory settings, flash memory includes the four folders shown in Figure 2-59.
The nvram stores the startup-config, and the system memory (volatile) holds the running-config.

3. In the left section, choose the folder in which you want to save the file.
4. Alternatively, create a new folder (in the flash memory only).
   a. Click the **New Folder** button. The **New Folder** screen is displayed.

   ![New Folder Screen](image)

   **Figure 2-60. New Folder Screen**

   b. Name the folder and click the **OK** button.
   c. Your new folder is displayed in the left section of the **Select Config file** screen. Select this folder.
5. Choose the filename.

The path to the folder you have selected is displayed in the field at the bottom of the screen. Files in this folder display to the right. You can select one of these files and write over it, or you can choose a new file. To create a new file add the filename to the path in the field at the bottom of the screen. For example: flash/myfolder/configA.

6. Click the **OK** button.

7. The path and filename that you have selected are displayed in the **File** field.

8. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

**Deleting a Configuration File**

From the **Management > System Maint.—Config Files** screen, you can delete any configuration file that is stored in flash—except the startup-config file. To delete a configuration file, complete these steps:

1. Select the configuration file and click the **Delete** button. As shown in Figure 2-61, you will be prompted to confirm that you want to delete this configuration file.

   ![Confirm File Delete](image_url)

   **Figure 2-61. Confirm File Delete Prompt**

2. Click the **Yes** button to delete the file.

**Note**

If you attempt to delete the startup-config file, the Web browser interface allows you to go through the steps of deleting the file, but when you confirm that you want to delete the file, the following message is displayed at the bottom of the navigation bar:

**You have selected the system startup-config file. This file cannot be edited.**
Rather than trying to delete the startup-config file when you are using the Web browser interface, you should return the file to factory default settings, as explained in the next section. (You can enter the `erase` command in the CLI to delete the startup-config. The module then uses the factory default startup-config file.)

Returning the Startup-Config File to Factory Default Settings

Although you cannot delete the startup-config file if you are using the Web browser interface, you can return this file to factory defaults. Complete these steps:

1. On the Management > System Maint.—Config Files screen, click the Restore Defaults button. A prompt is displayed, asking you to verify that you want to return the startup-config file to factory defaults.

![Restore Factory Defaults Prompt](image)

2. Click the Yes button if you want to revert to factory settings. A prompt is displayed, telling you that the Wireless Edge Services zl Module must be rebooted in order for the change to take effect.

3. Click the Yes button to reboot the module.

Update Server

The Wireless Edge Services zl Module can communicate with an Update Server, on which you can store backup copies of the software image and the configuration file for your Wireless Edge Services zl Module. If the module’s software image or configuration file becomes corrupted, you can reboot the module, and it will retrieve the necessary file from the Update Server—provided you have configured the Update Server settings correctly and copied the necessary files to the Update Server.

When you configure the Update Server on the Wireless Edge Services zl Module, you define the following:

- IP address of the Update Server
- protocol of the Update Server (FTP or TFTP)
server username and password (for FTP server)
location of the software image on the Update Server
software image that the module should use
location of configuration file
location of a redundancy configuration file—a common configuration for an entire redundancy group, an optional supplement to (not replacement for) the configuration file

Checking the Software Image File

When the Wireless Edge Services zl Module reboots, it checks the Update Server settings that you have configured to ensure that it is using the correct software image. If the module is already using the software image that you specified, it simply reboots and then checks the configuration file. (See “Checking the Configuration File” on page 2-99.)

However, if you have specified a different software image for the Update Server settings, the module requests that image from the Update Server. For example, if you configure the Update Server settings and specify that the software image is WS.1.1, the module first checks its own software image file to see if it is using WS.1.1. If the module is using WS.1.1, it reboots with this image. If the module is using a different image—such as WS.1.0—it contacts the Update Server and requests the WS.1.1 image. If the Update Server has the WS.1.1 image and sends it, the module boots with WS.1.1.

Whenever the module requests the software image file from the Update Server, it also requests the configuration file. The configuration file that the Update Server sends must be exactly the same as the startup-config saved on the module. You can ensure that these files are the same by always saving the latest startup-config to the Update Server.

Checking the Configuration File

The configuration file is handled slightly differently from the software image. For the configuration file, the Update Server is designed to recover a corrupted configuration file. It is not intended to deploy new configurations.

You cannot define the configuration file in the Update Server settings. The Wireless Edge Services zl Module always requests the startup-config. When you define the **File Name (with Path)** field in the Update Server settings, you define the location of the startup-config file on the Update Server.
Whatever name you give the file that you save to the Update Server, it should always contain the same configuration that is saved on the module’s startup-config. When you change the startup-config, you should immediately copy the new file to the Update Server.

When you save the startup-config file and the Update Server is enabled, the Wireless Edge Services zl Module saves a checksum of the startup-config. When the Wireless Edge Services zl Module reboots, it compares the checksum it saved with the checksum of the startup-config that it loads. If the two checksums match, the module boots normally with the startup-config.

If the startup-config is corrupted, the checksums will not match, and the module will request the configuration file from the location specified in the Update Server settings. When the module receives the configuration file from the Update Server, it compares the checksum that it saved for the startup-config with this file’s checksum. If the two checksums match, the module loads the configuration file that it received from the Update Server.

If the two checksums do not match, the module assumes that the Update Server does not have the correct configuration file. The module boots with the factory default startup-config.

However, you can configure the Wireless Edge Services zl Module to ignore the checksum and always use the startup-config file sent by the Update Server. This option is called forcing the config update.

**Avoiding Problems in Using the Update Server**

To ensure that the Wireless Edge Services zl Module does not boot with the wrong software image or the factory default settings, follow these guidelines:

- Keep the Update Server settings current.

  For example, if you upgrade the software image on the Wireless Edge Services zl Module, you must save the new software image to the Update Server and change the software image file defined in the module’s Update Server settings. If the Update Server settings specify an older software image, the module will attempt to use this older software image the next time that it is rebooted.

  Alternatively, you can also force the Update Server to upload the configuration file whether or not the checksum matches. While perhaps less secure, this option prevents the Wireless Edge Services zl Module from reverting to factory default settings when you do not follow the above guidelines exactly.
Ensure that the Update Server is available when the Wireless Edge Services zl Module reboots.

If the module must request an image or configuration file, but the Update Server is unavailable for any reason, the module uses its current image to reboot and loads the factory default startup-config.

Ensure that the latest software image and a file named “startup-config” are saved on the Update Server.

Problems can occur if the Update Server does not have the specified software image or a file name “startup-config.” In this case, the module boots with its primary image and the factory defaults.

Figure 2-63. Forcing the Update Server to Upload the Configuration File Whether or Not the Checksums Match
Table 2-5 lists the image and configuration file that the Wireless Edge Services zl Module uses if:

- the image file specified in the Update Server settings is the image file that the module is already using
- the Update Server is enabled, but no settings are configured for the image file and the configuration file location
- the Update Server is unavailable

Table 2-5. Image and Configuration Files Loaded when an Update Server Is Defined

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1 Startup-config</td>
<td>Image 1 Startup-config</td>
<td>Does not matter</td>
<td>Does not matter</td>
</tr>
<tr>
<td>Image 1</td>
<td>Not set</td>
<td>Does not matter</td>
<td>Image 1</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 1 Startup-config</td>
<td>Does not matter</td>
<td>Image 1</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 2 Startup-config</td>
<td>Update Server is unavailable or file location is incorrect</td>
<td>Image 1 Factory default startup-config</td>
</tr>
<tr>
<td>Image 1</td>
<td>Image 2 Startup-config</td>
<td>Update Server is unavailable or file locations are incorrect</td>
<td>Image 1 Factory default startup-config</td>
</tr>
</tbody>
</table>

If the Wireless Edge Services zl Module cannot reach the Update Server, it disables the Update Server settings. On the Management > System Maint.—Update Server screen, the Update Server Unreachable box is checked. To enable the Update Server once again, you must manually uncheck this box.
Table 2-6 shows which software image and configuration file are loaded in other circumstances.

**Table 2-6. Image and Configuration Files Loaded when an Update Server Is Defined**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1 Startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 2 Matches startup-config</td>
<td>Image 2 Startup-config</td>
</tr>
<tr>
<td>Image 1 Startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 2 Does not match startup-config</td>
<td>Image 2 Factory default startup-config</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 1 Startup-config</td>
<td>Does not matter Matches startup-config</td>
<td>Image 1 Startup-config</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 1 Startup-config</td>
<td>Does not matter Does not match startup-config</td>
<td>Image 1 Factory default startup-config</td>
</tr>
<tr>
<td>Image 1 Startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 3 Matches startup-config</td>
<td>Image 1 Factory default startup-config</td>
</tr>
<tr>
<td>Image 1 Startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 3 Does not match startup-config</td>
<td>Image 1 Factory default startup-config</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 2 Matches startup-config</td>
<td>Image 2 Startup-config</td>
</tr>
<tr>
<td>Image 1 Corrupted startup-config</td>
<td>Image 2 Startup-config</td>
<td>Image 2 Does not match startup-config</td>
<td>Image 2 Factory default startup-config</td>
</tr>
</tbody>
</table>
Configuring the Update Server Settings

To configure the Update Server settings, complete these steps:

1. Select **Management > System Maint.—Update Server**.

2. Check the **Update Server Unreachable** box if you do not want the Wireless Edge Services zl Module to use the Update Server.

3. In the **IP Address** field, enter the IP address of the FTP or TFTP server on which the software image is saved.

4. In the **Transfer Protocol** field, use the drop-down menu to specify whether the Update Server is an FTP server or a TFTP server.
5. Enter the login credentials for the FTP server.
   a. In the User ID field, enter the username.
   b. In the Password field, enter the password for this username.

6. In the Software section, configure the version number, filename and path for the software image.
   a. In the Version field, enter the version of the software image that is stored on the FTP or TFTP server.
   b. In the File Name (with Path) field, enter the name of the file that contains the software image and the path to that filename (if the path is required by the Update Server). If you are using an FTP server and the configuration file is saved at the server's root level, enter a period followed by a slash (./) for the path. If the configuration file resides at a different level on the FTP server, enter the complete path. (If you are using a TFTP server, this field may not be required.)

7. In the Configuration File section, in the File Name (with Path) field, enter the name of the file that contains the configuration and the path to that filename (if the path is required by the Update Server).

8. If your Wireless Edge Services zl Module is a member of a redundancy group, you should store a common configuration for all members on the Update Server. Specify the name and path for this common configuration in the Redundancy File Name (with Path) field.

   The file specified in the File Name (with Path) field should include individualized settings, such as IP address, for this particular module. You must specify the individualized configuration. The redundancy configuration alone is not sufficient.

9. Click the Apply button to save your changes to the running-config.

10. Click the Save button in the navigation bar to save your changes to the startup-up config.

**Password Encryption**

The Wireless Edge Services zl Module might store a variety of passwords. Encryption prevents someone from accessing the module's configuration file (whether through the CLI or an insecurely transmitted file) and reading the passwords.
By default, only two types of passwords are encrypted when you view the configuration:
- SNMP v3 user passwords
- Web-User passwords (encrypted by SHA)

Other types display in plaintext, by default:
- passwords for users in the local RADIUS database
- shared secrets for the RADIUS servers specified in WLAN settings
- shared secret for globally configured RADIUS servers (used for authentication, authorization, and accounting [AAA])
- WEP keys
- WPA/WPA2 preshared keys (PSK)

However, you can configure SHA256-AES256 encryption for these five types of passwords. In addition to obscuring the passwords in the configuration file, encryption protects passwords that the module might send over the wire to facilitate seamless Layer 2 roaming for Web-Auth.

To enable password encryption, configure the encryption secret. The Wireless Edge Services zl Module uses this secret to encrypt:
- all previously configured passwords of the five types listed above
  - The SNMP v3 and Web-User passwords (by default, encrypted) are unaffected by the password encryption configuration.
- all new passwords of the five types listed above
- all Web-Auth passwords that the module sends to other modules in order to facilitate roaming

Make sure to configure the same password on all modules.

To configure the encryption key, follow these steps:

1. Select Management.
2. Click the **ConfigPasswdEn** button.

![Figure 2-65. ConfigPasswdEn Button](image)

![Figure 2-66. ConfigPasswdEncryption Screen](image)
3. Set the key that encrypts passwords in the **Password** and **Confirm Password** fields.

   The key can be between 8 and 32 alphanumeric and special characters.

4. Click the **OK** button.

To disable password encryption, you must access the CLI and enter this command from the global configuration mode context:

```
ProCurve(wireless-services-C)(config)# no password-encryption
```

All previously configured passwords, as well as all new passwords, now are displayed in plaintext.

You cannot disable password encryption from the Web browser interface.
SNMP is an industry-standard protocol that allows you to manage and monitor a variety of network devices from a central location. Specifically, you can configure these SNMP-compliant devices and apply consistent security and management policies to these devices across your network. By default, the Wireless Edge Services zl Module supports SNMP v1, v2, and v3.

In addition to providing support for SNMP applications, SNMP v3 is required for the Web browser interface to function. If you attempt to disable support for SNMP v3, a warning message is displayed. Disabling SNMP v3 also disables the applet required for the Web browser interface, and you will be logged out. You will be unable to access the Web browser interface until you enable SNMP v3 again.

SNMP support also enables you to set up alarms on the Wireless Edge Services zl Module. You simply enable the SNMP traps for the alarms you want to log. (For more information, see “Enabling SNMP Traps” on page 2-113.)

SNMP Communities

The Wireless Edge Services zl Modules uses the following community names:
- public
- private
- trap

Each community name is assigned an access control, which determines the operations an SNMP server can complete on the Wireless Edge Services zl Module:
- Read-only—The SNMP server can retrieve information from the module.
- Read-write—The SNMP server can retrieve information and modify the configuration settings.

By default, the public and trap communities have read-only access, and the private community has read-write access.

The Wireless Edge Services zl Module uses the following SNMP v1/c2 community names:
- public
- private
- trap
You can also set up traps using the SNMP v3 trap user.

Modifying SNMP v2 Communities

By default, the Wireless Edge Services zl Module names the read-only community “public” and the read-write community private. To change the community name or access control setting for these communities, complete these steps:

1. Select **Management > SNMP Access > v1/v2c**.

![Figure 2-67. Management > SNMP Access > V1/V2c Screen](image)

2. Select the community that you want to modify, and then click the **Edit** button. The **Edit SnmpV1/V2c** screen is displayed. (See Figure 2-68.)
3. In the **Community Name** field, enter the new name for the community.

4. In the **Access Control** field, use the drop-down menu to select the access control.

5. Click the **OK** button. The changes are applied to the running-config.

6. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**SNMP Statistics**

You can view a number of SNMP statistics. To understand these statistics, you should know the five basic messages exchanged between SNMP servers and agents:

- **GET**—SNMP servers send a GET message to request information about a setting.
- **GET-NEXT**—SNMP servers send a GET-NEXT message to request information about several SNMP objects in the device.
- **SET**—SNMP servers send a SET message to modify a configuration setting. Servers must have read-write access to make configuration changes.
- **GET-RESPONSE**—In response to a GET, GET-NEXT, or SET message, SNMP agents send a GET-RESPONSE message. This message includes one of the following:
  - requested information
  - confirmation that the requested change was made
  - error that explains why the agent cannot supply the requested information or make the requested change
- **TRAP**—SNMP agents use TRAP messages to report events.

Many SNMP statistics reference these messages.
To view SNMP statistics, select **Management > SNMP Access** and click the **Statistics** tab.

![Management > SNMP Access > Statistics Screen](image)

## SNMP Traps

To generate alarm logs, you must enable the Wireless Edge Services zl Module to generate SNMP traps, and you must enable specific SNMP traps. For example, you may want the module to generate an alarm if file system space becomes low or if a user fails to authenticate.

After you enable the SNMP trap function and the specific traps you want, the Wireless Edge Services zl Module will begin to log events that match the SNMP traps you have enabled. In addition to viewing these logs through the Web browser interface, you can configure the Wireless Edge Services zl Module to send the SNMP trap information to your SNMP server. (For information about viewing logs through the Web browser interface, see “Configuring Logging” on page 12-64 in Chapter 12: “Wireless Network Management.”)
Enabling SNMP Traps

By default, all SNMP traps are disabled. To enable SNMP traps, complete these steps:

1. Select **Management > SNMP Trap Configuration** and click the **Configuration** tab.

![Management > SNMP Trap Configuration Screen](image)

**Figure 2-70. Management > SNMP Trap Configuration Screen**
The SNMP traps for the Wireless Edge Services zl Module are divided into the following categories:

- Redundancy
- Miscellaneous
- NSM
- Mobility
- DHCP
- Radius
- SNMP
- Wireless

2. Check the **Allow Traps to be generated** box.

3. To view the SNMP traps in a category, click the Plus ( + ) sign next to the category. To view the SNMP traps in all categories, click the **Expand all items** button.

4. To enable all the traps, select **All Traps** and click the **Enable all sub-items** button.

5. To enable all the SNMP traps in a category, select the category and click the **Enable all sub-items** button.

6. To enable a specific SNMP trap, select the trap and click the **Enable** button or double-click the trap. A green check mark is displayed next to enabled traps. A red x is displayed next to disabled traps.
7. Click the **Apply** button to save the change to the running-config.

8. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

### Disabling SNMP Traps

To disable an SNMP trap that you previously enabled, complete these steps:

1. Select **Management > SNMP Trap Configuration** and click the **Configuration** tab.

2. To disable a specific SNMP trap, expand the **SNMP** category. Select the SNMP trap that you want to disable, and then click the **Disable** button, or double-click the SNMP trap.

3. To disable all the SNMP traps in a category, select the category and click the **Disable all sub-items** button.
Configuring the ProCurve Wireless Edge Services zl Module

SNMP Traps and Error Reporting

4. Click the **Apply** button to save the change to the running-config.

5. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Setting Thresholds

You can set the thresholds that determine when SNMP traps are generated. Select Management > SNMP Trap Configuration and click the **Wireless Statistics Thresholds** tab.

![Management > SNMP Trap Configuration > Wireless Statistics Thresholds Screen](image)

Table 2-7 shows which thresholds you can set for stations, radios, and WLANs, and for the Wireless Edge Services zl Module itself.

![Table showing SNMP Trap Configuration thresholds](image)
Table 2-7. Wireless Statistics Thresholds

<table>
<thead>
<tr>
<th>Thresholds</th>
<th>Set for Station, Radio, WLAN, or Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Per Second</td>
<td>Station, radio, WLAN, or module</td>
</tr>
<tr>
<td>Throughput</td>
<td>Station, radio, WLAN, or module</td>
</tr>
<tr>
<td>Average Bit Speed</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Average Station Signal</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Non-Unicast Packets</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Transmitted Packet Dropped</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Transmitted Packet Average Retries</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Undecrypt Received Packets</td>
<td>Station, radio, or WLAN</td>
</tr>
<tr>
<td>Total Stations</td>
<td>Radio, WLAN, or module</td>
</tr>
</tbody>
</table>

You can also configure the minimum number of packets required to send an SNMP trap. By default, the minimum number of packets is 1,000.

Sending Traps to an SNMP Receiver

SNMP agents send only one type of unsolicited message: trap messages. SNMP agents send trap messages to report events. These messages enable the SNMP server to generate logs and alarms. You can configure SNMP trap receivers—the SNMP servers to which the Wireless Edge Services zl Module sends trap messages.

The module can send two types of traps:
- **v2c traps**—always use public for the community name
- **v3 traps**—use the trap username and password (see “Change the Password for SNMP v3 Traps” on page 2-119)

**Define an SNMP Server.** To define an SNMP server, complete these steps:

1. Select Management > SNMP Trap Receivers.
SNMP Traps and Error Reporting

2. Click the **Add** button. The **Add Trap receivers** screen is displayed.

3. In the **IP Address** field, enter the IP address of the SNMP server.
4. In the **Port Number** field, enter the port on which your SNMP server listens for traps.

   The valid range is from 1 to 65535. The default port is 162.

5. Choose **v2c** or **v3** from the **Protocol Options** drop-down menu.

6. Click the **OK** button. The configuration change is applied to the running-config.

7. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**Change the Password for SNMP v3 Traps.** When an SNMP v3 server receives a trap, it checks the username and password of the sender. The Wireless Edge Services zl Module uses the trap profile to send SNMP v3 traps.

   The username for this trap is always trap, but you can change the password. Follow these steps:

   1. Select **Management > SNMP Access** and click the **V3** tab.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access Control</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>trap</td>
<td>Read Only</td>
<td>HMAC-MD5</td>
<td>CBC-DES</td>
<td>Active</td>
</tr>
<tr>
<td>manager</td>
<td>Read Write</td>
<td>HMAC-MD5</td>
<td>CBC-DES</td>
<td>Active</td>
</tr>
<tr>
<td>operator</td>
<td>Read Only</td>
<td>HMAC-MD5</td>
<td>CBC-DES</td>
<td>Active</td>
</tr>
</tbody>
</table>

**Figure 2-75. Management > SNMP Access > V3 Screen**
2. Select the **trap** user and click the **Edit** button.

![Configuration Page](image)

**Figure 2-76. Changing the Password for SNMP v3 Traps**

3. In the **Old Password** field, enter the current password—by default, “procurve.”

4. In the **New Password** and **Confirm Password** fields, enter the new password.

5. Click the **OK** button.
View Information about SNMP Receivers. After you define an SNMP server, the server is displayed in the Management > SNMP Trap Receivers screen.

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Port</th>
<th>Community String/ User Name</th>
<th>Retry Count</th>
<th>Timeout</th>
<th>Trap Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.20</td>
<td>162</td>
<td>public</td>
<td>3</td>
<td>1500V2x</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2-77. Management > SNMP Trap Receivers Screen

You can view the following information about that server:
- **Destination Address**—the IP address of the SNMP server
- **Port**—the port number that the module uses to communicate with the SNMP server. By default, the module uses port 162.
- **Community String/User Name**—the community string for the trap. Receivers are automatically assigned to the public community.
- **Retry Count**—the number of times that the Wireless Edge Services zl Module will try to contact the SNMP server
- **Timeout**—the number of seconds that the Wireless Edge Services zl Module waits for a response from the SNMP server before ending the session
- **Trap Version**—the version of the SNMP trap sent to the SNMP server
Edit an SNMP Trap Receiver. If you define an SNMP trap receiver and later need to change its IP address, complete these steps:

1. Select **Management > SNMP Trap Receivers**.
2. Click the **Edit** button.
3. You can change these settings:
   - IP address
   - port

To change the SNMP version, you must delete the receiver from the **Management > SNMP Trap Receivers** screen and re-add it with the correct version.

4. Click the **OK** button.
5. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

---

Radio Port Licenses

Each Wireless Edge Services zl Module (J9051A) ships with 12 nonremovable RP licenses. When you install the Wireless Edge Services zl Module into a switch, the module can automatically adopt up to 12 RPs. If you move the Wireless Edge Services zl Module to another switch, these 12 RP licenses move with the module. They cannot be uninstalled or transferred to another Wireless Edge Services zl Module.

If you want to manage more than 12 RPs through a Wireless Edge Services zl Module, you can purchase and install additive licenses. You can purchase two types of additive licenses:

- a license which allows the Wireless Edge Services zl Module to adopt 12 additional RPs
- a license which allows the Wireless Edge Services zl Module to adopt 48 additional RPs

You can install multiple licenses; the Wireless Edge Services zl Module can adopt a maximum of 156 RPs. Because each RP has a maximum of two radios, each Wireless Edge Services zl Module can manage up to 312 radios. Typically, you would add 12 RP Licenses when your module must support fewer than 60 RPs. If the module must support more than 60 RPs, install up to three 48 RP Licenses. (See Table 2-8.)
Table 2-8. RP Licenses and the Number of RPs Supported

<table>
<thead>
<tr>
<th>Products</th>
<th>Maximum Number of RPs</th>
<th>Maximum Number of Radios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>24</td>
<td>48</td>
</tr>
<tr>
<td>Wireless Services Module 12 RP License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>36</td>
<td>72</td>
</tr>
<tr>
<td>2 Wireless Services Module 12 RP Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>48</td>
<td>96</td>
</tr>
<tr>
<td>3 Wireless Services Module 12 RP Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>60</td>
<td>120</td>
</tr>
<tr>
<td>1 Wireless Services Module 48 RP License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>108</td>
<td>216</td>
</tr>
<tr>
<td>2 Wireless Services Module 48 RP Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Edge Services zl Module (J9051)</td>
<td>156</td>
<td>312</td>
</tr>
<tr>
<td>3 Wireless Services Module 48 RP Licenses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If you install additive RP licenses on a Wireless Edge Services zl Module, these licenses remain with the module if you move the module:

- from one slot to another slot in the same wireless services-enabled switch
- from one wireless services-enabled switch to another

It is possible, however, to move additive licenses—though not the default 12 RP license—from one Wireless Edge Services zl Module to another. For example, suppose your company's marketing department moved from the North building to the South building at your company's main office. Both buildings have a wireless services-enabled switch: the Wireless Edge Services zl Module in the North building has 108 RP licenses, and the Wireless Edge Services zl Module in the South building has 72 RP licenses. After you move the marketing department, there are fewer users in the North building, so you no longer need as many RP licenses in the North building. With the added users in the South building, however, you need more RP licenses on that Wireless Edge Services zl Module.
Figure 2-78. Sample Network with Additive Licenses Installed on the Wireless Services-Enabled Switch in the North Building
In situations such as this one, you can uninstall the Wireless Services Module 48 RP License from the Wireless Edge Services zl Module in the North building. You can then install the Wireless Services Module 48 RP License on the Wireless Edge Services zl Module in the South building. Now the North module supports 60 RPs while the South module supports 120.
Figure 2-79. Sample Network with Additive Licenses Installed on the Wireless Services-Enabled Switch in the South Building
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Licenses

Only the Wireless Edge Services zl Module has RP licenses. The Redundant Wireless Services zl Module does not include radio port licenses and cannot independently adopt radio ports. When the Redundant Wireless Services zl Module is configured as part of a redundancy group, however, it can adopt radio ports under certain circumstances (such as if the Wireless Edge Services zl Module fails or if it is assigned an active role).

Installing or Uninstalling Licenses on a Wireless Edge Services zl Module

You can use one of the following methods to install or uninstall RP licenses on the Wireless Edge Services zl Module:

- **Manual method**—You can use either the Web browser interface or the CLI to manually install and manage the Wireless Services Module 12 RP License or the Wireless Services Module 48 RP License. You may want to use the manual installation method if you are managing a small number of RP licenses or if you do not currently use ProCurve Manager.

- **ProCurve Manager**—You can use ProCurve Manager to install and uninstall the Wireless Services Module 12 RP License or the Wireless Services Module 48 RP License. If you do not currently use ProCurve Manager, you may find it worth installing. The CD-ROM that accompanies your licenses contains a copy of ProCurve Manager.

This management and configuration guide focuses on using the Web browser interface for the Wireless Edge Services zl Module.

Registering on the My ProCurve Web Portal

Whichever method you use to install or uninstall the Wireless Services Module 12 RP License or the 48 RP License, you must register on the My ProCurve Web portal (http://my.procurve.com). Registration is free and allows you to manage not only the Wireless Services Module RP Licenses but also licenses for other ProCurve products.

The My ProCurve Web portal allows you to:

- generate a license
- view the licenses that you have registered
- view your license history
- uninstall a license
- export license information to a spreadsheet
If you have not yet registered with the My ProCurve Web portal, visit http://my.procurve.com and follow the registration instructions.

Understanding the Numbers: IDs and Keys

Installing and uninstalling the Wireless Services Module 12 RP License or the Wireless Services Module 48 RP License involves several different numbers:

- **Registration ID**—The Wireless Services Module RP Licenses include a registration ID. You do not input this number to install the license. Instead, you enter this number on the My ProCurve Web portal, which then generates the license key that you enter to install the license.

- **Hardware ID**—This number identifies the Wireless Edge Services zl Module. It includes the module’s serial number and an identifier for the additional license.

- **License key**—The My ProCurve Web portal generates the license key, after you enter both the registration ID and the hardware ID. You must enter this number to enable the RPs that you are licensing.

- **Uninstall verification key**—This number is generated if you uninstall a radio-port license from a ProCurve device. If you want to install the Wireless Services Module RP License on another module, you use the uninstall verification key to generate a new registration ID on the My ProCurve portal.

Installing RP Licenses

If you decide to use the manual method to install the RP license, you must be able to access the My ProCurve Web portal and the Web browser interface for the Wireless Edge Services zl Module. For convenience, you should open two browsers so that you can move easily between the portal and the Web browser interface.

After you open two Web browsers, complete these steps:

1. Locate the registration ID for the Wireless Services Module 12 RP License or the Wireless Services Module 48 RP License. Place it within easy reach.


3. On the main My ProCurve page, click **My Software**. (See Figure 2-80.)
4. Click **ProCurve Device Software**. You can now begin to generate a license key. (See Figure 2-81.)
Figure 2-81. Enter the Registration ID

5. Enter the registration ID that you located in step 1 in the Registration ID field and click Next. The Hardware ID page is displayed.

6. Find out the hardware ID for the Wireless Edge Services zl Module.
   a. Open a second browser (if you have not already done so) and access the Web browser interface for the Wireless Edge Services zl Module.
   b. Select Management > Licenses and click the License-Install Summary tab. (See Figure 2-82.)
c. Click the Install button at the bottom of the screen. The Install License (Step 1 and Step 2) screen is displayed. (See Figure 2-83.)
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Licenses

d. In the Step 1—Generate Hardware ID section, click the Gen-Hw-ID button.
e. When a number is displayed in the System Generated Hardware Id field, copy it (using Ctrl-C) or write it down. (Copying the number is easier and more accurate.) You must enter this number on the My ProCurve Web portal.

7. Return to the My ProCurve Web portal. In the Enter Hardware ID# field, paste (using Ctrl-V) or enter the hardware ID.

8. Enter notes in the Customer Notes field. This field is optional. For example, you might want to enter a short description that explains where this Wireless Edge Services zl Module is located. These notes are stored, along with the registration ID number, in your account on the My ProCurve Web portal.

9. Click the Next button. The License Agreement page is displayed.

10. Read the license terms. If you agree to these terms, check the I agree to the license terms box.

11. Click the Generate License button. The My ProCurve Web portal generates a license key and displays it on the License Key Confirmation page. In addition, the portal emails you the license key.

12. Copy the license key (Ctrl-C) from the screen or write it down.

13. Return to the Install License (Step 1 and Step 2) screen in the Web browser interface for the Wireless Edge Services zl Module.

14. In the Step 2—Install License Key section, enter the license key and click the Lic-Install button. A message confirms a successful installation or identifies a problem that prevented the license from installing.

15. If you have successfully installed the license, click the Close button. The new license is now listed on the Management > Licenses screen.

Removing RP Licenses

If you want to transfer the Wireless Services Module 12 RP License or 48 RP License from one Wireless Edge Services zl Module to another, you must first access the Web interface browser and uninstall the license. During this process, the module generates an uninstall verification key. You must copy or record this key so that you can enter it on the My ProCurve Web portal. The Web portal, in turn, uses this key to generate a new verification key, which you can use to install the license on the new Wireless Edge Services zl Module.
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Licenses

To simplify the process of uninstalling a license, you may want to use two Web browsers as you complete these steps:

1. Access the Web browser interface for the Wireless Edge Services zl Module.
2. Select Management > Licenses and click the License-Install Summary tab.
3. Highlight the license that you want to uninstall and click the Uninstall button at the bottom of the screen. The Un-Install License screen is displayed. (See Figure 2-84.)

![Figure 2-84. Un-Install License Screen]

4. For Feature-Group, accept the default setting of radio ports.
5. For FG-specific-data, enter 12 or 48. FG is short for Feature-Group, and this field specifies the number of RP licenses.
6. Click the Lic-Uninstall button. A warning message is displayed, reminding you that if stations are associated with RPs that use these licenses, the stations will lose their network connection.

![Figure 2-85. Warning Message Displayed When You Attempt to Uninstall Licenses]

7. Click the Yes button if you want to continue the process of uninstalling the licenses.
8. When the uninstall verification key is displayed, copy the key (using Ctrl-C) or write it down. (Copying the key is easier and more accurate.) You will enter the key on the My ProCurve portal.

**Note**

If you forget or misplace the uninstall verification key, you can view it by selecting **Management > Licenses** and clicking the **License Uninstall Summary** tab. Alternately, you can enter the **show licenses uninstalled** command from the CLI. This command displays the last uninstall verification key that was generated by the Wireless Edge Services zl Module.


10. On the My ProCurve page, click **My Software**. The **License Activation** page is displayed.

11. Click **Device Software**. The **Registration ID** page is displayed.

12. Click the **Uninstall License** tab in the navigation bar. The Uninstall ProCurve device license page is displayed.

![Figure 2-86. Uninstall ProCurve Device License Page](image-url)
Configuring the ProCurve Wireless Edge Services zl Module
Radio Port Licenses

13. Paste (using Ctrl-V) or enter the uninstall verification key in the Uninstall verification ID# field, and click the Next button. My ProCurve Web portal generates and displays a new registration ID. The portal emails the registration ID to you and maintains a record of it.

14. To view your registration IDs, click the View available reg IDS link on the My ProCurve Web portal.

To transfer the Wireless Services Module 12 RP License or 48 RP License to another Wireless Edges Services zl Module, complete the installation steps described in “Installing RP Licenses” on page 2-128.

Redundancy Groups and RP Licensing

To ensure high availability of your company's wireless services, you can create a redundancy group, which can include up to 12 Wireless Edge Services zl Modules or Redundant Wireless Services zl Modules. If one module fails, the others provide failover capabilities. To eliminate a single point of failure, you should install at least some of the modules in different switches. In the unlikely event that one wireless services-enabled switch fails, the module installed in the remaining wireless services-enabled switch will continue to provide services for mobile users.

The group must include at least one Wireless Edge Services zl Module because Redundant Wireless Services zl Modules do not have RP licenses and, on their own, cannot adopt RPs. When you create a redundancy group, the RP licenses assigned to the Wireless Edge Services zl Module with the highest number of licenses is the total number of licenses for the redundancy group. All modules (both primary and redundant) share the group’s licenses among them.

For this reason, a redundancy group should usually include one Wireless Edge Services zl Module and one or two Redundant Wireless Services zl Modules.
Setting System Information— Name, Time, and Country Code

Access the **Network Setup** screen to configure system information:
- system name and other information that the Wireless Edge Services zl Module reports to an SNMP server
- the time and time zone for the internal clock
- the country code

You can also view information about the wireless services-enabled switch and reset passwords for the SNMP users (manager and operator).

![Network Setup Screen]

*Figure 2-87. Network Setup Screen*
Follow these steps to configure the system information, which the Wireless Edge Services zl Module reports to an SNMP server:

1. Name module by entering a string in the **System Name** field.
   The string can include spaces and special characters.
   The default name is “Wireless Services.” Note that, by default, RPs send DNS requests for “Wireless Services” when attempting to be adopted at Layer 3. See “Enabling Layer 3 Adoption Through DNS Lookup” on page 2-67 to learn how to change the name that RPs request.

2. Enter a string in the **Location** field to identify where the module is installed.

3. Enter a string in the **Contact** field to identify the person responsible for managing this module.

4. Click the **Apply** button.

Follow these steps to configure the internal clock manually:

1. Enter the current date in the **Date** field.
   Enter the date in this format, in which MM is the number of the month, DD is the date, and YYYY is the year:
   
   MM/DD/YYYY

2. Enter the current time in the **Time** field.
   Use this format, in which HH is the hour in the 24-hour clock and MM is the minutes:
   
   HH:MM

3. Choose your time zone from the **Time Zone** drop-down menu.
   The menu lists many countries and cities from which you can choose. You can also choose a time relative to Greenwich Mean Time (GMT)—for example, GMT -8.

4. Click the **Apply** button.

---

**Note**

The Wireless Edge Services zl Module can also receive the date and time from a time server. You must set the time zone manually, however, for the module to receive the correct time. See “Enabling Secure Network Time Protocol (NTP)” on page 2-138.
The country code configures the Wireless Edge Services zl Module to choose legal channels and transmit powers for RP radios. You must set the country code before the module can adopt RPs. Follow these steps:

1. From the **Country** drop-down menu, select your country.
2. The Wireless Edge Services zl Module OS warns you that you must select the correct country code. Click the **OK** button.
3. Click the **Apply** button.

---

### Enabling Secure Network Time Protocol (NTP)

Because the Wireless Edge Services zl Module supports NTP, you can configure the module to take its time from an NTP server. This ensures that the module is always using the correct time, which helps you maintain and monitor your company's wireless services. The module can function as a secure NTP client, which means that it accepts the time only from authenticated sources.

In addition to receiving the time, the Wireless Edge Services zl Module can act as a secure NTP server for other devices. Receiving a highly accurate time by communicating with other NTP servers or NTP peers, or both, the module serves this time to clients.

### Secure NTP Overview

NTP is used to synchronize the clocks of computer systems to another server or reference time source, such as a radio or satellite receiver or modem. NTP data packets use a 64-bit timestamp to provide a high degree of accuracy relative to Coordinated Universal Time (UTC). The server might receive its time via a Global Positioning System (GPS) receiver, for example.

Typical NTP configurations use multiple redundant servers and diverse network paths to ensure accuracy and reliability. The NTP client software runs continuously in the background and periodically receives updates from one or more servers. The client software ignores responses from servers that appear to be sending the wrong time and averages the results from those that appear to be correct.
NTP Modes and Communications

NTP relies on the standard client-server relationship:
- Clients send time requests to servers.
- Servers respond with the time.

The Wireless Edge Services zl Module can operate as both a client and a server. To configure the module as a client, you must configure an NTP neighbor that acts as the module's server.

NTP defines two additional modes:
- **Peer mode**—Peers operate on an equal level. Peers act as both clients and servers to each other. They send each other control queries either to synchronize their clocks entirely or simply to exchange information.
- **Broadcast mode**—Broadcast mode is similar to client-server mode. Rather than responding to direct time requests, however, a server broadcasts time information.

To configure your Wireless Edge Services zl Module to act as a peer to another NTP device, add that device as an NTP neighbor in peer mode.

If your network includes an NTP server that operates in broadcast mode, you can enable your module to listen for these broadcasts.

NTP Hierarchy

NTP uses a hierarchical system of 16 clock stratum levels (numbered 0 through 15) to define:
- the distance (number of “hops”) from the reference clock to the Secure NTP server
- the associated accuracy

Figure 2-88 illustrates the top four NTP clock stratum levels.
Configuring the ProCurve Wireless Edge Services zl Module

Enabling Secure Network Time Protocol (NTP)

Figure 2-88. NTP Clock Stratum Levels

The devices at stratum 0 are GPS clocks or other radio clocks. These devices are not attached to the network but are locally connected to computers.

Computers at stratum 1 are attached to stratum 0 devices. Stratum 1 devices can act as time servers for timing requests from stratum 2 servers via NTP.

Computers at stratum 2 send NTP requests to stratum 1 servers. Normally, a stratum 2 computer will reference a number of stratum 1 servers and use the NTP algorithm to gather the best data sample, dropping any stratum 1 servers that seem obviously wrong. Stratum 2 computers are peers to other stratum 2 computers, providing more stable and robust time for all devices in the peer group. Stratum 2 computers normally act as servers for stratum 3 NTP requests.

Computers at stratum 3 and higher employ exactly the same NTP functions of peering and data sampling as stratum 2, and can themselves act as servers for higher strata, potentially up to 16 levels (stratum 0 through stratum 15).
Several organizations on the Internet offer NTP servers at stratum 1 through 3. Some require you to purchase the service, and others grant it for free. You can configure your Wireless Edge Services zl Module to communicate with one of these servers and then, acting as a server, pass the time on to clients in your network.

When you configure your Wireless Edge Services zl Module to act as the master clock, it uses its internal clock to set the time. In this case, you must set this clock's stratum. (See “Configuring Secure NTP Options” on page 2-144.)

Secure NTP Enhancements

Knowing the correct time is not only crucial for proper network functioning but also for security. Most security protocols involve timestamps to prevent replay attacks. If an attacker can tamper with your network's NTP implementation, then he or she may be able to circumvent protections built into otherwise secure protocols. Secure NTP provides several mechanisms for ensuring that devices receive the time from trusted sources:

- **Access Control Lists (ACLs)**—You can apply ACLs to control the sources from which the Wireless Edge Services zl Module accepts particular types of NTP messages.

- **Authentication**—If you configure the module to require authentication, it accepts the time only from neighbors that prove they are legitimate. Neighbors authenticate their messages by adding a message authentication code that is generated using an encryption key. In addition to requiring authentication, the module can authenticate to other NTP hosts.

Encryption for authentication comes in two varieties:

- **With symmetric keys**—You manually set the same key on the module and its neighbor or client. Each message exchanged includes a message authentication code that is generated using this key.

- **With autokey**—The Wireless Edge Services zl Module and the neighbor or client use the public key infrastructure (PKI) algorithm to automatically generate encryption keys.

The client sends the public key associated with its digital certificate to the secure NTP server. The server uses a fast algorithm and a private value to create a cookie, which it encrypts with the client's public key and returns to the client. Both the client and the server then use the cookie to generate a list of keys for creating message authentication codes.
By encrypting the cookie with the client’s public key, the server ensures that only the client can use the cookie. The client, for its part, must initially trust the server. After this initial trust, the client knows that the same server is sending the time because only that server has the cookie that generates the correct keys.

Configuring a Secure NTP Server

As an NTP server, the Wireless Edge Services zl Module sends the time to stations and devices that request this information. To obtain the correct time, it can use its internal clock, exchange messages with other servers in your network (called its NTP neighbors), or both.

To configure secure NTP, first determine the module’s function in your network’s NTP implementation:

1. If the Wireless Edge Services zl Module simply needs to accept the time from an NTP server, complete one of the tasks below:
   - Enable the module to listen for NTP broadcasts.
   - Configure the module to request the time from NTP servers:
     - Add up to three NTP neighbors in server mode.
     - For additional security, require authentication.
       - When you require symmetric key authentication, first configure a key that matches each server’s key.
       - When you require autokey authentication, make sure that your module has the appropriate certificate.

2. If the module should act as an NTP server, complete these tasks:
   - If you want the module to use its internal clock to serve the time, configure it to act as the master clock.
   - Optionally, apply ACLs to control access to the module’s NTP services.
   - Optionally, require authentication for neighbors, configuring one of the following options for keys:
     - For auto-key, enable the feature and make sure that the module has the necessary public and private keys (stored in a server certificate in a trustpoint configuration).
     - Manually create symmetric keys.
Configuring the ProCurve Wireless Edge Services zl Module
Enabling Secure Network Time Protocol (NTP)

- Add up to three neighbors. The correct neighbor configuration depends on your network's NTP implementation:
  - Your module acts as the master clock and is your network's only time server. No neighbors are required.
  - Your module acts as your network's only time server and receives its time from one or more servers on the Internet. Specify up to three Internet servers as neighbors in server mode.
  - Your module works with other NTP servers in your network. You can add a combination of up to three servers and peers. For example, you might configure an NTP server on the Internet as a neighbor in server mode and two other NTP servers on your LAN as neighbors in peer mode.
Configuring Secure NTP Options

To configure a Secure NTP server, complete these steps:

1. Select **Special Features > Secure NTP > Configuration**.

2. Optionally, in the **Other Settings** section, check the **Authenticate Time Sources** box.

   This setting requires the Wireless Edge Services zl Module to include a credential authentication step when communicating with its neighbors and clients. See “Configuring Authentication for Secure NTP” on page 2-148.

3. Optionally, check the **Act as NTP Master Clock** box to specify that the module use its internal clock to act as the master clock.

   If you enable your module to act as the master clock, it can serve the time whether or not it receives the time from another server or peer.
4. If you checked the **Act as NTP Master Clock** box (in step 3), in the **Clock Stratum** field, enter how many hops (from 1 to 15) the Wireless Edge Services zl Module is from an NTP time source.

Valid values are from 1 to 15, although your clock stratum value should be **at least 2** (because you are not actually connected to a stratum 0 device). Typically, you should set the stratum somewhat higher (for example, to 10): the Wireless Edge Services zl Module automatically chooses the NTP resource with the lowest stratum number, and its internal clock should not take precedence over a more robust clock.

The NTP-enabled module compares the time reported by several sources and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower. You do not need to worry that your module will synchronize to a NTP server that is not synchronized itself.

5. Check the **Listen to NTP Broadcasts** box to allow the Wireless Edge Services zl Module to receive the time from an NTP broadcast server.

The module and the NTP broadcast server must be on the same subnet.

6. If you check the **Listen to NTP Broadcasts** box, you have the option of setting the broadcast delay in the **Broadcast Delay** field.

By default, the Wireless Edge Services zl Module exchanges a series of packets with the broadcast server to estimate the average delay to the server. With this information, the module knows by how much to offset the time it receives from the server.

Alternatively, you can manually specify the estimated delay to the server by entering a value between 1 and 999999 microseconds in the **Broadcast Delay** field.

7. Click the **Apply** button.

You can now set up optional security mechanisms (see “Applying ACLs to NTP Services” on page 2-146 and “Configuring Authentication for Secure NTP” on page 2-148) and add neighbors (see “Configuring NTP Neighbors” on page 2-152.)
Configuring the ProCurve Wireless Edge Services zl Module
Enabling Secure Network Time Protocol (NTP)

Applying ACLs to NTP Services

For additional security, you can set access controls on the NTP messages that your Wireless Edge Services zl Module receives. The module only accepts a particular type of message if the ACL applied to that type permits it.

You will first need to configure the ACLs for NTP resource access before completing this task. (See Chapter 7: “Access Control Lists (ACLs).” Use standard IP ACLs. Each ACL should permit the IP addresses of devices that are allowed a particular type of NTP access. For ACLs used with Secure NTP, the ACL IDs must be numeric (not strings).

To apply the access controls, move to the Special Features > Secure NTP screen. Then, enter the index numbers for the appropriate ACLs in the ACL Ids fields in the Access Group section of the screen.

![Special Features > Secure NTP](image)

Figure 2-90. Applying ACLs to NTP Services
You can control four types of access to NTP resources:

- **Full Access**—The Wireless Edge Services zl Module accepts all messages from devices permitted by the associated ACL and will synchronize with these devices. This is typically the type of access that you would grant your NTP neighbors.

- **Only Control Queries**—The module accepts only control queries from devices permitted by the ACL. NTP peers might exchange both time requests and control queries, so you should usually grant NTP peers full access instead.

- **Server and Query Access**—The module accepts both time requests and control queries from devices permitted by the ACL but does not synchronize with these devices.

- **Only Server Access**—The module only accepts time requests from these devices. Grant this type of access to authorized NTP clients—which might be any device in the world or only devices in your LAN.

Table 2-9 summarizes these types of access control.

**Table 2-9. Controlling NTP Access**

<table>
<thead>
<tr>
<th>Field</th>
<th>Queries That Permitted Devices Can Send</th>
<th>Can the Module Synchronize with Permitted Devices?</th>
<th>Type of Devices for Which the Access Control Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Access</td>
<td>Time requests and control queries</td>
<td>Yes</td>
<td>Trusted Secure NTP servers</td>
</tr>
<tr>
<td>Only Control Queries</td>
<td>Control queries</td>
<td>No</td>
<td>Secure NTP servers (which might be vulnerable to attack or less accurate)</td>
</tr>
<tr>
<td>Server and Query Access</td>
<td>Time requests and control queries</td>
<td>No</td>
<td>Secure NTP servers in a peer relationship (which might be vulnerable to attack or less accurate)</td>
</tr>
<tr>
<td>Only Server Access</td>
<td>Time queries</td>
<td>No</td>
<td>Any device on the Internet or any device in your network</td>
</tr>
</tbody>
</table>

To grant no access of a particular type, leave the respective ACL ID at 0.
Configuring Authentication for Secure NTP

When the Wireless Edge Services zl Module requires authentication for secure NTP, it drops all NTP packets unless they are encrypted with the correct key. Authentication ensures that the server providing system time to the Wireless Edge Services zl Module is trusted.

You have two options for configuring authentication:
- **Using auto key**—NTP devices authenticate with digital certificates, which they use to generate encryption keys automatically.
- **Using symmetric keys**—You manually specify the keys that NTP devices use to encrypt communications.

**Configuring Auto Key for Secure NTP.** To configure auto key, follow these steps:

1. Select **Special Features > Secure NTP.** Configure initial settings as described in “Configuring Secure NTP Options” on page 2-144.
2. Select the **Configuration** tab.
3. In the **Auto Key** field, use the drop-down menu to enable auto key:
   - **Host Enabled**—The Wireless Edge Services zl Module requires clients and neighbors to use auto key to authenticate themselves.
   - **Client only Enabled**—The module uses auto key only to authenticate itself to a server.

4. Click the **Apply** button.

5. To enable the module to use auto key with a particular neighbor, follow these steps:
   a. Click the **Neighbor** tab.
   b. Select the neighbor and click the **Edit** button. (Or, add a new neighbor. See “Configuring NTP Neighbors” on page 2-152.)
   c. Select **AutoKey Authentication**.
   d. Click the **OK** button.
6. Click the Save link.

7. Make sure that your Wireless Edge Services zl Module has the proper certificates. See “Digital Certificates” on page 2-166.

**Adding Symmetric Keys.** Symmetric key authentication uses a single (symmetric) key for encryption and decryption. Because both the sender and the receiver must know the same key, it is also referred to as shared key cryptography. The secure NTP devices use the symmetric key to authenticate their communications: they only accept packets that have been encrypted with the shared key.

To set up symmetric keys on the Wireless Edge Services zl Module, first configure keys and assign them a numeric key ID value. When you configure NTP neighbors (see “Configuring NTP Neighbors” on page 2-152), you will specify the symmetric key by entering its numeric key ID.

To add a symmetric key, complete these steps:

1. Select **Special Features > Secure NTP.** Configure initial settings as described in “Configuring Secure NTP Options” on page 2-144.

2. Select the **Symmetric Keys** tab.
3. Click the **Add** button. The **ADD** screen is displayed. (See Figure 2-93.)

4. In the **Key ID** field, enter the key ID, from 1 through 65534.
5. In the **Key Value** field, enter any string up to 32 characters for the authentication key value.

This key must match the key configured on the neighbor for which you specify this key ID.

6. To define this key as a trusted key, check the **Trusted Key** box.

The Wireless Edge Services zl Module considers a neighbor that uses this key to be a trusted source. Manually create a symmetric trusted key when you know a neighbor's public key, but cannot guarantee that the module can automatically obtain that key securely from the neighbor.

7. Click the **OK** button. The new key is now listed in the section of the **Special Features > Secure NTP > Symmetric Keys** screen.

### Configuring NTP Neighbors

The Wireless Edge Services zl Module receives the time from NTP resources, or neighbors. You can define a neighbor in one of two ways:

- **A peer**—The module and the neighbor can both send time requests and responses to each other. The two synchronize with each other.

- **A server**—The module acts as a client to the neighbor. It sends time requests to the neighbor and synchronizes to it. (The neighbor does not synchronize with the module.)

To configure an NTP neighbor, complete these steps:

1. Select **Special Features > Secure NTP** and click the **NTP Neighbor** tab.
Figure 2-94. Special Features > Secure NTP > NTP Neighbor Screen

2. Click the **Add** button. The **Add Neighbor** screen is displayed.
Configuring the ProCurve Wireless Edge Services zl Module
Enabling Secure Network Time Protocol (NTP)

3. Select the neighbor type:
   • **Peer**—A peer is another NTP server in a close relationship with your Wireless Edge Services zl Module. The module synchronizes with its peers, and at any given moment, only one peer in the group acts as the NTP server.
   • **Server**—Select this type if the NTP neighbor is a server to which the Wireless Edge Services zl Module's acts as a client.
   • **Broadcast Server**—Instead of adding a neighbor, selecting this option actually configures the module itself to act as a broadcast server. See “Configuring the Wireless Edge Services zl Module as a Broadcast Server” on page 2-155.

4. To specify the IP address or hostname of the neighbor, do one of the following:
   • Click **IP Address** and enter the IP address of the peer or server.
   • Click **Hostname** to enter the fully qualified domain name (FQDN) of the peer or server.
5. In the **NTP Version** field, use the drop-down menu to select the version of NTP to use with this configuration.

Although the latest version of the NTP implementation is NTPv4, the official Internet standard is NTPv3.

6. Select the authentication method:
   - **No Authentication**—No authentication is used.
   - **AutoKey Authentication**—The Wireless Edge Services zl Module and the neighbor automatically generate the keys that authenticate their communications, using digital certificates to secure the automatic process.
     
     This option is not available when **Broadcast Server** is selected as the neighbor type in step 3.
   - **Symmetric Key Authentication**—The module and the neighbor authenticate communications with the same shared key.

7. If you selected **Symmetric Key Authentication** in step 6, in the **Key ID** field, enter the symmetric key ID.

   The key ID references the symmetric key that you created earlier for this neighbor. (See “Adding Symmetric Keys” on page 2-150). The key value for the symmetric key must be the same for both the sender and the receiver.

8. Check the **Preferred Source** box if the neighbor is a preferred NTP resource.

   Preferred sources are contacted before non-preferred resources. You can specify more than one preferred source.

   This option is not available when **Broadcast Server** is selected as the neighbor type (see step 3).

9. Click the **OK** button. The neighbor is now listed on the **Special Features > Secure NTP > NTP Neighbor** screen.

Configuring the Wireless Edge Services zl Module as a Broadcast Server

To enable the Wireless Edge Services zl Module to act as a broadcast server, follow these steps:

1. Select **Special Features > Secure NTP** and click the **NTP Neighbor** tab.
2. Click the **Add** button. The **Add Neighbor** screen is displayed.
3. Select **Broadcast Server** for the neighbor type.

4. In the **IP Address** field, enter the broadcast address for the module’s subnetwork.

   For example, you want the module to run the broadcast server on its VLAN 8 interface, which has the address 10.4.8.30/24. Enter 10.4.8.255.

5. In the **NTP Version** field, use the drop-down menu to select the version of NTP to use with this configuration.

   Although the latest version of the NTP implementation is NTPv4, the official Internet standard is NTPv3.

6. Choose the authentication mode required by clients: No Authentication or Symmetric Key Authentication.

   When you implement NTP in broadcast mode, it is recommended should configure your clients to require authentication. Otherwise, they might receive the time from a rogue server.

   Autokey authentication is not an option for broadcast services on the Wireless Edge Services zl Module.
7. If you selected **Symmetric Key Authentication** in step 6, in the **Key ID** field, enter the symmetric key ID.

   The key ID references the symmetric key that you created earlier. (See “Adding Symmetric Keys” on page 2-150). You must configure clients in this network to match the key referenced by the ID.

8. Click the **OK** button. The broadcast server is now listed on the **Special Features > Secure NTP > NTP Neighbor** screen.

**Viewing NTP Associations and Status**

The interaction between the Wireless Edge Services zl Module and an NTP resource (typically, one of the module’s neighbors) constitutes an association. As described in “Configuring NTP Neighbors” on page 2-152, associations come in two modes:

- **Peer association**—The module synchronizes to the resource or allows the resource to synchronize to it.
- **Server association**—Only the module synchronizes to the other resource, which is the NTP server.

To view your NTP associations, select **Special Features > Secure NTP** and click the **NTP Associations** tab.
Enabling Secure Network Time Protocol (NTP)

The screen includes the following fields:

- **Address**—the numeric IP address of the resource providing NTP updates to the switch
  
  Typically, the NTP system is a peer or server that you have configured as your Wireless Edge Services zl Module's neighbor. If you have enabled the module to act as the master clock, one of the resources is the module's internal clock at 127.127.1.0.

- **Reference**—the timestamp at which the local clock was last set or corrected

- **Stratum**—how many hops the Wireless Edge Services zl Module is from an NTP time source. The module automatically chooses the NTP resource with the lowest stratum number. However, it also compares the time reported by several sources and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower. That is, the module never synchronizes to a machine that is not synchronized itself.
When—the number of seconds since a message has been received from the remote resource

Peer Poll—the maximum interval between successive messages, in seconds (always a power of 2 value, such as 8 or 64).

Reach—the status of the last eight NTP messages displayed in octal format.

If an NTP packet reaches the resource successfully, the packet is assigned the value of 1. Otherwise, it is assigned a value of 0. The results for eight packets make up an eight-digit binary number. That number, expressed in octal format, is the reach status.

You hope to see 377 for the reach status. This value indicates that all of the last eight messages have reached the remote NTP device successfully, producing this binary number: 11111111, which in octal is 377. If the most recent NTP packet were lost, but the previous seven successful, the reach status would be 376 (11111110).

The lost packet continues to be tracked over the next eight NTP messages. In this example, if the next three packets were successful, the reach status would become 370 (11110111). However, if the next three packets were to fail as well, the reach status would become 360 (11110000).

Note that, as the 0 indicating the lost packet shifts, the reach status decreases no matter the success of the following packets. Therefore a decreasing value in the Reach column does not necessary indicate that packets are no longer reaching the remote resource. For example, just before the status returns to 377, it would read 177 (01111111).

Delay (sec)—the round-trip delay (in seconds) for NTP broadcasts between the NTP resource and the module

Offset (sec)—the calculated offset (in seconds) between the clock on the module and the NTP resource. The module adjusts its clock to match the server's time value. The offset gravitates toward zero over time, but never completely reduces its offset to zero.

Dispersion (sec)—how scattered the time offsets are (in seconds) from an Secure NTP time server.

To view more detailed information about a particular NTP association, select the association and click the Details button. The Details screen is displayed. (See Figure 2-99.)
Configuring the ProCurve Wireless Edge Services zl Module

Enabling Secure Network Time Protocol (NTP)

Figure 2-99. Details Screen

The Details screen includes the following additional information:

- **Association**—state of the association
- **Sanity**—an indicator of the “sanity” of NTP packets. The sanity indicates whether the time sent by the resource seems reasonable based on time from other resources.
- **Validity**—an indicator of the validity of NTP packets
- **Authority**—the relationship between the module and the remote resource. If the Authority is master, the module will synchronize to the resource.
- **Leap State**—indicates if the module has received notice that a leap second will be inserted
Host Mode—the Wireless Edge Services zl Module's mode:

client—The module is associated with a resource which operates in server mode. The module polls the server, but does not respond to polls from the server. If the server sends valid NTP packets, the module may synchronize with it.

server—The module allows itself to be polled by clients that want to synchronize with it. The module does not poll the clients.

active—The module is in a peer association with the NTP resource. That is, both the module and the other resource can send and respond to polls.

Peer Mode—the mode of the other NTP resource in the association

The peer might operate in any of the modes described for the host mode. If the mode is "unspec," the Wireless Edge Services zl Module cannot reach the peer.

Host Poll—the maximum interval between successive polls received from the remote resource. To find this interval in seconds, subtract 1 from the value listed and raise the new value to the power of 2. For example, if the value is 7, the maximum interval in seconds is 64.

Peer Poll—the maximum interval between successive polls sent to the remote resource. The interval in seconds is calculated from the value shown as described for the host poll.

The Details screen also shows timestamps for the most recent NTP exchange:

Reference Time—the time at which the local clock was last set or corrected, in 64-bit timestamp format.

Org Time—the origination time at which the request departed the client for the server, in 64-bit timestamp format.

Receive Time—the time at which the request arrived at the server, in 64-bit timestamp format.

Transmit Time—the time at which the reply departed the server for the client, in 64-bit timestamp format.

By tracking timestamps for all NTP exchanges, the Wireless Edge Services zl Module calculates the following:

Root Delay—a 32-bit signed fixed-point number indicating the total round-trip delay to the primary reference source, in seconds with fraction point between bits 15 and 16. Note that this variable can take on both positive and negative values, depending on the relative time and frequency offsets. The values that normally are displayed in this field range from negative values of a few milliseconds to positive values of several hundred milliseconds.
Configuring the ProCurve Wireless Edge Services zl Module
Enabling Secure Network Time Protocol (NTP)

- **Root Dispersion**—a 32-bit unsigned fixed-point number indicating the nominal error relative to the primary reference source, in seconds with fraction point between bits 15 and 16. The values that normally are displayed in this field range from 0 to several hundred milliseconds.
- **Delay**—the number of milliseconds required for NTP packets to make the round-trip from the module to the remote server and back. The delay is an important factor when the module selects the “best” server. Minimizing delay is one reason why you want to pick servers that are close to you.
- **Offset**—the difference in milliseconds between the clocks in your host and the remote resource. As clocks synchronize, the offset decreases. Your mode and the mode of the peer, as well as other factors, dictate whether the module synchronizes to the remote resource.
- **Dispersion**—A measure, in seconds, of how scattered the time offsets have been from a given time server.
- **Precision**—an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. The values that normally are displayed in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations.

To refresh the screen, click the **Refresh** button.

To close the screen, click the **Close** button.

**Viewing Secure NTP Status**

The **Special Features > Secure NTP > Secure NTP Status** screen displays current status information for the Wireless Edge Services zl Module’s NTP services. (The **NTP Associations** tab shows the status for all associations with potential time sources.)
Enabling Secure Network Time Protocol (NTP)

The following information is listed on the screen:

- **Leap**—the time source’s leap state, that is, whether it inserts leap seconds.
- **Stratum**—how many hops time source is from a clock.
- **Reference**—the address of the time source to which the Wireless Edge Services zl Module is synchronized.
- **Frequency**—a Secure NTP server clock’s skew (difference) for the Wireless Edge Services zl Module.
- **Precision**—the precision (accuracy) of the Wireless Edge Services zl Module’s time clock, in Hz. The values that normally are displayed in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations.
- **Reference time**—the timestamp at which the local clock was last set or corrected.
Clock Offset—the calculated offset, in seconds, between the module and the source. The module adjusts its clock to match the server’s time value. The offset gravitates toward zero over time, but is never completely reduced to zero.

Root delay—the total round-trip delay, in seconds. This variable can take on both positive and negative values, depending on the relative time and frequency offsets. The values that normally are displayed in this field range from negative values of a few milliseconds to positive values of several hundred milliseconds.

Root Dispersion—the nominal error relative to the primary time source, in seconds. The values that normally are displayed in this field range from 0 through several hundred milliseconds.
Digital Certificates

The Wireless Edge Services zl Module supports digital certificates, which are used to identify a host uniquely.

The Wireless Edge Services zl Module uses certificates for several purposes:

- **HTTPS access**—The module's server certificate authenticates the module to your Web browser.
- **RADIUS authentication services**—802.1X authentication with Extensible Authentication Protocol (EAP) requires mutual authentication. In other words, the module's RADIUS authentication server must send a server certificate and authenticate to supplicants.
- **Autokey authentication for secure NTP**—The module sends its certificate to the secure NTP server to authenticate itself and generate keys to secure NTP exchanges.

**Overview**

Digital certificates rely on asymmetric encryption with public/private key pairs. Data encrypted by a private key must be decrypted by the corresponding public key. A host "signs" data by encrypting it with its private key—something only it can do because only it knows the private key. Other hosts verify the signature by decrypting the signature with the public key.

A digital certificate ties a public key to a particular host's identity. Typically, a trusted third-party, called the certificate authority (CA), issues certificates. A less secure option is a self-signed certificate, which is issued by the host itself. In either case, the issuer of a certificate is referred to as a trustpoint.

A certificate itself consists of:

- the host's identification information
- the host's public key
- the function used to hash the certificate
- the CA's digital signature
A host authenticates itself by sending its certificate, to which it appends its
digital signature. It creates the digital signature by hashing the certificate and
then encrypting the hash with its private key.

When the peer receives the digital certificate, the peer extracts the host’s
public key and hash function. The peer decrypts and unhashes the signature
and compares it to the certificate. If the signature and certificate match, the
peer knows that no one has tampered with the certificate en route.

To fully authenticate a host, the peer must also have the CA's certificate in its
system. This certificate includes the CA's public key, which the peer uses to
verify the CA's signature. A genuine CA signature attests that the holder of a
certificate is who it says it is. CAs also issue certificate revocation lists (CRLs),
which list certificates that are no longer valid.

Because a host can freely distribute its public key, it can authenticate itself to
anyone who trusts the host's CA. However, no one can pose as the host,
because only the host's unshared, private key can encrypt and “sign” the
certificate.

Configuring Digital Certificates

On the Wireless Edge Services zl Module, you create and manage trustpoints,
in which you create or load the following elements:

- **Server certificate**, which is the certificate that identifies and authenticates
  the module

  For a self-signed certificate, you create the server certificate yourself and
  have the Wireless Edge Services zl Module sign it. Otherwise, you create
  a certificate request, which you submit to a CA. After the CA returns the
  certificate, you install it on the module as a server certificate.

  Part of creating a certificate or certificate request is generating the public/
  private key pair.

- **CA certificate**, which is the certificate of the CA that issues the server
  certificate

  This certificate is not necessary if the server certificate is self-signed.
  Otherwise, however, you must load the CA certificate before or at the
  same time that you load the server certificate.

- **CRL**

  This element is optional, but recommended to prevent your module from
  accepting invalid certificates. Your CA should provide you with a CRL.
You must complete these tasks to configure a self-signed certificate:

1. Optionally, pre-create a specific key for the certificate. Typically, however, you can allow the module to automatically generate a key when you create the certificate.

2. Use the Certificates Wizard to create the certificate.

You must complete these tasks to install a server certificate signed by a CA:

1. Optionally, pre-create a specific key for the certificate. Typically, however, the module can automatically generate a key when you create the certificate request.

2. Use the Certificates Wizard to create the certificate request.

3. Submit the certificate request to your CA.

4. The CA will send generate the server certificate and send it to you. It should also send the CA certificate and a CRL. Load these files on an FTP server, TFTP server, or the station that runs the Web browser interface.

5. Use the Certificates Wizard to upload the server certificate and CA certificate.

6. Use the CLI to upload the CRL.

You access the Certificates Wizard, as well as manage trustpoints, in the Management > Certificate Management screen.
Configuring the ProCurve Wireless Edge Services zl Module

Digital Certificates

Figure 2-101. Management > Certificate Management Screen

The Management > Certificate Management screen has two main tabs:

- **Trustpoints**—This screen lists the trustpoints on the Wireless Edge Services zl Module and the certificates associated with each trustpoint. The left panel displays all trustpoints configured on your module. Initially, the only trustpoint is the “default-trustpoint.” The right panel displays the details for the certificates in the selected trustpoint: the module’s own certificate (Server Certificate) and the CA certificate (CA Root Certificate).

- **Keys**—This screen lists the key pairs that have been created on the Wireless Edge Services zl Module. You can associate a key pair with a trustpoint, and the module includes the public key for that pair in the self-signed certificate or the certificate request. (The Keys tab is shown in Figure 2-114 on page 2-192.)
Using the Certificates Wizard

Use the Certificates Wizard to:

■ create a new certificate, either as a self-signed certificate or a certificate request to be sent to a CA
■ upload a certificate (either a server certificate or a CA certificate) from an external source
■ delete trustpoints, certificates, or keys

You can complete all necessary tasks for creating or installing certificates through the Certificates Wizard. However, if you want create a specific key for a particular certificate, you must do so first in the Management > Certificate Management > Keys screen.

To run the Certificates Wizard, complete these steps:

1. Select Management > Certificate Management and click the Trustpoints tab.
2. Click the Certificates Wizard button. The Certificates Wizard Welcome screen is displayed.
Creating Certificates

On the Certificates Wizard Welcome screen, you can select the Create a new certificate option to do the following:

- create a self-signed certificate
- prepare a certificate request to send to a certificate authority
Creating a Self-Signed Certificate. To create a new self-signed certificate, complete these steps:

1. On the Certificates Wizard Welcome screen, in the Select a certificate operation section, select **Create a new certificate**.

2. Click the **Next** button. The screen shown in Figure 2-103 is displayed.

![Figure 2-103.Certificates Wizard Options Screen (Self-Signed Certificate)](image)

3. In the Select a certificate operation section, select **Generate a self-signed certificate**.
4. In the **Select a trustpoint for the new certificate** section, select one of the following:
   - **Use existing trustpoint**—You can select a trustpoint that you have created previously from the drop-down menu. (This option is available only when an existing trustpoint does not have a current certificate.)
   - **Create a new trustpoint**—Enter the trustpoint name in the field.

5. In the **Specify a key for your new certificate** section, select one of the following:
   - **Automatically generate a key**—Generate a key specifically for this certificate.
   - **Use existing key**—Use a key that you created previously; Select the key from the drop-down menu.
   - **Create a new key**—Create a new key for this certificate that you can also use for future certificates.
     - In the **Key Label** field, enter a name for the key.
     - In the **Key Size** field, enter the key size, from 1,024 through 2,048 bytes.

**Note**
You can also create keys in a separate procedure; see “Creating a Key” on page 2-191 for information.

6. Click the **Next** button. The screen shown in Figure 2-104 is displayed.
Configuring the ProCurve Wireless Edge Services ZL Module

Digital Certificates

7. If you specified in step 4 that you are creating a new trustpoint, check the Configure the trustpoint box to configure the trustpoint.

8. Select Automatically generate certificate with default values to generate a certificate with default credential values. The default values simply repeat the field name for all values except the IP address, which is used to identify the module and which is automatically filled in from the management VLAN.

Figure 2-104. Certificate Credentials Screen (Self-Signed Certificate)
Configuring the ProCurve Wireless Edge Services zl Module
Digital Certificates

Alternatively, select Enter certificate credentials and enter the following credentials for the certificate:

- **Country**—the two-character country code (abbreviation) for your country
- **State**—the state or province in which the module operates
- **City**—the city in which the module operates
- **Organization**—your organization (typically your company name)
- **Organizational Unit**—your organizational unit (typically your department name)
- **Common Name**—the URL that you use to access the Web browser interface. The text that you enter must exactly match the URL exactly and cannot include spaces or special characters other than periods (.) and hyphens (-). For example: WirelessServices.procurve.com
- **Email Address**—a valid email address for you or the person responsible for managing the Wireless Edge Services zl Module. This field is optional.
- **FQDN**—the module's fully qualified domain name. This field is optional.
- **IP Address**—the IP address for the certificate. This field is optional.

9. Check the Enroll the trustpoint box to create the self-signed certificate.
   
   If you do not enroll the trustpoint at this time, you will be able to select the trustpoint as an existing trustpoint when you run the Certificates Wizard in the future. (See step 4.) However, the information that you entered will be lost.

10. Click the Next button. The completion screen that is displayed summarizes the operations that you have performed using the Certificates Wizard.

11. Click the Finish button.

**Creating a Certificate Request to Send to a CA.** Instead of creating a self-signed certificate for a trustpoint, you can upload a certificate signed by a CA. A certificate signed by a trusted CA carries more validity than a self-signed certificate. Also, if your company has a full PKI, your Wireless Edge Services zl Module should have a certificate issued by your company’s CA.
To obtain a certificate signed by a CA, you must first generate a certificate request. Complete these steps:

1. On the **Certificates Wizard Welcome** screen, in the **Select a certificate operation** section, select **Create a new certificate**.
2. Click the **Next** button. The screen shown in Figure 2-105 is displayed.

3. In the **Select a certificate operation** section, select **Prepare a certificate request to send to a certificate authority**.
4. In the **Select a trustpoint for the new certificate** section, select one of the following:
   - **Use existing trustpoint**—You can select a trustpoint that you have created previously from the drop-down menu. (This option is available only when an existing trustpoint does not have a current certificate.)
   - **Create a new trustpoint**—Enter the trustpoint name in the field.

5. You must include a public key in the certificate request. In the **Specify a key for your new certificate** section, select one of the following:
   - **Automatically generate a key**—Generate a key specifically for this certificate.
   - **Use existing key**—Use a key pair that you created previously; Select the key from the drop-down menu.
   - **Create a new key**—Create a new key pair for this certificate that you can also use for future certificates.
     - In the **Key Label** field, enter a name for the key.
     - In the **Key Size** field, enter the key size, from 1,024 through 2,048 bytes.

**Note**

You can also create keys in a separate procedure; see “Creating a Key” on page 2-191 for information.

6. Click the **Next** button. The screen shown in Figure 2-106 is displayed.
Figure 2-106. Certificate Credentials Screen (Certificate Request)

7. Check the **Configure the trustpoint** box and enter the following credentials for the certificate:

- **Country**—the two-character country code (abbreviation) for your country
- **State**—the state or province in which the module operates
- **City**—the city in which the module operates
- **Organization**—your organization (typically your company name)
- **Organizational Unit**—your organizational unit (typically your department name)
- **Common Name**—the URL that you use to access the Web browser interface. The text that you enter must exactly the URL exactly and cannot include spaces or special characters other than periods (.) and hyphens (-). For example: WirelessServices.procurve.com
Configuring the ProCurve Wireless Edge Services zl Module
Digital Certificates

- **Email Address**—a valid email address for you or the person responsible for managing the Wireless Edge Services zl Module. This field is optional.
- **FQDN**—the module's fully qualified domain name. This field is optional.
- **IP Address**—the IP address for the certificate. This field is optional.
- **Password**—a password that must be entered to install the certificate. This field is optional. Only specify a password if requested by your CA.

**Note**
Do not type special characters in any of the certificate credential fields; some CAs may not create a certificate if the credentials contain special characters. This includes most nonalphanumeric characters; however, periods ( . ) and hyphens ( - ) are allowed.

Also, optional fields may not be optional for your particular CA. For example, some CAs require certain subject alternate names for server certificates. Check your CA's requirements before configuring the certificate request.

8. Check the **Enroll the trustpoint** box to generate the certificate request.
   If you do not enroll the trustpoint at this time, you will be able to select the trustpoint as an existing trustpoint when you run the Certificates Wizard in the future. (See step 4.) However, the information that you entered will be lost.

9. Click the **Next** button. The screen shown in Figure 2-107 is displayed.
   The screen shows the certificate request, which is in Base 64-encoded PKCS#10 format.
Figure 2-107.Copy or Save Certificate Request Screen

10. To save the text of the certificate request to send to a CA, you can do either (or both) of the following:

- Check the Copy the certificate request to clipboard box; After you click the Next button in step 11, you can paste the text into a text file.

- Check the Save the certificate request box to upload the certificate request to an external server or the local disk of the station running the Web browser.

To save the certificate request to an external server, follow these steps:

i. In the To drop-down menu, select Server.

ii. Choose a name for the request and enter it in the File field.
iii. Choose **FTP** or **TFTP** from the **Using** drop-down menu, and, if necessary choose the port for your server. (The default port is usually correct.)

iv. Specify the server's IP address.

v. For FTP, enter the username and password.

vi. Leave the **Path** field blank to save to the server's base directory. Or enter a valid directory path on the server.

To save the certificate request to the workstation running the Web browser, follow these steps:

i. In the **To** drop-down menu, select **Local Disk**.

ii. Choose a name for the request and enter it in the **File** field with a valid path. For example: C:/myrequest. Alternatively, click the browse button and browse for the directory in which to save the request.

11. Click the **Next** button. A completion screen summarizes the certificate request operation that you have performed.

12. Click the **Finish** button.

### Uploading a Certificate to the Module

After a CA issues your company a certificate, you must upload the certificate to the Wireless Edge Services zl Module. You can upload the certificate from an FTP server, TFTP server, or your local workstation. The certificate should be in Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) format.

To upload a certificate using the Certificates Wizard, complete these steps:

1. On the **Certificates Wizard Welcome** screen, in the **Select a certificate operation** section, select **Upload an external certificate**.
Figure 2-108.Certificates Wizard—Uploading a Certificate

1. Click the Next button. The screen shown in Figure 2-109 is displayed.
Figure 2-109. Upload Certificate to Trustpoint Screen

2. In the Select a trustpoint to upload the certificate section, select one of the following:
   - **Use existing trustpoint**—to upload the certificate to an existing trustpoint; use the drop-down menu to select the trustpoint.
   - **Create a new trustpoint**—to upload the certificate to a new trustpoint; enter the name of the new trustpoint in the field.

3. Select the certificates to upload:
   - To upload a server certificate, check the **Upload Server Certificate** box.
   - To upload a CA root certificate, check the **Upload CA Root Certificate** box.
You can select either or both certificates to upload. However, you can only upload a certain type of certificate if the selected trustpoint does not already include that type. If you want to upload a new certificate, first delete the current certificate. See “Deleting Trustpoints, Certificates, and Keys” on page 2-184.

4. For each certificate that you will upload, specify the certificate file source:

   To upload the certificate from an external server, follow these steps:
   i. In the From drop-down menu, select Server.
   ii. In the File field, enter the name of the certificate as stored on the server.
   iii. Choose FTP or TFTP from the Using drop-down menu, and, if necessary choose the port for your server. (The default port is usually correct.)
   iv. Specify the server’s IP address.
   v. For FTP, enter the username and password.
   vi. Leave the Path field blank if the file is in the server’s base directory. Or enter a valid directory path on the server.

   To upload the certificate from the workstation running the Web browser, follow these steps:
   i. In the From drop-down menu, select Local Disk.
   ii. In the File field, enter the certificate filename with a valid path.
      For example: C:/mycert.der. Alternatively, click the browse button and browse for the certificate.

5. Click the Next button. The completion screen summarizes the certificate upload operation that you have performed.

6. Click the Finish button.

Deleting Trustpoints, Certificates, and Keys

To delete selected trustpoints, certificates, and keys using the Certificates Wizard, complete these steps:

1. On the Certificates Wizard Welcome screen, in the Select a certificate operation section, click Delete Operations.
2. Click the **Next** button. The screen shown in Figure 2-111 is displayed.

![Figure 2-110.Certificates Wizard—Deleting Certificates](image)
3. Select your delete operations:
   - To delete an entire trustpoint, select **Delete trustpoint and all certificates inside it**. Then use the drop-down menu to select the trustpoint to delete.
     
     This selection deletes the trustpoint and everything it contains, including certificates, a certificate request, and a CRL.
   - To delete a certificate, but leave the trustpoint, follow these steps:
     i. Select **Remove certificates from this trustpoint**.
     ii. Use the drop-down menu to select the trustpoint that contains the certificate.
     iii. Check the **Server Certificate** box or the **CA Root Certificate** box (or both).
4. Click the Next button.

5. On the confirmation screen, click the Next button to confirm the deletion. Or, click the Cancel button to cancel the deletion.

6. After the deletion is complete, on the completion screen that is displayed, click the Finish button.

7. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

**Uploading a CRL to a Trustpoint**

If you have created a trustpoint based on an external CA, you should upload the CA’s CRL to the trustpoint. The CRL lists certificates that the CA issued but has since revoked. You configure the location to which the CA publishes the CRL, and the Wireless Edge Services zl Module periodically checks this location for the most recent CRL.

Use this command, entered from the global configuration mode context:

```
ProCurve(wireless-services-C)# crypto pki import <trustpoint name> crl <URL> <hours>
```

Replace `<trustpoint name>` with the name of the trustpoint to which you want to save the CRL. You can enter the URL as a reference to an HTTP publication point or a file on an FTP or TFTP server. For FTP and TFTP servers, include the filename, path, and (for FTP) login information. For `<hours>` enter a value from 1 to 168 to set how often the module updates the CRL.

**Transferring Trustpoints**

You can transfer trustpoints either:

- from the Wireless Edge Services zl Module to an FTP or TFTP server
- from a server to the Wireless Edge Services zl Module

You can transfer trustpoints to a secure location for archiving. Transferring trustpoints to an external server is recommended to ensure that server certificate information is available if problems are encountered with the Wireless Edge Services zl Module.

You can also transfer an entire trustpoint to the module. For example, you might want to move a trustpoint from one module to another. You would save the trustpoint on the first module out to an external server and then transfer the trustpoint from the external server to the second module.
When you transfer a trustpoint, you copy these elements (if included in that particular trustpoint):
- server certificate
- CA certificate
- CRL

Transferring Trustpoints from the Wireless Edge Services zl Module to a Server

To transfer a trustpoint from the Wireless Edge Services zl Module to a server, complete these steps:
1. Select **Management > Certificate Management** and click the **Trustpoints** tab.
2. Click the **Transfer Trustpoints** button. The **Transfer Trustpoints** screen is displayed.
3. In the **Source** section, select Wireless Services Module from the **From** drop-down menu.
4. Choose the trustpoint from the drop-down menu below.

5. In the **Target** section, the **To** drop-down menu displays **Server**. In the **File** field, specify a name for the trustpoint file. The default filename is the name of the trustpoint being transferred.
6. From the **Using** drop-down menu, select the protocol for the trustpoint transfer, either FTP or TFTP.

7. In the **Port** field, enter the respective FTP or TFTP port number; the default port number (port 21 for FTP, port 69 for TFTP) should apply in most cases.

8. In the **IP Address** field, enter the IP address of the FTP or TFTP server.

9. If you are using an FTP server, enter the login credentials.
   a. In the **User ID** field, enter the username for your account on the FTP server.
   b. In the **Password** field, enter the password for this username.

10. In the **Path** field, enter the path where the trustpoint will be stored on the server. (If you are using a TFTP server, this field may not be required.)

11. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

12. After the trustpoint transfer is complete, click the **Close** button.

### Transferring Trustpoints from a Server to the Wireless Edge Services zl Module

To transfer a trustpoint from an external server to the Wireless Edge Services zl Module, complete these steps:

1. Select **Manager > Certificate Management** and click the **Trustpoints** tab.

2. Click the **Transfer Trustpoints** button. The **Transfer Trustpoints** screen is displayed.
3. In the **Source** section, select **Server** from the **From** field.
4. In the **File** field, enter the filename of the source trustpoint file.
5. In the **Using** drop-down menu, select the protocol for the external server, either FTP or TFTP.
6. In the **Port** field, enter the respective FTP or TFTP port number; the default port number (port 21 for FTP, port 69 for TFTP) should apply in most cases.
7. In the **IP Address** field, enter the IP address of the FTP or TFTP server.
8. If you are using an FTP server, enter the login credentials:
   a. In the **User ID** field, enter the username for your account on the FTP server.
   b. In the **Password** field, enter the password for this username.
9. In the **Path** field, enter the path where the trustpoint is stored on the server. (If you are using a TFTP server, this field may not be required.)
10. In the **Target** section, **Wireless Services Module** is displayed in the **To** drop-down menu.
11. In the **File** field, enter a character string to name the trustpoint on the Wireless Edge Services zl Module.

---

**Figure 2-113. Transfer Trustpoints from Server Screen**

- In the **Source** section, select **Server** from the **From** field.
- In the **File** field, enter the filename of the source trustpoint file.
- In the **Using** drop-down menu, select the protocol for the external server, either FTP or TFTP.
- In the **Port** field, enter the respective FTP or TFTP port number; the default port number (port 21 for FTP, port 69 for TFTP) should apply in most cases.
- In the **IP Address** field, enter the IP address of the FTP or TFTP server.
- If you are using an FTP server, enter the login credentials:
  - In the **User ID** field, enter the username for your account on the FTP server.
  - In the **Password** field, enter the password for this username.
- In the **Path** field, enter the path where the trustpoint is stored on the server. (If you are using a TFTP server, this field may not be required.)
- In the **Target** section, **Wireless Services Module** is displayed in the **To** drop-down menu.
- In the **File** field, enter a character string to name the trustpoint on the Wireless Edge Services zl Module.
12. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

13. After the trustpoint transfer is complete, click the **Close** button.

**Certificate Keys**

A certificate relies on a public/private key pair. You can use the same key pair for multiple certificates, or you can use a different pair for each certificate.

When you configure certificate requests and self-signed certificates, you can automatically create a public/private key pair for the certificate. You can also create a named key pair for that certificate and use the key pair for future certificates. You manage named key pairs from the **Management > Certificate Management > Keys** screen. From this screen you can:

- create new keys or delete existing keys
- transfer keys to a secure location for archiving
- upload keys from an external server

**Creating a Key**

This section explains how to use the **Management > Certificate Management > Keys** screen to create keys.

---

**Note**

You can also create keys within the Certificates Wizard when you create certificate requests and self-signed certificates; see “Creating Certificates” on page 2-171 for more information.

To create a key, complete these steps:

1. Select **Management > Certificate Management** and click the **Keys** tab.
2. Click the Add button. The Add Key screen is displayed.
3. In the **Key Name** field, enter a name for the key. Enter between 2 and 64 characters. The only permissible special character is "_".

4. In the **Key Size** field, enter the key size, from 1,024 through 2,048 bytes.

5. Click the **OK** button.

**Transferring Keys**

You can transfer key pairs to a secure location for archiving. Transferring keys is recommended to ensure that server certificate key information is available if problems are encountered with the switch and this data needs to be retrieved. Also, if you transfer a trustpoint to a different device, the device requires the associated key pair.

You can transfer keys either:

- from the Wireless Edge Services zl Module to an FTP server, a TFTP, or the local disk of the workstation running the Web browser
- from an external server or the local disk to the Wireless Edge Services zl Module

**Transferring Keys from the Wireless Edge Services zl Module to a Server or Local Disk.** To transfer a key from the Wireless Edge Services zl Module to either an FTP or TFTP server or a local disk, complete these steps:

1. Select **Management > Server Certificates** and click the **Keys** tab
2. Click the **Transfer Keys** button. The **Transfer Keys** screen is displayed.
3. In the **Source** section, in the **From** field, use the drop-down menu to select **Wireless Services Module**.
4. Use the next drop-down menu to select the key to be transferred.

5. In the **Passphrase** field, enter a passphrase, which can include spaces and special characters.

   The passphrase encrypts the key pair, and, although optional, is recommended for security. In order to decrypt and use the key, a person must know the correct passphrase.

6. In the **Target** section, from the **To** drop-down menu, select the destination for the key transfer, either **Server** or **Local Disk**.

7. In the **File** field, enter the filename of the target key file. The default filename is the name of the key being transferred.

8. If you specified a server target in step 6, specify the following for the key transfer target:
   a. In the **Using** drop-down menu, select the protocol for the key transfer, either **FTP** or **TFTP**.
   b. In the **Port** field, enter the respective FTP or TFTP port number; the default port number (port 21 for FTP, port 69 for TFTP) should apply in most cases.
   c. In the **IP Address** field, enter the IP address of the FTP or TFTP server.
Configuring the ProCurve Wireless Edge Services zl Module
Digital Certificates

d. If you are using an FTP server, enter the login credentials.
   i. In the User ID field, enter the username for your account on the FTP server.
   ii. In the Password field, enter the password for this username.

e. In the Path field, enter the path where the key will be saved on the server. (If you are using a TFTP server, this field may not be required.)

9. If you specified Local Disk in step 6, click the browse button to choose the directory in which to save the key.

10. Click the Transfer button. In the Status section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

11. After the key transfer is complete, click the Close button.

Transferring Keys from a Server or Local Disk to the Wireless Edge Services zl Module. To transfer a key from either a server or a local disk to the Wireless Edge Services zl Module, complete these steps:

1. Select Management > Certificate Management and click the Keys tab

2. Click the Transfer Keys button. The Transfer Keys screen is displayed.

3. In the Source section, in the From field, use the drop-down menu to select either Server or Local Disk.

Figure 2-117. Transfer Keys from Server or Local Disk
4. In the **Key Name** field, enter the filename of the source key file. If you selected **Local Disk** as the source in step 3, include the path with the filename.

5. If you selected **Server** as the source in step 3, in the **Source** section, specify the following for the key transfer source:
   a. From the **Using** drop-down menu, select the protocol for the key transfer, either **FTP** or **TFTP**.
   b. In the **Port** field, enter the respective FTP or TFTP port number; the default port number (port 21 for FTP, port 69 for TFTP) should apply in most cases.
   c. In the **IP Address** field, enter the IP address of the FTP or TFTP server.
   d. If you are using an FTP server, enter the login credentials:
      i. In the **User ID** field, enter the username for your account on the FTP server.
      ii. In the **Password** field, enter the password for this username.
   e. In the **Path** field, enter the path where the key is stored on the server. (If you are using a TFTP server, this field may not be required.)

   The fields in this step do not apply to key transfers from a local disk source.

6. In the **Pass phrase** field, enter the passphrase to encrypt the key.

   Unless you enter the correct passphrase, the Wireless Edge Services zl Module cannot install the key. However, if the key has not been encrypted, leave this field empty.

7. In the **Target** section, in the **File** field, enter the filename of the target key file.

8. Click the **Transfer** button. In the **Status** section at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.

9. After the key transfer is complete, click the **Close** button.
Radio Port Configuration

Contents

Overview ......................................................... 3-2
Country-Code and Regulatory Procedures ....................... 3-4
Configuring Radio Settings .................................. 3-5
    Creating a Radio Adoption Default Configuration ........... 3-8
    Viewing and Configuring Properties ....................... 3-10
    Configuring Radio Settings ................................ 3-12
    Setting Advanced Radio Properties ....................... 3-17
Creating a Radio Configuration for a Particular Radio ....... 3-25
    Configuring Properties .................................. 3-28
    Configuring Radio Settings for a Particular Radio ....... 3-31
    Configuring Advanced Properties for a Particular Radio .. 3-33
    Configuring Multiple Radios at Once ..................... 3-36
Running ACS .................................................. 3-36
Resetting a Radio ............................................. 3-38
Managing RP Radios .......................................... 3-40
Considerations for Enabling Client Roaming ................. 3-44
Quality of Service (QoS) on RP Radios ....................... 3-46
    WMM ..................................................... 3-46
    SpectraLink Voice Priority (SVP) ......................... 3-48
Overview

The ProCurve Wireless Edge Services zl Module manages the ProCurve Radio Ports (RPs) 210, 220, and 230. Using their Ethernet port and one or two radios, these IEEE 802.11-compliant RPs grant wireless stations access to an Ethernet network.

RPs provide the radio signal and the physical connection to wireless users, but little intelligence on their own. Instead of configuring each RP individually through its own management interface, you manage them all centrally with the Wireless Edge Services zl Module. The advantage of this design is that the entire Wireless LAN System (the module together with its adopted RPs) is controlled together for consistent and transparent network access for all users.

In this chapter, you will learn how to configure Procurve RPs 210, 220, and 230 using the Wireless Edge Services zl Module's Web browser interface. You will first learn about the radio country codes, which ensure that radios operate at the frequencies and power levels specified by various countries' regulations.

You will then learn about creating radio configurations for the Wireless Edge Services zl Module to deploy to adopted RPs.

These configurations include basic settings such as a radio’s channel, power, and rate sets. When configuring these settings, you must consider the method that radios should use to select their channel and the level at which to set radios’ maximum power. You will also learn how to specify basic and supported data rates depending on the types of stations that a radio must support.

This chapter will also discuss setting advanced radio properties, which may be necessary when you want to:

- install an external antenna on a radio
- use a radio to support Voice-over-wireless LAN (VoWLAN) devices
- improve a radio’s data throughput rate
- enable self healing functions on a radio
The ProCurve RPs 210, 220, and 230 support client roaming, which allows a mobile wireless station to maintain connectivity while moving from one radio coverage area to another. This chapter will give you a few guidelines for setting up wireless coverage to facilitate seamless roaming. More detailed instructions on enabling the best possible roaming between RPs adopted by multiple Wireless Edge Services zl Modules can be found in Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility.”

In addition, the ProCurve RPs improve quality of service (QoS) in the wireless network with support for Wi-Fi Multimedia (WMM). Each radio can divide outbound wireless traffic into four queues based on priority value or on WLAN. For example, voice traffic (if appropriately marked) is placed in the highest-priority queue. The default settings for each queue are designed to provide a high QoS for voice and video traffic from RPs to associated stations. The RPs’ QoS capabilities are discussed with the capabilities of the Wireless LAN System as a whole in “Traffic Management (QoS)” on page 4-89 of Chapter 4: “Wireless Local Area Networks (WLANs).”
Country-Code and Regulatory Procedures

While IEEE has codified the international wireless network specifications and standards, each country has its own regulations for legal frequencies and wireless use requirements. It is important to be aware of your country's standards when configuring your network.

Setting a device’s country code configures it to use radio settings that are legal in that country. You must set the country code on your ProCurve Wireless Edge Services zl Module before it will adopt RPs. Complete these steps:

1. Select **Network Setup** and click the **Configuration** tab.
2. In the **Country** field, use the drop-down menu to select your country. (See Figure 3-1.)
3. Click the **Apply** button.

![Figure 3-1. Configuring the Country Code](image)
Refer to http://www.hp.com/rnd/support/manuals/rports.htm for information about each country’s regulations and permissible radio settings.

Configuring Radio Settings

You configure radio settings for the ProCurve RPs 210, 220, and 230 through the Wireless Edge Services zl Module.

The ProCurve RP 220 and 230 each have two built-in radios; one radio supports 802.11a standards while the other supports 802.11bg standards. The ProCurve 210 has a single radio that supports the 802.11bg standards. You can have multiple RPs on the network; the Wireless Edge Services zl Module manages the configurations for each type of radio on all of the RPs that it adopts.

The Wireless Edge Services zl Module stores two types of radio configurations:
- radio adoption default configurations
- specific radio configurations

Settings established in the first type of configuration are deployed to all radios when first adopted. In other words, the two radio adoption default configurations (one for each radio type) are like customized default configurations for RPs in your network.

The second type of configurations are targeted to particular radios. You can only create such a configuration for a radio after the Wireless Edge Services zl Module has identified it:
- You can alter the configuration of a radio that has been adopted and begun using the radio adoption default configuration.
- You can create a configuration for an RP radio that has been identified but not adopted.

When you create a configuration for a specific radio, the configuration is preserved even if the radio powers down.

You configure the same types of settings for adoption default and specific radio configurations, and the Web browser screens from which you do so look quite similar, as shown in Figure 3-2 and Figure 3-3.
Configuring Radio Settings

The screen for configuring the radio adoption default settings is labeled Network Setup > Radio Adoption Defaults > Configuration > Edit. The top left on the screen reads Configuration, and the top right displays the radio type: 802.11a or 802.11bg. For ease of reference, this guide will call that screen a radio type's default Configuration screen.

The screen for configuring radio settings on a particular radio is labeled Network Setup > Radio > Configuration > Edit. The top left also reads Configuration, but the top right displays the description for that particular radio. The guide will refer to that screen as a radio's Configuration screen.

Figure 3-2. Default Configuration Screen for a Radio Type
Configuring Radio Settings

Be careful to make configuration changes on the correct screen. Otherwise, the changes will not take effect as expected.

Table 3-1 summarizes how you edit the radio configurations and how the Wireless Edge Services zl Module deploys them. For more information, see Chapter 1: “Introduction.”

**Table 3-1. Radio Configurations**

<table>
<thead>
<tr>
<th>Radio Adoption Default Configuration</th>
<th>Configuration for a Targeted Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration screen</td>
<td>Network Setup &gt; Radio Adoption Defaults</td>
</tr>
<tr>
<td>Deployed to</td>
<td>any newly adopted radio</td>
</tr>
<tr>
<td>Deployed when</td>
<td>the module adopts a new, unconfigured radio</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating a Radio Adoption Default Configuration

The Wireless Edge Services zl Module stores two radio adoption default configurations, one for 802.11a radios and one for 802.11bg radios. It deploys the configurations to radios on any unconfigured RP that it adopts. These configurations only affect newly adopted radios. Therefore, configuration changes do not take effect unless a new RP is adopted, and they only take effect on that new RP; RP radios adopted before the changes continue using the settings that they received either from the former radio adoption default configuration or from a targeted configuration.

The radio adoption default configurations included in the factory default settings for the Wireless Edge Services zl Module are shown in Table 3-2.

You should establish the settings best suited for most radios in your environment. Best practice is to alter these configurations before you install the RPs. You can then alter a particular radio’s settings as necessary. (See “Creating a Radio Configuration for a Particular Radio” on page 3-25.)

Table 3-2. Radio Adoption Default Configurations

<table>
<thead>
<tr>
<th>Setting</th>
<th>802.11a</th>
<th>802.11bg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placement</td>
<td>Indoors</td>
<td>Indoors</td>
</tr>
<tr>
<td>Channel</td>
<td>Random</td>
<td>Random</td>
</tr>
<tr>
<td>Power</td>
<td>Depends on country code</td>
<td>Depends on country code</td>
</tr>
<tr>
<td>Rate settings</td>
<td>Basic: 6, 12, 24</td>
<td>Basic: 1, 2, 5.5, 11</td>
</tr>
<tr>
<td></td>
<td>Supported: 6, 9, 12, 18, 24, 36</td>
<td>Supported: 1, 2, 5.5, 6, 9, 11,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>Antenna mode</td>
<td>Diversity</td>
<td>Diversity</td>
</tr>
<tr>
<td>Maximum stations</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>RTS threshold (bytes)</td>
<td>2346</td>
<td>2346</td>
</tr>
<tr>
<td>Beacon interval (microseconds)</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Adoption preference ID</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DTIM period (beacons)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Support short preamble</td>
<td>—</td>
<td>No</td>
</tr>
<tr>
<td>Self healing offset</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
As described above, you establish settings for a radio adoption default configuration from a radio type’s default **Configuration** screen. To access this screen, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.

   This screen includes two rows, one for 802.11a and one for 802.11bg. Each row displays basic settings currently configured for that type of radio:
   
   - placement
   - channel
   - power in dBm and power in mW

<table>
<thead>
<tr>
<th>Type</th>
<th>Placement</th>
<th>Channel</th>
<th>Power dBm</th>
<th>Power mW</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>Indoor</td>
<td>Random</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>802.11b</td>
<td>Indoor</td>
<td>Random</td>
<td>20</td>
<td>100</td>
</tr>
</tbody>
</table>

**Figure 3-4. Accessing the Radio Adoption Default Configurations**

2. Select the radio type for which you want to alter the configuration.

3. Click the **Edit** button. The **Configuration** screen for that radio type is displayed. (See Figure 3-5.)
Radio Port Configuration
Configuring Radio Settings

This screen includes three sections: **Properties**, **Radio Settings**, and **Advanced Properties**. In the following sections, you will learn how to configure each of the settings on this screen.

**Viewing and Configuring Properties**

For the most part, you view, rather than configure, settings in this section. The **Model** field indicates that these radio settings apply to the 200 series ProCurve RPs, and the **Radio Type** field indicates for which 802.11 mode you are configuring settings.

You can also define all radios of this mode as dedicated detectors.

**Adopting Radios as Detectors.** To increase network security, you can configure a radio to constantly scan for neighboring access points (APs) not connected to this Wireless Edge Services zl Module. Such a radio is called a detector, and it cannot provide a connection for wireless stations.

---

3-10
When you configure this setting as part of the default configuration, you dedicate all radios of that 802.11 mode. For example, if your network does not include any stations that use 802.11a mode, you could dedicate all 802.11a radios in your network to scanning for rogue APs. (Note, however, that these radios will only detect APs operating in an 802.11a channel.)

**Note**

As a security measure, you can configure all RPs to be adopted as detectors. In this way, no RP radio can send wireless traffic into your network until you access the settings for that particular radio and disable the dedicated detector option.

For more information on AP detection, see Chapter 12: “Wireless Network Management.”

To configure all RP radios of a particular type (802.11a or 802.11bg) to be adopted as dedicated detectors, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the correct radio type and click the **Edit** button.
3. Check the **Dedicate this Radio as a Detector** box.
4. Click the **OK** button.

**Enabling a Single-Channel Scan for Unapproved APs.** A dedicated detector radio sends probes for unapproved APs on all allowed channels in its frequency, but does not support wireless stations. To allow RP radios to detect some APs, while still supporting stations, enable the radios to scan for rogue APs only on their individual channels.

To configure single-channel scanning on all adopted RP radios of a particular type (802.11a or 802.11bg), complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the correct radio type and click the **Edit** button.
3. Check the **Single-channel scan for Unapproved APs** box.
4. Click the **OK** button.
Configuring Radio Settings

Configure the basic radio settings in the default Configuration screen’s Radio Settings section, as shown in Figure 3-6. These settings include:

- radio placement
- channel selection method
- transmit power
- rate settings

You should configure the settings in this order; the radio placement setting dictates available channel options, and the channel selection method affects available power levels.

Figure 3-6. Radio Adoption Default Configuration Radio Settings

**Defining the Radio Placement.** You can configure a radio for indoor use or for outdoor use. Because a radio adjusts its power and channel settings according to its placement, it is important to configure this setting accurately. Not doing so can create various problems, and can even cause you to break the law. For example, an outdoor RP may need to transmit at higher power to
overcome distance-based signal loss, but an indoor RP should broadcast at a lower power to accommodate closer stations and minimize interference with other local RPs. In addition, some countries allow certain channels to be used only outdoors.

Unless you are certain that all RPs will operate outdoors, you should leave the Placement setting at Indoors for the radio adoption default configurations. You can override the setting for outdoor RP radios after they are installed. (See “Configuring Radio Settings for a Particular Radio” on page 3-31.)

To define the RP placement, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the Configuration tab.

2. Select the radio type and click the Edit button.

3. In the Radio Settings section, in the Placement field, use the drop-down menu to select Indoors or Outdoors.

4. Click the OK button.

Configuring the Desired Channel Selection Method. The 802.11 standards allow RPs to transmit and receive data on several radio channel frequencies within the frequency specified for a particular mode. For example, the 2.4 GHz range (for 802.11bg) includes 14 channels, some of which are allowed only in certain countries.

The Wireless Edge Services zl Module allows newly adopted radios to select a channel in one of two ways:

- **Randomly**—When each RP radio is adopted, it automatically selects a random channel within the acceptable frequencies.

- **Using auto channel select (ACS)**—The Wireless Edge Services zl Module helps radios to select the best channel based on noise and signal properties.

The default configuration is Random.

To specify how newly adopted radios should select a channel, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the Configuration tab.

2. Select the radio type and click the Edit button.
3. In the **Desired Channel** field, use the drop-down menu to select either Random or ACS.

4. Click the **OK** button.

If you want to set channels manually, then you must do so for particular radios after they are adopted. (See “Configuring Radio Settings for a Particular Radio” on page 3-31).

**Setting the Desired Radio Power.** After you have selected a channel, you must select the radio power. Available settings are determined by previously defined channel and location settings. A radio’s power determines the broadcast radio frequency (RF) signal strength in dBm. It is important to set the power level to a value that is strong enough to clearly reach all the stations, but not so strong that the RF signal is garbled, overwhelms stations, or interferes with other RPs. The maximum broadcast power may also be governed by local and national restrictions. The optimal power level for a particular channel is best determined by a site survey prior to installation.

You might need to set a higher power to ensure RF coverage when:
- a radio experiences electromagnetic interference—for example, from a nearby microwave oven or from other wireless technology
- the distance between the RP and wireless stations is long

Likewise, you may need to decrease the RF power level when:
- the radio is close to other RP radios (unintentionally overlapping RF coverage may cause lost packets and complicate roaming)
- the radio uses an external antenna

The default radio power setting for 802.11bg radios is 20 dBm, and the default setting for 802.11a radios is 20 dBm. However, this default might change based on your country code.

To set the radio power, complete these steps:

1. Select **Network Setup** > **Radio Adoption Defaults** and click the **Configuration** tab.

2. Select the radio type and click the **Edit** button.

3. In the **Desired Power (dBm)** field, use the drop-down menu to select the default power setting that you have determined for radios of this type.

4. Click the **OK** button.
A warning box may be displayed, reminding you to be careful when setting a power for a radio that is using external antennas. Verify that the power and channel settings are within local limits, and then click the OK button.

**Configuring Rate Settings.** You can specify the data rates, in Mbps, that default radios support for traffic passing between the radio and a station. These data rates determine the types of wireless stations that radios will support.

On the default Configuration screen for a radio type, click the Rate Settings button to display a screen similar to the one shown in Figure 3-7.

![Rate Settings Screen](image)

**Figure 3-7. Rate Settings Screen**

On this screen, you can set basic and supported rates. The data rates displayed depend on which type of radio you are configuring.
The basic rates are rates for which RP radios advertise support. A radio uses and allows stations to use basic rates for:

- management frames
- broadcast frames
- multicast frames

Such frames are sent to all stations associated to a basic service set (BSS); therefore, if an RP is to support 802.11b stations, it must use only the rates (1, 2, 5.5, and 11 Mbps) supported by those slower stations.

If an 802.11bg radio does not need to support 802.11b stations, you can set the basic rates to g only rates (for example, 6, 12 and 24). The higher data rates for management and broadcast traffic can improve performance in the wireless network. They also prevent the 802.11b stations from associating to the RP radio and slowing the network.

To select basic data rates for newly adopted radios of a particular type, complete these steps:

1. Access the Rate Settings screen for the radio type:
   a. Select Network Setup > Radio Adoption Defaults and click the Configuration tab.
   b. Select the radio type and click the Edit button.
   c. Click the Rate Settings button.
2. In the Basic Rates column, check the boxes next to the data rates that radios should use for management, broadcast, and multicast traffic.

   By default, the station supports both 802.11b and 802.11g stations with basic rates 1, 2, 5.5, and 11.

   To configure Wi-Fi g-only or pure-g mode on an 802.11bg radio, deselect 1, 2, 5.5, and 11 and select 6, 12, and 24.
3. Configure supported rates, as described below, or finish configuring rate settings by clicking the OK button.

The supported rates are data rates that the radio will allow for all other traffic. The radio automatically selects the most efficient rate to a station based on factors such as error rate and the distance to that station.

Basic rates are automatically included as supported rates, but you can configure additional data rates. The additional rates allow stations that support higher data rates to actually use them, possibly improving network performance.
In addition, even when you have selected g rates (such as 6, 12, and 24) for the basic rates, you should consider allowing b rates (1, 2, 5.5, and 11) for the supported rates. 802.11b stations still cannot connect to the WLAN, but RPs and 802.11g stations can use the b rates to avoid interference from any 802.11b stations that might be in the vicinity. Adding the b rates to the supported rates is characteristic of Wi-Fi g-only mode (as opposed to pure-g mode): Wi-Fi g-only protects against 802.11b interference.

To select supported data rates for newly adopted radios of a particular type, complete these steps:

1. Access the Rate Settings screen for the radio type.
2. In the Supported Rates column, check the boxes next to the additional data rates that you want the radio to support.
3. Click the OK button.

To deselect all of a radio’s data rates at once, click the Clear All Rates button. Remember, however, that you must configure at least one basic data rate for the radio. Otherwise, an error message will be displayed when you click the OK button, as shown in Figure 3-8.

![Figure 3-8. Clear All Rates Error Message.](image)

Setting Advanced Radio Properties

The third section of a radio type’s default Configuration screen allows you to configure advanced radio properties. You can:

- alter the antenna mode
- limit the maximum number of stations supported by the radio
- set an adoption preference ID
- require support for the short preamble (typically, to raise data rates in a network that includes only 802.11g stations or VoWLAN devices)
- improve wireless network performance by fine tuning:
  - the Request to Send (RTS) threshold
  - the delivery traffic indication messages (DTIM) and beacon intervals
- set the self healing offset in networks that use neighbor recovery
The RTS Threshold, Beacon Interval, and Self Healing Offset fields are accompanied by a column that describes the units in which these settings are configured. For example, the RTS threshold is configured in bytes, and the beacon interval is configured in units of 1,000 microseconds (or 1 millisecond).

![Figure 3-9. Radio Adoption Default Configuration Advanced Properties](image)

**Setting the Antenna Mode.** A diversity antenna consists of two closely spaced matching antennas designed to minimize small gaps in coverage: the RP automatically selects the antenna that provides the strongest signal to a particular station. The ProCurve RPs 210 and 230 always use their internal omnidirectional diversity antennas, and the default setting for the antenna mode is Diversity.

You may need to change the antenna mode for RP 220s, which use external antennas. ProCurve Networking offers a variety of 2.4 and 5 GHz external antennas for both indoor and outdoor use. Depending on its design, each antenna offers a different pattern of coverage; some of the antennas are diversity antennas and some are not. You connect the diversity antennas to both SMA connectors on the radio. You connect non-diversity external antennas to only one of the SMA connections (marked either primary or secondary).
You can select one of three options for the antenna mode: diversity, primary, and secondary. The Diversity option requires the RP radio to have a diversity antenna (either internal or external). If an RP radio uses a non-diversity external antenna, you must specify to which connector you have attached it by selecting Primary or Secondary.

**Note**
If your network includes a mix of models in the ProCurve RP 200 Series, or a mix of external antenna types, you should also customize the antenna mode for specific radio configurations. See “Configuring Advanced Properties for a Particular Radio” on page 3-33.

To configure newly adopted radios to use a specific antenna mode, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the radio type and click the **Edit** button.
3. In the **Advanced Properties** section, in the **Antenna Mode** field, use the drop-down menu to select Diversity, Primary, or Secondary.
4. Click the **OK** button.

**Defining the Maximum Number of Stations.** To ensure that all stations receive enough bandwidth and transmission time, you can limit the number of stations that can associate with a radio. Each radio can handle an absolute maximum of 64 wireless stations, but you may set a lower maximum to help ensure better quality.

To configure the maximum number of stations that you want radios in your network to handle, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the radio type and click the **Edit** button.
3. In the **Advanced Properties** section, in the **Maximum Stations** field, enter the maximum number of stations (up to 64) for radios to support.
4. Click the **OK** button.

**Setting the Adoption Preference ID.** The adoption preference ID influences which of two or more Wireless Edge Services 21 Modules in a system adopts an RP, helping you to control RP adoption. You might alter this setting to ensure that the same module adopts all RPs in the same area.
A Wireless Edge Services zl Module preferentially adopts RPs that have the same ID as the module itself. (See “Configure an Adoption Preference for the Module” on page 10-28 in Chapter 10: “Redundancy Groups” for instructions on setting this ID.)

You have several options for setting the radio adoption default adoption preference ID:

- Set the radio adoption default preference ID to match the Wireless Edge Services zl Module’s adoption preference ID, which allows the module to adopt any RPs that it detects. To move an RP to a different module, change the preference ID for one of the radios on that particular RP. (See “Configuring Advanced Properties for a Particular Radio” on page 3-33.)

- Set the radio adoption default preference ID to match the ID configured on a different Wireless Edge Services zl Module, pushing all RPs toward that second module. You might use this option to have a single module pre-adopt all RPs. You can then set adoption preference IDs in configurations targeted to specific radios and move some of the RPs to different modules.

- Leave the radio adoption default preference ID at 0 (the default), no matter the ID on this Wireless Edge Services zl Module. This configuration allows the module to adopt any RP that it detects, unless a preference ID set up in a targeted configuration pushes the RP toward a different module.

**Note**

Configuring the adoption preference ID in the radio adoption default configuration is only one part of the overall process of configuring adoption preference IDs—and not always a necessary one. See “Setting up Adoption Preference IDs to Control RP Adoption” on page 10-24 of Chapter 10: “Redundancy Groups” for instructions on this process.

To set the adoption preference ID for all RP radios that this Wireless Edge Services zl Module adopts, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the radio type and click the **Edit** button.
3. In the **Adoption Preference ID** field, enter a preference ID number from 1 through 65,535. (The default is 1.) Set a matching adoption preference ID on the Wireless Edge Services zl Module that should adopt these RPs when they are installed in their final location. (To set the ID, on the **Network Setup > Radio** screen, click the **Global Settings** button.)
4. Click the **OK** button.
To force another Wireless Edge Services zl Module to adopt a particular radio, change the radio's preference ID to the ID on that second module, as explained in “Configuring Advanced Properties for a Particular Radio” on page 3-33.

**Enabling Support for a Short Preamble.** As part of the 802.11 standards, stations and radios are required to prepend a preamble to transmitted frames. A preamble is a known string of bits that signals the destination device to prepare to receive data, and alerts all devices sharing a common channel that a data transmission is beginning.

There are two types of preambles: a long preamble and a short preamble. It takes a maximum of 192 ms to process the long preamble and 96 ms to process the short preamble. Because the short preamble yields about 50 percent savings in frame overhead, it can improve the throughput of a network, particularly one transmitting traffic such as VoWLAN and streaming video frames.

However, 802.11b devices do not support the short preamble, and by default, RP 802.11bg radios allow stations to use either the short or the long preamble. You can configure these radios to require the short preamble—raising overall throughput in wireless cells. But you should never require the short preamble in an environment with any 802.11b stations; this configuration prevents your wireless devices from avoiding interference with those stations.

The short preamble is part of the 802.11a standard. So you cannot configure this option for radios of that type: the short preamble is always required.

To configure 802.11bg radios to support a short preamble, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the radio type and click the **Edit** button.
3. Check the **Short Preambles only** box.
4. Click the **OK** button.

**Setting the RTS Threshold.** Your wireless network may have “hidden” stations: two stations that can each hear RP beacons but cannot hear each other’s transmissions because of a wall or other barrier between them. Because these stations cannot detect contention from each other, their frames may collide; valuable transmission time is spent in resending data.
Stations can avoid transmitting at the same time by exchanging RTS and Clear to Send (CTS) packets with the RP. A wireless station sends an RTS packet to notify the radio that it would like to transmit. If the channel is clear, the radio sends a CTS packet to the requesting station. This procedure clears the air for a specific transmission when many stations may be contending for transmission time.

Employing RTS/CTS exchanges can result in fewer data collisions and better communication with hidden or obscured nodes. However, the RTS/CTS exchange itself consumes bandwidth and can increase latency and reduce data-frame throughput.

You can set an RTS threshold size, in bytes, which determines when an RTS/CTS exchange must be made. If a station wants to send a data frame larger than the threshold size, it must exchange RTS/CTS frames with the radio. Otherwise, it can follow typical 802.11 procedures.

It is important to consider the needs of your wireless network when setting this threshold. If your network has a high level of wireless traffic, hidden stations, or interference, you should set a lower RTS. However, if your network has a relatively low amount of wireless traffic and transmission contention, you could set a higher RTS to allow a higher data throughput.

To configure the RTS threshold for adopted radios of a particular type, complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select the radio type and click the **Edit** button.
3. In the **RTS Threshold** field, enter the data frame size, in bytes, at which a station must send an RTS frame.
   
   The default threshold is 2,346 bytes, which means that the RTS/CTS exchange will never be used (because 2,346 bytes is the maximum size for an 802.11 frame).
4. Click the **OK** button.
Radio Port Configuration
Configuring Radio Settings

Setting the Beacon Interval. A beacon is an 802.11 management frame that is broadcast by an RP radio to advertise its presence as a network point of access and to keep the network synchronized. Beacon frames include information such as:

- the service set identifier (SSID) for a WLAN
- the RP radio’s basic SSID (BSSID) (media access control [MAC] address)
- the broadcast destination address
- a time stamp for synchronization
- indicators about traffic and delivery, such as DTIMs

To let stations sleep longer and preserve battery life, you can increase the time between beacons. Decreasing the beacon interval, on the other hand, helps to support streaming multicast audio and video applications that are jitter-sensitive.

To adjust the default beacon interval for radios in your network, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the Configuration tab.
2. Select the radio type and click the Edit button.
3. In the Advanced Properties section, enter a value in the Beacon Interval field.
   This value determines the time that the radio allows between sending beacons. You specify the beacon interval in units of 1,000 ms. The default setting is 100,000 ms.
4. Click the OK button.

Setting the DTIM Period. The DTIM is a known string of bits that can be sent in a beacon frame. The DTIM notifies wireless stations using power save that the RP has buffered broadcast or multicast frames that it will be sending soon. DTIMs are simple data frames that do not require an acknowledgement, so stations sometimes miss them. To overcome this, RPs are configured to send periodic DTIMs out on beacons until the data is sent.

To allow wireless stations to sleep longer between transmissions, you can increase the number of beacons between DTIMs. This helps to preserve battery life for the wireless station. However, spacing DTIMs further apart increases the chance that a station may miss the DTIM, which can cause increased jitter and delay. To support streaming multicast audio and video or other jitter-sensitive applications, you can decrease the number of beacons between DTIMs.
Radio Port Configuration
Configuring Radio Settings

The default DTIM period on all BSSIDs is 2 beacons.

To set the default number of beacons between DTIMs that radios in your
network broadcast, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the
   Configuration tab.
2. Select the radio type and click the Edit button.
3. In the DTIM field, enter the number of beacons between DTIMs.
4. Click the OK button.

Setting the Self Healing Offset. In a wireless network that implements
neighbor recovery, an RP radio may increase its power to compensate for a
failed RP. In this case, by default, power is increased to the country’s regulatory
maximum. However, when RPs are situated close to each other or when they
use external antennas, transmitting at this power may cause interference or
even illegal operation.

To prevent such interference, set a self healing offset, which is subtracted from
the radio’s maximum power to produce a new maximum for the RP radio
responding to a failed neighbor. (For more information on neighbor recovery,
see “Neighbor Recovery” on page 12-89 of Chapter 12: “Wireless Network
Management.”)

Like the radio’s normal power setting, the self healing offset is configured in
terms of dBm. The default value is 0. For additional information on determin-
ing an appropriate offset value, see the documentation shipped with the RP.

To set the default self healing offset for radios in a network that uses neighbor
recovery, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the
   Configuration tab.
2. Select the radio type and click the Edit button.
3. In the Self Healing Offset field, specify the self healing offset value.
4. Click the OK button.

Note
Like the desired power setting, you may need to tailor the self healing offset
from radio to radio. To learn how to configure a self healing offset for a
particular radio, see “Configuring Advanced Properties for a Particular Radio”
on page 3-33.
Creating a Radio Configuration for a Particular Radio

When the Wireless Edge Services zl Module is powered on, it can identify and adopt the RPs that are connected to the network. In “Creating a Radio Adoption Default Configuration” on page 3-8, you learned how to configure the settings that the module deploys to RPs when first adopted.

In this section, you will learn about configuring override settings for particular identified radios. A radio’s Configuration screen (accessed through the Network Setup > Radio > Configuration screen) allows you to modify radios’ settings and properties. (See Figure 3-10.) The Wireless Edge Services zl Module associates these settings with the MAC address of the targeted radio and always deploys this configuration to it, instead of the radio adoption default configuration.

Most settings are established for particular radios in much the same way as they are established in the radio adoption default configuration. (You simply specify the setting on a particular radio’s Configuration screen instead of on a radio type’s default Configuration screen.)

This section will explain how to alter settings for a particular radio; however, it will focus on settings that are configured only for particular radios, not as a part of a radio adoption default configuration. For more detailed information on other settings, refer to sections in “Creating a Radio Adoption Default Configuration” on page 3-8.
Radio Port Configuration
Configuring Radio Settings

The Network Setup > Radio > Configuration screen lists all of the radios that the Wireless Edge Services zl Module has identified and their current settings and status. Radios are listed by index number. (The first radio that the module identifies is typically assigned the first index, and so on.) Radios are further identified by a name and a type.

Refer to the Adopted column to determine whether an identified radio has actually been adopted.
An RP does not have to be adopted before you create a configuration for its radio (or radios); it can simply be identified in the list. An unadopted radio might display in the list because:

- the module had once adopted the RP
- you added the RP radio manually using the Add button

To create the configuration, select the unadopted radio, click the Edit button, and configure the settings. The Wireless Edge Services zl Module deploys the configuration after it adopts the RP.

For each RP radio, the Network Setup > Radio screen lists information in these columns:

- **Index**—the radio’s index number, by default assigned in the order in which radios are adopted
- **Name**—a descriptor for the radio. The default name is “RADIOX,” in which X is the radio’s index number.
- **RP Type**—the model of the RP that includes this radio
- **Type**—the 802.11 mode for the radio
- **Adopted**—the radio’s adoption state (a green check mark for adopted and a red X for not adopted)
- **RP Ethernet MAC**—the MAC address on the RP’s Ethernet interface
  
  Use this MAC address to identify the RP for manual adoption.
- **Base Radio MAC**—the MAC address on the radio. As you can see in Figure 3-10, two radios can be on the same RP and have the same RP Ethernet MAC address.
- **State**—whether the radio associates with stations (Normal) or exclusively scans for neighboring APs (Detector)
- **VLAN**—the VLAN on which the RP was adopted. By default, the Radio Port VLAN is 2100. However, you can change the VLAN. If an RP is adopted at Layer 3, the VLAN column shows a non-Radio Port VLAN.

The Properties section at the bottom of the screen displays the actual settings that the selected radio is using. For example, you can check the radio’s channel and transmit power. The Last Adopted field shows in hours, minutes, and seconds the length of time since the radio was most recently adopted.

The following sections of the guide will explain how to configure settings on the radio’s Configuration screen.
Radio Port Configuration
Configuring Radio Settings

To view the Configuration screen for a particular radio, complete these steps:
1. Select Network Setup > Radio and click the Configuration tab.
2. Select the radio that you want to configure and click the Edit button.

Like the default Configuration screen for a radio type, a particular radio’s Configuration screen includes three sections: Properties, Radio Settings, and Advanced Properties. These are described in the following sections.

Figure 3-11. Radio Configuration Properties

Configuring Properties

The Properties section on a radio’s Configuration screen differs from that in a radio type’s default Configuration screen: the radio’s reports more detailed information about the specific radio, including the radio’s base MAC address, its radio type, and its index type. In the Properties section, you can set an appropriate description for this radio and define the radio as a dedicated detector.
Setting the Radio Description. While configuring a radio description will not affect radio functions, doing so can save time and effort when managing or troubleshooting your wireless network.

The default radio description is “RADIO” followed by the radio’s index number. For example, the radio that has been assigned to index 1 has “RADIO1” as its description. It is often a good idea to describe a radio according to its intended coverage area or function.

To modify the description, complete these steps:

1. Select Network Setup > Radio and click the Configuration tab.
2. In the Radio Descr. field, enter a text string of up to 20 characters to describe the radio.
3. Click the OK button.

Dedicating a Radio as a Detector for Unapproved APs. You can dedicate a particular radio to detecting APs in your environment. Such a radio constantly scans for neighboring APs on all allowed channels, but it does not support stations.

To enable this function, complete these steps:

1. Select Network Setup > Radio and click the Configuration tab.
2. Select the radio that you want to configure and click the Edit button.
3. Check the Dedicate this Radio as a Detector box.
4. Click the OK button.

Note

If you enabled this function in the radio adoption default configurations as a security feature, you can uncheck this box to enable an authorized radio to support stations.

Take care. Any stations currently associated with this radio must move to a different radio or lose their connections.

On the Network Setup > Radio > Configuration screen, in the State column, the radio’s state should change to either Normal or Detector, as you have specified. (See Figure 3-10 on page 3-26.)
Configuring a Radio as a Single-Channel Detector for Unapproved APs. A dedicated detector radio sends probes for unapproved APs on all allowed channels in its frequency, but does not support wireless stations. To allow an RP radio to detect some APs, while still supporting stations, enable the radio to scan for rogue APs only on its own channel.

To configure a single-channel scan, complete these steps:

1. Select **Network Setup > Radio > Configuration**.
2. Select the radio that you want to configure and click the **Edit** button.
3. Check the **Single-channel scan for Unapproved APs** box.
4. Click the **OK** button.

**Base Radio MAC.** The MAC address displayed in the *Properties* section is the hardware MAC address for that radio. A dual-radio RP has two separate radio MAC addresses (as well as an Ethernet MAC address).

A BSSID, which is the MAC address that the radio uses to carry traffic for a particular WLAN (or WLANs), is generated from this base MAC address. Each RP radio includes four BSSIDs, each of which can carry traffic for four WLANs.

**Radio Type.** The *Radio Type* listed in the *Properties* section describes the 802.11 standard with which this radio complies.

The ProCurve 220 and 230 RPs each support two radios: an 802.11a and an 802.11bg radio. Make sure that you are configuring the correct radio on a dual-radio RP.

The 802.11 standard for a particular radio also determines the channel frequencies and power options available in this screen.

**Index Type.** The *Index Type* value in the *Properties* section describes whether a radio was pre-configured before the Wireless Edge Services zl Module adopted it. If a radio was adopted with the default configuration, the index type is displayed as Dynamic. If you created a configuration for the radio before allowing the module to adopt it, the index type is Static. Refer to the *Index Type* value to verify that a particular radio is using the correct configuration.
Configuring Radio Settings for a Particular Radio

The Radio Settings section on a particular radio’s Configuration screen includes the same options as the corresponding section in a radio type’s default Configuration screen.

However, the section also includes an Actual column to the right of the settings that displays the channel and power level that the radio is actually using. You can view this column to verify that the radio is using appropriate settings and to determine whether you must make any configuration changes or corrections.

The Actual column also helps you to monitor your wireless network. For example, even if a radio uses ACS to select its channel, you may want to know which channel the radio has selected.

Figure 3-12. Radio Configuration Radio Settings

To change the radio settings, complete these steps:

1. Select Network Setup > Radio and click the Configuration tab.
2. Select the radio that you want to configure and click the Edit button.
3. In the **Placement** field, use the drop-down menu to select the placement, Indoors or Outdoors.

   It is very important that the radio's placement be accurate. (See “Defining the Radio Placement” on page 3-12 for more information.)

4. In the **Actual** column (see Figure 3-12), view the channel that was selected, either randomly or using ACS, when the radio was adopted. You can now select a channel manually.

5. If you want, in the **Desired Channel** field, use the drop-down menu to select either:
   • Random
   • ACS
   • a specific channel number

   Channel numbers will vary, depending on the type of radio (802.11a or 802.11bg) that you are configuring, the radio’s country code, and the radio’s placement (indoors or outdoors).

6. If you want, in the **Desired Power (dBm)** field, use the drop-down menu to select a non-default transmit power.

   Depending on its channel, placement, and other factors discussed in “Setting the Desired Radio Power” on page 3-14, a particular radio might need to use a different power from that in the radio adoption default configuration. As you determine this power, be careful to comply with your country’s regulations.

   After you configure the radio’s power level, channel, and placement, the radio’s RF output is displayed in mW below the **Desired Power (dBm)** field.

7. Click the **OK** button.

**Configuring Rate Sets for a Particular Radio.** If your wireless network supports different types of stations in different areas, you might need to configure different rate settings on various radios. Complete these steps:

1. Select **Network Setup > Radio** and click the **Configuration** tab.
2. Select the radio that you want to configure and click the **Edit** button.
3. In the **Radio Settings** section, click the **Rate Settings** button.
4. On the screen that is displayed, check the boxes for the desired basic and supported rates, and then click the **OK** button. See “Configuring Rate Settings” on page 3-15 for more information.
5. Click the **OK** button.
Configuring Advanced Properties for a Particular Radio

The Advanced Properties section of a radio’s Configuration screen includes, in most cases, the same settings as the corresponding section in radio types’ default Configuration screens:

- **Antenna Mode**
- **Maximum Stations**
- **Adoption Preference ID**
- **Short Preambles only** (802.11 bg radios only)
- **RTS Threshold**
- **Beacon Interval**
- **DTIM Period**
- **Self Healing Offset**

See “Setting Advanced Radio Properties” on page 3-17 for more information on each setting. Setting the **DTIM Period** is slightly different for the targeted radio configuration; see “Setting DTIM Periods for a Particular Radio” on page 3-34.

You can alter any of these settings for a particular radio. On the Network Setup > Radio > Configuration screen, select the radio and click the Edit button. On the Configuration screen that is displayed, locate the Advanced Properties section.

Situations in which you might alter these settings on a radio include, but are not limited to:

- **This radio uses two non-matching antennas**—In the Antenna Mode field, use the drop-down menu to select the antenna that the radio should use.
- **You want a different module to adopt this RP**—Change the value in the Adoption Preference ID field to match the module preference ID for the module that should adopt this RP.
- **The RF network supported by this radio experiences many collisions**—Perhaps caused by “hidden” stations—Lower the value in the RTS Threshold field.
- **This radio supports multicast video streaming traffic and users have reported jittery video**—Have the radio send DTIMs more frequently by lowering the values for the DTIM Period. You could also lower the value in the Beacon Interval field.
- **This radio is configured to raise its transmit power in response to a failed neighbor**—Configure the Self Healing Offset field so that the radio does not raise its power too high.
Setting DTIM Periods for a Particular Radio. For radio adoption defaults, you specify a single value for the DTIM period (the number of beacons between DTIMs). (See “Setting the DTIM Period” on page 3-23.)

However, a particular RP radio sends out beacons on each of its four BSSIDs, and the Wireless Edge Services zl Module allows you to set a different DTIM period for each BSSID. In this way, you can, for example, set a higher DTIM period on a BSSID that supports a traditional data WLAN, but a lower DTIM period on a BSSID that supports a voice WLAN.

To find the BSSID used by your WLAN (with normal configuration), see Table 3-3. Advanced mode configuration allows you to change these assignments. (See “Configuration Options: Normal Versus Advanced Mode” on page 4-4 of Chapter 4: “Wireless Local Area Networks (WLANs).”)

Table 3-3. WLAN Assignment to BSSID

<table>
<thead>
<tr>
<th>SSIDs for WLANs</th>
<th>BSSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 5, 9, 13</td>
<td>1</td>
</tr>
<tr>
<td>2, 6, 10, 14</td>
<td>2</td>
</tr>
<tr>
<td>3, 7, 11, 15</td>
<td>3</td>
</tr>
<tr>
<td>4, 8, 12, 16</td>
<td>4</td>
</tr>
</tbody>
</table>

To configure DTIM periods for a particular radio, complete these steps:

2. Select the radio that you want to configure and click the Edit button.
3. In the Advanced Properties section, click the DTIM Periods button. The DTIM Periods screen is displayed.

4. In the field for each BSS, enter the number of beacons between DTIMs.

5. Click the OK button.
Configuring Multiple Radios at Once

To save time, you can configure settings for multiple radios at once. Hold down <Ctrl> as you select the radios and click the Edit button.

The Configuration screen is displayed. You can edit the configuration much as you would for a single radio. However, certain parameters are grayed out; these parameters are restricted to configuration on one radio at a time. The restricted promontories are:

- channel setting
- transmit power
- short preamble requirement

If you have choose radios of both 802.11a and 802.11bg type, the restricted parameters are:

- placement
- channel setting
- transmit power
- rate settings
- short preamble requirement

For certain parameters, you can either edit the setting for all radios or allow each radio to keep its current setting. These parameters are:

- placement (for radios of the same type)
- antenna mode

Other settings become identical for every selected radio after you click the OK button.

Running ACS

If you have configured one or more radios to use ACS, you can have the Wireless Edge Services zl Module reinitiate the ACS process. Rerunning ACS after all RPs are adopted helps the radios to select the actual channel with the least interference.

Complete these steps:

2. Click the **Tools** button.

3. On the pop-up menu that is displayed, select **Run ACS Now**.

The Wireless Edge Services zl Module scans all channels and discovers which radios are adopted and using which channels. The module then analyzes the radios' channels and moves each ACS-enabled radio to the channel where it is least likely to experience interference from other radios. (See Figure 3-16.)
Resetting a Radio

It may become necessary for you to reboot an RP. For a dual-radio RP (such as the RP 220 or 230), you can either reset the entire RP or only one of its radios. Complete these steps:

1. Select **Network Setup > Radio** and click the **Configuration** tab.
2. Select the radio that you want to reset and click the **Tools** button.
3. On the pop-up menu that is displayed, select \textbf{Reset}. The \textbf{Confirm Reset} screen is displayed.

4. Select a reset option:
   - If you click the \textbf{Reset Radio only} button, only the selected radio will reset.
   - If you click the \textbf{Reset entire Radio Port} button, the RP for the selected radio will reset, along with both radios on the same RP. Each radio will reset with its specific configuration (not with the radio adoption default configuration).
Managing RP Radios

You can perform several actions on an RP radio in the Network Setup > Radio screen. Select the radio from the list and clicking the buttons at the bottom of the screen:

- Click the Edit button to alter a radio’s configuration. The Configuration screen for that radio is displayed. (See “Configuring Radio Settings for a Particular Radio” on page 3-31.)

- Click the Delete button to delete a radio configuration and unadopt the radio. The radio will immediately be readopted unless you have taken steps to prevent it being so (for example, clicking the Global Settings button and disabling manual adoption). However, the radio receives the radio adoption default configuration, which writes over any configuration previously created for it.

Clicking the Delete button also erases the configuration of an RP radio that was once adopted by this module, but is so no longer.

- Click the Add button to adopt an RP when automatic adoption is disabled. (See “Radio Port Adoption” on page 2-57 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)

You also use the Add button to create a pre-adoption configuration targeted for a particular radio.

When you click the Add button, the Add Radio screen is displayed.

![Add Radio Screen](image-url)
Enter the RP’s Ethernet MAC address in the **RP MAC Address** field. Then choose the appropriate radio or radios for the RP and assign them index numbers not currently used on this Wireless Edge Services zl Module.

Click **OK**, and you can then select and edit the configuration for this RP’s radios before the RP is even adopted.

- Click the **Tools** button to view a pop-up menu with the following options:
  - **Reset**—Select this option to reboot the radio. See “Resetting a Radio” on page 3-38.
  - **Run ACS Now**—Select this option to force radios that use ACS to select a new channel based on the best signal to noise ratio (SNR). See “Running ACS” on page 3-36.
  - **Export**—Select this option to save information about the radio to a comma separated file on your workstation. The file includes the information in the columns at the top of the **Network Setup > Radio** screen.

- Click the **LLDP** button to configure a Link Layer Discovery Protocol (LLDP) name for a radio.

LLDP is an IEEE 802.1ab Layer 2 protocol that allows a network device (such as a radio) to advertise its identity and capabilities to neighboring devices on the local network. These neighboring devices then store the information in standard simple network management protocol (SNMP) management information bases (MIBs).
Radio Port Configuration
Configuring Radio Settings

The **LLDP** screen is displayed.

If you select a radio before clicking the LDAP button, the **MAC Address** field is automatically filled with the RP's Ethernet MAC address. See Figure 3-21.
You might have already customized the radio’s name. Select **Set Radio Name as LLDP Name** to use this name for the LLDP name as well.

Alternatively, manually enter a name in the **LLDP Name** field. (The name can include alphanumeric and special characters, as well as spaces.)

In the **MAC Address** field, enter the Ethernet MAC address of the RP. Or enter 00-00-00-00-00-00 to apply the LLDP name to all radios.

Then click the **OK** button.

Note that the LLDP name applies to the RP as a whole. If the RP has another radio, that radio’s LLDP name is automatically changed when you click the **OK** button.
Considerations for Enabling Client Roaming

A mobile station may roam back and forth between several RPs. Ideally, such roaming is hidden from wireless users, who do not need to know when they connect to a new RP. They simply want their applications to continue functioning smoothly.

A station itself determines when it needs to roam (typically, in order to associate to a radio with a better signal). However, your wireless network infrastructure should support roaming. When planning roaming, you must consider the Physical Layer, Data Link Layer (Layer 2), and Network Layer (Layer 3) of the Open Systems Interconnection (OSI) model.

At the Physical Layer, most wireless stations roam seamlessly as long as your RP radios provide seamless coverage. Generally, you should deploy RPs so that their coverage areas overlap: stations should be able to roam between RPs without losing the signal.

**Note**

When the coverage areas of 802.11b/g radios overlap significantly, remember to set the channels to non-interfering channels:
- 1, 6, and 11
- 1, 7, and 13

See “Configuring Radio Settings for a Particular Radio” on page 3-31 for more instructions on setting a radio’s channel.

While a detailed discussion of wireless network design is beyond the scope of this management and configuration guide, you should understand that the size and pattern of an RP radio’s coverage depends on several factors, including:
- the radio’s power level

  The higher the power level, the larger the coverage area. An external antenna raises the power level (to the degree that you may need to manually lower the radio's power in order to comply with your country's regulations). See “Setting the Desired Radio Power” on page 3-14 for more information on configuring this setting.
Radio Port Configuration
Considerations for Enabling Client Roaming

Setting the power level lower than the maximum can help you provide seamless coverage. Place RPs more closely together and configure self healing, as described in “Network Self Healing” on page 12-89 of Chapter 12: “Wireless Network Management.”

■ the antenna type

The RP 210's and RP 230's internal radios use omnidirectional diversity antennas, which send out the signal in all directions equally. The two antennas of the diversity antenna ensure even coverage over the area.

You can install a variety of external antennas on the RP 220. These antennas can be diversity or non-diversity. They can be omnidirectional, providing a sphere of coverage like that of the RP 210 and 220 antennas, or directional, providing a cone of coverage directed toward a specific area.

See “Setting the Antenna Mode” on page 3-18 for more information on this setting.

■ the supported data rates

An RP radio supports the highest data rates only at close proximity. If you want your wireless network to provide faster connections, then you must lower RP radios’ power levels and space the RPs more closely together.

For more information on configuring data rate settings and power levels, see “Configuring Rate Settings” on page 3-15 and “Setting the Desired Radio Power” on page 3-14.

At the Data Link Layer, roaming can be slowed when the station must authenticate to the network. Roaming to an RP supported by a different Wireless Edge Services zl Module introduces the Network Layer: if the second module does not place the station’s traffic on the same subnetwork that the first module did, the station’s IP address is no longer valid. A Layer 3 roaming solution is necessary to solve this problem. See Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility” for more information on enabling fast and seamless roaming throughout your wireless network.
Quality of Service (QoS) on RP Radios

All traffic on a radio shares the same medium. So an RP radio may queue traffic for multiple WLANs together. By default, RPs queue traffic according to the classification of the WLAN to which it belongs. Because, by default, this classification is normal for all WLANs, all traffic receives the same handling. That is, each frame must contend for the medium on equal footing.

One way to configure RPs to prioritize transmitted traffic is to assign different classifications to traffic in different WLANs. See “Manually Classifying a WLAN’s Traffic” on page 4-111 of Chapter 4: “Wireless Local Area Networks (WLANs).”

For more precise prioritization, you can enable Wi-Fi Multimedia (WMM) on a WLAN.

WMM

WMM, which is Wi-Fi's implementation of a portion of the IEEE 802.11e-2005 ratified specification for wireless QoS enhancements, includes packet prioritization, scheduled access, and call admission control. WMM divides traffic into four access categories (ACs): voice, video, best effort, and background and allows RPs to queue outbound wireless traffic according to each AC.

The RP creates one queue for each AC on each of its radios, using an 802.1p value (by default) or Differentiated Service Code Point (DSCP) to assign a particular frame to a queue. The RP radio then transmits traffic in the queue according to the RP WMM parameters for that AC.

Table 3-4 shows the WMM queues on the ProCurve RPs 210, 220, and 230. Each radio on an RP has four queues for outbound wireless traffic. These queues and all radio WMM settings apply to traffic from the RP to wireless stations.

<table>
<thead>
<tr>
<th>Queue Number</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Best effort</td>
</tr>
<tr>
<td>3</td>
<td>Video</td>
</tr>
<tr>
<td>4</td>
<td>Voice</td>
</tr>
</tbody>
</table>
Each outbound radio queue is defined by different WMM parameters, which determine how the RP contends for the medium in order to transmit frames in that queue. These parameters include:

- the arbitration IFS number (AIFSN)—the time that the medium must be contention free before the RP can attempt to transmit a frame (first decrementing a random backoff time)
- the minimum contention window (CW Min)—the maximum value for the initial random backoff time
- the maximum contention window (CW Max)—the maximum value for the random backoff time for a frame that has collided
- the transmit opportunity (Transmit Ops)—the continuous time during which a device that has won control of the radio can retain control

You can view the parameters that RP radios apply to each queue by selecting **Network Setup > Radio** and clicking the **WMM** tab.

![Network Setup > Radio > WMM Screen](image_url)
For more information about WMM and other QoS mechanisms, see “Traffic Management (QoS)” on page 4-89 of Chapter 4: “Wireless Local Area Networks (WLANs).” To learn how to customize RP WMM parameters, see “Viewing and Customizing RP WMM Parameters” on page 4-105 on Chapter 4: “Wireless Local Area Networks (WLANs).”

SpectraLink Voice Priority (SVP)

To raise voice quality over a wireless network, SpectraLink Corporation has developed a de facto industry QoS mechanism called SpectraLink Voice Priority (SVP). SVP is implemented in wireless phone handsets, wireless APs or RPs, and SpectraLink servers. This IEEE 802.11-compliant mechanism minimizes latency for voice traffic by establishing priority queues for voice packets and by increasing the probability that all voice packets are transmitted in a predictable and timely manner.

Any transmission delays can have an adverse effect on voice traffic. In addition to priority queuing, SVP-enabled RPs and phone handsets transmit voice packets in a coordinated fashion, using a zero backoff interval and thereby eliminating delays introduced by random backoff intervals.

The RPs 210, 220, and 230 are all SVP compliant. You enable this feature in the WLAN configuration. See Chapter 4: “Wireless Local Area Networks (WLANs).”
# Wireless Local Area Networks (WLANs)

## Contents

- **Overview** ................................................. 4-3
- **Configuration Options: Normal Versus Advanced Mode** ........ 4-4
  - Normal Mode Configuration ................................ 4-4
    - Why Use Normal Mode ...................................... 4-4
    - Enabling WLANs Using Normal Mode ...................... 4-5
    - Enabling More Than Four WLANs Using Normal Mode .... 4-7
  - Advanced Mode Configuration ............................... 4-11
    - Why Use Advanced Mode ................................... 4-12
    - Enabling WLANs Using Advanced Mode Configuration .... 4-13
    - Using Normal and Advanced Mode Together .............. 4-22
    - Changing from Advanced Mode to Normal Mode............ 4-23

## Configuring a WLAN

- **Setting Basic Configuration Options: SSID and VLAN Interface** . 4-30
  - Necessary Configurations on the Wireless Services-Enabled Switch ........................................... 4-33
- **Configuring Security Options** ................................ 4-33
  - Configuring Authentication ................................ 4-33
  - Configuring Encryption .................................... 4-47
- **Configuring Advanced WLAN Settings** ........................ 4-62
  - Controlling Inter-Station Traffic .......................... 4-63
  - Enabling Closed System Operations ....................... 4-65
  - Configuring the Inactivity Timeout ....................... 4-67
Configuring Accounting on a WLAN ......................... 4-68
Enabling Logging to a Syslog Server on a WLAN ........... 4-69
Enabling RADIUS Accounting on a WLAN ................. 4-71
Configuring Global WLAN Settings ....................... 4-75
Enabling the WLAN ............................................. 4-76
VLAN Assignment ............................................... 4-80
WLAN-Based VLAN Assignment ............................. 4-82
   Considerations for WLAN-Based VLAN Assignment ...... 4-84
Identity-Based, or Dynamic, VLAN Assignment .......... 4-87
Traffic Management (QoS) ........................................ 4-89
   SVP .................................................................. 4-90
   WMM ................................................................. 4-91
      Prioritization with WMM ................................. 4-92
      Enabling WMM on a WLAN ............................ 4-95
      Changing the Protocol that Prioritizes Traffic and Enabling
         Admission Control ........................................ 4-97
      Viewing Station WMM Parameters ................... 4-100
      Customizing Station WMM Parameters ................ 4-102
      Viewing and Customizing RP WMM Parameters ....... 4-105
      Customizing How QoS Marks Map to ACs ............ 4-108
Manually Classifying a WLAN’s Traffic ..................... 4-111
Enabling Prioritization of Voice Traffic .................... 4-113
Specifying Multicast Addresses for Voice Traffic .......... 4-113
Overview

A wireless LAN (WLAN) is a LAN that uses a wireless medium; typically it provides wireless stations a connection to a private LAN, the Internet, or both. The WLAN might include multiple radio ports (RPs), each of which is identified by an individual basic service set identifier (BSSID), but supports the same service set identifier (SSID). Stations associated to one RP can roam to another RP that provides access to the same WLAN (shares the same SSID).

By default, all RP radios adopted by a ProCurve Wireless Edge Services zl Module support all WLANs that you enable on that module. In “Configuration Options: Normal Versus Advanced Mode” on page 4-4, you will learn about how the module assigns these WLANs to BSSIDs on each RP radio. (This process may affect which WLANs operate in open and which in closed system.) Mastering these concepts will help you better design your network, and is particularly important when you plan to configure more than four WLANs.

The WLAN defines settings that control the wireless communications. These range from the method that wireless stations must use to authenticate themselves to the encryption algorithms that protect data to the parameters by which stations compete for access to the wireless medium. When you configure the WLAN, you must choose these settings, as described in “Configuring a WLAN” on page 4-26 and “Traffic Management (QoS)” on page 4-89.

Because all RPs in a WLAN must agree upon settings, the Wireless Edge Services zl Module, as a single wireless controller, greatly simplifies configuration. After you configure and enable a WLAN on the module, the module can automatically configure these settings on all adopted RPs.

The RPs send and receive traffic in these WLANs. The traffic that they receive from wireless stations, they forward (via Radio Port virtual LANs [VLANs]) to the Wireless Edge Services zl Module, which assigns this traffic to a VLAN. The module can:

- assign all traffic from a WLAN to the same VLAN (manual VLAN assignment)
- assign traffic to different VLANs depending on the identity of the user that sent the traffic (dynamic VLAN assignment)

You will learn about both of these options in “VLAN Assignment” on page 4-80.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Configuration Options: Normal Versus Advanced Mode

When the Wireless Edge Services v1 Module deploys a WLAN’s configuration to an RP, it assigns the SSID associated with that WLAN to a BSSID on the RP’s radio (or radios). You can configure the module to assign WLANs to RPs in one of two modes: normal or advanced. In normal configuration mode, the Wireless Edge Services v1 Module handles mapping WLANs to BSSIDs on all RP radios. In advanced mode, you must manually assign WLANs to radios and to BSSIDs.

Normal configuration is the generally recommended option. However, you can use advanced configuration to restrict certain WLANs to certain areas, to select which WLANs the RPs announce, or to increase the number of WLANs supported by your network.

The following sections describe how to use normal mode and advanced mode configuration. The instructions assume that you have already configured all of the WLANs for your network and that you are ready to enable them.

Normal Mode Configuration

You almost always use normal mode configuration. In this mode, the Wireless Edge Services v1 Module OS automatically adds enabled WLANs to the default configuration for adopted radios, matching each WLAN’s SSID to a particular BSSID. Whenever the module adopts an RP, it deploys this configuration to the RP.

In normal mode configuration, a Wireless Edge Services v1 Module (and its RPs) can support up to 16 WLANs.

Why Use Normal Mode

Normal mode configuration is simple to use and suitable for most environments. The deployment is entirely transparent: you simply enable WLANs, and as soon as an RP is adopted by the module, that RP begins to support those WLANs.

Unless you need more than 16 WLANs or have a pressing reason to force certain RPs to support certain WLANs only, you should not deviate from normal mode.
Enabling WLANs Using Normal Mode

In normal mode, to configure and activate WLANs, you complete these steps:

1. Configure the SSID, VLAN, and other options for each WLAN that you want to include in your network. See “Configuring a WLAN” on page 4-26 for instructions on how to do so.

2. On the Network Setup > WLAN Setup screen, select the WLANs and click Enable.

The Wireless Edge Services zl Module then automatically implements this process:

1. It assigns the SSID for WLAN 1 to the first BSSID on every radio on every adopted RP.

2. It assigns the SSID for WLAN 2 to the second BSSID on every RP radio. In our example, it assigns SSID B to BSSID 2.

3. This process continues for up to four WLANs.

The figures below illustrate this process.

![Figure 4-1. Assigning WLANs (Normal)](image-url)
Figure 4-2 shows the screen in which you can verify that radios have received the WLAN assignment.

To view the screen in Figure 4-2, select **Network Setup > Radio** and click the **WLAN Assignment** tab. Select a radio, and information is displayed in the area in the right of the screen, called **Assigned WLANs**.

The **Assigned WLANs** area lists the four BSSIDs on the radio and the SSID (or SSIDs) assigned to each BSSID. View this screen whenever you want to see exactly which WLANs each RP radio in your wireless network supports.

Note that if the RP includes two radios, each WLAN is matched to corresponding BSSIDs on each radio, as shown on the RP 230 in Figure 4-1. Figure 4-3 shows the screen in the Web browser interface in which you can verify that radio 2 has also received the WLAN configuration. (To view the SSID for both radios at the same time, hold down the **Shift** key and select the two.)
You must understand that these assignments are constant: WLAN 2 is always assigned to BSSID 2, even if you have not enabled WLAN 1.

Enabling More Than Four WLANs Using Normal Mode

Using normal mode, you can configure and enable up to 16 WLANs, which all adopted RP radios will support. However, because the RPs only support four BSSIDs per radio, the process of assigning WLANs changes slightly when you enable more than four WLANs.

For the four WLANs with the lowest index numbers, the Wireless Edge Services zl Module uses the process described above.

WLANs subsequent to WLAN 4 share the BSSID that the first four WLANs use. For example, in Figure 4-4, SSID E (that for WLAN 5) is mapped to all radios’ BSSID 1 along with SSID A (for WLAN 1). SSID F (that for WLAN 6), as well as SSID B, is assigned to the second BSSID, and so on.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

As always, if the RP includes two radios, every WLAN is assigned to a BSSID on each.

This process is illustrated in the figures below.

Figure 4-4. Assigning Six WLANs to a Radio (Normal)
Wireless Local Area Networks (WLANs)  
Configuration Options: Normal Versus Advanced Mode

Figure 4-5. Viewing Six WLANs Assigned to a Radio (Normal)

RP radios send beacon frames to announce the WLANs that they support. The source of a beacon frame is a BSSID, and each beacon can include only one SSID. Therefore, if you enable more than four WLANs, RPs support all of them, but only announce the first four. The WLAN that each BSSID announces is the primary WLAN—in normal mode, always the WLAN with the lowest index number on that BSSID.

On the **Network Setup > Radio > WLAN Assignment** screen, a green check mark under the beacon icon indicates the SSID that the RP announces. For example, in Figure 4-5, the RP uses BSSID 1 to send beacons for SSID A, but not for SSID E.

While RPs do not beacon non-primary WLANs, they do respond to probes for them, so wireless stations can connect these WLANs. Some wireless clients require the user to manually input the correct SSID; others automatically send out probes and discover the SSID.

You can configure WLANs 1 through 4 to operate in closed system. In this case, the RP does not announce any SSID in beacons from that BSSID. (It does not announce the SSID for another WLAN sharing that BSSID.)
In other words, with normal configuration, WLANs 5 through 16 always operate in partially closed system. If you want these WLANs to operate in completely closed system, you should disable responses to probe requests. You cannot disable closed system.

See “Enabling Closed System Operations” on page 4-65 to learn more about configuring this features described above.

Finally, again, note that the WLAN assignments are constant. If, for whatever reason, you configure and enable WLANs 2, 4, 5, and 6 instead of 1, 2, 3, and 4, SSID B (WLAN 2) is assigned to BSSID 2, not BSSID 1. SSID F (WLAN 6) is also assigned to BSSID 2, and no SSID is assigned to BSSID 3. (See Figure 4-6.) For this reason, you should generally configure WLANs in order, beginning at index 1.

Table 4-1 shows the BSSID to which all 16 WLANs available in normal mode are always assigned.
Table 4-1. WLAN Assignment to BSSID

<table>
<thead>
<tr>
<th>SSIDs for WLANs</th>
<th>BSSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 5, 9, 13</td>
<td>1</td>
</tr>
<tr>
<td>2, 6, 10, 14</td>
<td>2</td>
</tr>
<tr>
<td>3, 7, 11, 15</td>
<td>3</td>
</tr>
<tr>
<td>4, 8, 12, 16</td>
<td>4</td>
</tr>
</tbody>
</table>

When deciding which WLAN index number to use for a WLAN, keep in mind that this number determines on which BSSID RPs carry that WLAN’s traffic. You should generally avoid mixing bulk data and time-sensitive data such as voice on the same BSSID. For example, if stations connect to WLAN 1 to download files from your network’s FTP server, you should not configure WLAN 5 for VoWLAN devices.

Advanced Mode Configuration

In advanced mode, you manually control which RP radios support which WLANs. You can even control to which BSSID a WLAN’s SSID is assigned, and which of multiple SSIDs that share a BSSID is present in beacons (is the primary WLAN). However, because such precise control adds unnecessary complexity in most environments, this mode is not generally recommended.

In advanced mode configuration, the Wireless Edge Services zl Module supports up to 256 WLANs.

**Note**

Remember that advanced mode can lead to configuration errors that cut off network access for some users to some WLANs.

Whenever you prevent certain RPs or radios from supporting a WLAN, whether deliberately or not, you open the possibility that roaming wireless stations lose their connection to the network—which can be frustrating.

In addition, because you must manually assign WLANs to radios, advanced mode configuration can be tedious.
Why Use Advanced Mode

Reasons that you might use advanced mode include:
- You want to restrict access to a WLAN to a certain area.

For example, if a WLAN allows wireless users to access sensitive financial information, you might not want your network to support that WLAN, even protected by encryption, in a public lobby. Advanced mode allows you to assign a WLAN to certain RPs only, so you control where the WLAN exists.

For example, in Figure 4-7, the administrator has assigned SSID A to the RP in Building 2, and SSIDs B, C, and D to other RPs.

Figure 4-7. Restricting a WLAN to an Area

- Your network includes more than four WLANs, and you want beacons to include one of the WLANs with a higher index number.

In this case, you should assign the WLAN that you want RPs to beacon as the primary WLAN on a specific BSSID.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

■ You want your RPs to announce more than four SSIDs.

While a single RP radio can only beacon four SSIDs, it is possible to customize WLAN assignments so that different RP radios beacon different SSIDs. That is, you can configure certain WLANs as the primary WLANs on some of your organization’s RPs, and other WLANs as primary on others. However, such a configuration would mean that certain WLANs are beaconed only in certain areas, which may not be ideal.

■ You want more than 16 WLANs in your network.

With advanced mode configuration, you can configure up to 256 WLANs on the Wireless Edge Services zl Module. However, you cannot assign every WLAN to every RP.

Each RP radio has 4 BSSIDs, and each BSSID supports at most 4 WLANs. So each RP radio can support up to 16 WLANs. If your network includes dual-radio RPs, you can expand the number of WLANs on a single RP from 16 to 32: enable half of the WLANs on one radio and half on the other.

To provide coverage for different WLANs in different areas, simply assign the WLANs to the correct RPs.

Providing coverage for more than 16 WLANs in one area is more complicated. You can enable some WLANs on one RP and some on another, and then place the RPs close together. (Remember to set the RPs to non-overlapping channels.) For dual-radio RPs, you can also enable some WLANs on radios operating in 802.11bg and some WLANs on radios operating in 802.11a.

However, either method could cause connectivity problems and uneven support for WLANs throughout your wireless network. For example, if you use the second method, certain WLANs are supported only by radios operating in 802.11a mode and others only by radios operating in 802.11bg mode. Users might well have difficulty connecting to the desired WLAN.

Enabling WLANs Using Advanced Mode Configuration

To activate WLANs with advanced mode configuration, complete these steps:

1. Configure WLANs just as you would in normal mode. (Instructions on this process are provided in “Configuring a WLAN” on page 4-26.)

2. Enable advanced configuration:
   a. Select **Network Setup > WLAN Setup**.
   b. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed. (See Figure 4-8.)
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Figure 4-8. Global WLAN Settings Screen

c. Check the Advanced Configuration box, and then click the OK button.

3. Enable the WLANs.

4. You must now manually assign the WLANs to RP radios. You can do this in two ways:

   • You can manually assign WLANs as a part of a default configuration to be sent to any newly adopted RP.

     In this case, the Wireless Edge Services zl Module deploys the WLAN configuration to all RP radios when they are adopted, as it would in normal mode. However, instead of automatically assigning WLAN 1 to BSSID 1, and so on, the module allows you to select which WLANs are assigned to which BSSIDs.

   • You can manually assign WLANs to specific BSSIDs on specific RP radios.

     In this case, only the specified radios support the WLANs.

You can use both types of advanced configuration in conjunction. For example, you can create a radio adoption default configuration, but then override that configuration for specific RP radios after they are adopted.

For more security, you could leave the radio adoption default configuration empty so that newly adopted RP radios do not immediately support your network's WLANs. After you decide that an RP is authorized, you can manually configure the WLAN assignment on its radio or radios.

The following sections supply more information about these two methods.
Manually Assigning WLANs to the Radio Adoption Default Configuration. Configure the radio adoption default configuration to customize the WLANs that the Wireless Edge Services zl Module sends to all newly adopted radios. This configuration actually divides into two parts—one for 802.11a radios and one for 802.11bg radios.

Note

If you decide to use advanced mode configuration after the module has already adopted RPs, any WLAN assignments established in the radio adoption default configurations will not apply to these RPs. You must instead assign the WLANs to specific radios, as explained in “Manually Assigning WLANs to a Specific Radio” on page 4-18.

You should configure the radio adoption default configurations when you want all RPs in your network to support the same WLANs (as they would with normal mode configuration), but for some reason the normal WLAN assignment is inadequate.

For example:

■ You have added several WLANs to your network. You now want RP beacons to include one of the new WLANs in preference to one of the old, but the new WLAN has an index number higher than 4.

■ You have temporarily disabled several WLANs and you want to spread the others more evenly over the BSSIDs.

■ You want to enable more than 16 WLANs on a single RP, so you assign some of the WLANs to 802.11a radios and some to 802.11bg radios.

■ You want to configure different WLAN settings for stations that use different 802.11 types.

If you are using advanced mode to restrict one WLAN to a certain area, then you can create WLAN assignments in the radio adoption default configurations for all other, non-restricted WLANs.

For example, to restrict WLAN 1 to one building, you will explicitly assign that WLAN to RPs in that building, as described in “Manually Assigning WLANs to a Specific Radio” on page 4-18. All other RPs in the wireless network should support WLANs 2 through 5. You create a default configuration for both types of radios (802.11a and 802.11bg), in which you assign these WLANs.

Figure 4-9 displays an environment such as this. This figure also shows the option of enabling SSID A (WLAN 1) on the default configuration, but having SSID E (WLAN 5) be the primary WLAN. (Stations in WLAN 1 can then roam into areas in which WLAN 1 operates in closed system.) In this example, WLAN 1 is less a restricted WLAN than a WLAN that is primarily used by employees in one area.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Figure 4-9. Configuring an Area-Specific WLAN

Note
Depending on whether you enable WLANs or advanced mode configuration first, the radio adoption configuration begins with either the normal WLAN assignment or an empty WLAN assignment. Leaving the WLAN assignment in the default configurations empty is not necessarily undesirable: it can increase security. However, you should be aware that in this case newly adopted radios will not support WLANs until you manually configure them to do so.

To modify the default configuration using advanced mode, complete these steps:

1. Select Network Setup > Radio Adoption Defaults and click the WLAN Assignment tab.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Figure 4-10. Customizing WLAN Assignment for the Radio Adoption Default (Advanced Mode)

2. Choose the radio type from the **Select Radio** drop-down menu.

   **Note**
   If your network includes radios of both types, you should remember to configure a default WLAN assignment for each. Typically, these assignments should match.

   You can assign WLANs to the radio as a whole or to individual BSSIDs.

3. Check the **Assign** box for each WLAN that you want to assign to the radio, and then click the **Apply** button.

4. If you want to assign a specific WLAN to a specific BSSID number, or if you want to choose the primary WLAN, complete steps 5 through 8.

5. Select a BSSID from one of the four listed under the radio. Check the **Assign** box for each WLAN that you want to assign to this BSSID. (You can choose up to four. Generally, but not always, you should fill all four BSSIDs before you assign multiple WLANs to a BSSID.)
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Figure 4-11. Assigning WLANs to a BSSID in the Default Configuration

6. In the Primary WLAN drop-down menu, choose the WLAN for which the radio should beacon the SSID.

7. If you want to assign more WLANs to the radio, select another BSSID and repeat steps 5 and 6.

8. Click the Apply button.

Manually Assigning WLANs to a Specific Radio. Select this option to alter the WLAN assignment on a specific radio. By assigning different WLANs to different RP radios, you can:

- establish different WLANs in different areas of the network
- establish more than 16 WLANs in your network
- have different RP radios beacon different SSIDs

To manually assign WLANs, complete these steps:

1. Select Network Setup > Radio and click the radio that you want to configure.

2. Click the WLAN Assignment tab.
3. Click the **Edit** button. The **Network Setup > Radio > Assign Wireless Lanes to Radios** screen is displayed. (See Figure 4-12.)

![Network Setup > Radio > Assign Wireless Lanes to Radios](image)

**Figure 4-12. Assigning WLANs to a Specific RP Radio**

4. You can assign SSIDs either to the radio as a whole or to a specific BSSID. For example, you could assign SSIDs to the radio if:
   - you are assigning four or fewer WLANs to the radio
   - you are assigning more than four WLANs, but you want the radio to advertise the four with the lowest index numbers

   Complete step 5 to assign SSIDs to the radio as a whole. Complete step 6 to assign SSIDs to a specific BSSID.

5. As shown in Figure 4-13, check the **Assign** box for each WLAN that you want the radio (or radios) to support. You can select up to 16 WLANs, but, as in normal mode, the RP radio only beacons SSIDs for the four WLANs with the lowest index numbers.

   Click the **Apply** button.
6. Alternatively, you can assign a WLAN to a specific BSSID on the radio:
   a. In the left area, **Select Radio/BSS**, select that BSSID.
   b. Check the **Assign** box for each WLAN that you want to assign to the BSSID. You can select up to four WLANs, but as always, the beacons only include one.

   You can select which SSID RPs include in beacons by selecting a WLAN from the **Primary WLAN** drop-down menu.

   Repeat this step for the other BSSIDs until you have assigned all the WLANs that you want this radio to support. Generally, you should assign at least one WLAN to each BSSID before you add multiple WLANs to a BSSID. This maximizes the number of SSIDs that RPs can beacon to wireless stations.
7. Click the **Apply** button, and then click the **Close** button.

The screen such as that in Figure 4-14 is displayed; you can check your configuration in the **Assigned WLAN** area.

![Network Setup > Radio](image)

**Figure 4-14. Selected WLANs Assigned to Radio 1 (Using Advanced Mode)**

When you assign WLANs to the radio as a whole, as opposed to the BSSID, the Wireless Edge Services zl Module allocates SSIDs to the radio’s four BSSIDs much as it does in normal mode. However, only the SSIDs of the WLANs that you selected are part of the process. Instead of always assigning WLAN 1 to BSSID 1 and WLAN 2 to BSSID 2, the module assigns the SSID for the enabled WLAN with the lowest index number to BSSID 1, and so on.

For example, you use advanced mode configuration to assign WLANs 2, 4, 5, and 6 to a particular RP radio. The Wireless Edge Services zl Module assigns SSID B (for WLAN 2) to BSSID 1, SSID D (for WLAN 4) to BSSID 2, and so on.

Figure 4-15 illustrates this configuration.
Figure 4-15. Manually Assigning WLANs to an RP Radio

Figure 4-14 shows the **Network Setup > Radio** screen in which you would check this configuration.

If you had assigned a fifth WLAN to the radio, then two SSIDs would be assigned to BSSID 1, and beacons would advertise only one of these SSIDs.

If you want the beacons to include the WLAN with the higher index number, then you should select the BSSID for the WLAN on the **Network Setup > Radio > WLAN Assignment** screen. Then select the higher WLAN from the **Primary WLAN** drop-down menu, as shown in Figure 4-13.

**Using Normal and Advanced Mode Together**

Rather than using advanced mode alone, it is often a good idea to first enable WLANs in normal mode, producing a template WLAN assignment that you can then alter with advanced mode configuration.

To use normal and advanced mode together, complete these steps:

1. Select **Network Setup > WLAN Setup**.
2. Configure the WLANs, as described in “Configuring a WLAN” on page 4-26.
3. On the Network Setup > WLAN Setup screen, select the WLANs, and then click Enable.

4. Click the Global Settings button. The Global WLAN Settings screen is displayed.

5. Check the Advanced Configuration box, and then click the OK button.

6. If necessary, tailor the radio adoption default configurations:
   a. Select Network Setup > Radio Adoption Defaults and click the WLAN Assignment tab.
   b. Edit the WLAN assignment, as described in “Manually Assigning WLANs to the Radio Adoption Default Configuration” on page 4-15. For example, you might select a different WLAN from the Primary WLAN drop-down menu.

7. If necessary, tailor a specific radio’s configuration:
   a. Select Network Setup > Radio and click the WLAN Assignment tab.
   b. Select the radio and click the Edit button.
   c. Edit the WLAN assignment, as described in “Manually Assigning WLANs to a Specific Radio” on page 4-18. For example, you can prevent an RP in a public space from supporting a WLAN by unchecking the Assign box for that WLAN’s SSID.

Changing from Advanced Mode to Normal Mode Configuration

Before disabling advanced mode configuration, you must verify that all WLAN assignments are compatible with normal mode. Check that:

- WLANs 1, 5, 9, and 13 (if enabled) are assigned to BSSID 1
- WLANs 2, 6, 10, and 14 (if enabled) are assigned to BSSID 2
- WLANs 3, 7, 11, and 15 (if enabled) are assigned to BSSID 3
- WLANs 4, 8, 12, and 16 (if enabled) are assigned to BSSID 4

If necessary, reconfigure the WLAN assignments as described in “Enabling WLANs Using Advanced Mode Configuration” on page 4-13. You must also remove all WLANs with indexes 17 and higher from the BSSIDs.

Note

WLANs 17 through 256 are not available in normal mode. If you want the Wireless Edge Services zl Module to continue supporting one of these WLANs, then you must configure the corresponding SSID and settings on a WLAN with an index number from 1 through 16.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

You must check the WLAN assignment for all of the following configurations:
- the radio adoption default configuration for 802.11a radios
- the radio adoption default configuration for 802.11bg radios
- the configuration for every RP radio adopted by your module

To disable advanced mode configuration, complete these steps:
1. Click **Network Setup > WLAN Setup**.
2. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.
3. Uncheck the **Advanced Configuration** box, and then click the **OK** button. The screen shown in Figure 4-16 is displayed.

![Advanced Configuration](image)

**Figure 4-16. Disabling Advanced Configuration**

4. Click the **No** button if you have verified that the WLAN assignment is compatible with normal mode. This option disables advanced mode, but leaves currently enabled WLANs active.

**Caution**

Take care when selecting the button. Clicking the **Yes** button and clicking the **No** button will both disable advanced mode. However, clicking the **Yes** button also disables all WLANs.

If you click the **No** button but the WLAN assignment is incorrect, the screen shown in Figure 4-17 is displayed.
Wireless Local Area Networks (WLANs)
Configuration Options: Normal Versus Advanced Mode

Click the OK button. You can now either:
- check the WLAN assignments on all radios and default configurations, reassigning SSIDs to BSSIDs as described at the beginning of this section
- execute a forced disable by clicking the Yes button

Click the Yes button to force advanced mode to disable. This option disables advanced mode configuration as well as all WLANs, even those that are compatible with normal mode. Take care when selecting this option because it disassociates wireless stations and can disrupt network activity.

After you click the Yes button, you should move to the Network Setup > WLAN Setup screen and re-enable the WLANs. The Wireless Edge Services 21 Module then assigns the SSIDs to the correct BSSIDs.

Click the Cancel button to continue using advanced mode configuration.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

Configuring a WLAN

To configure a WLAN, you must set:
■ the SSID
■ the VLAN in which traffic will be forwarded
■ security options, which include:
  • authentication method
  • encryption option

Optionally, you can configure:
■ advanced settings for individual WLANs, which include:
  • inter-station blocking
  • closed system operations
  • inactivity timeouts
■ global settings for all WLANs, which include:
  • proxy Address Resolution Protocol (ARP)
  • shared-key authentication

The following sections will guide you through the process of configuring these settings. The first step is accessing the Network Setup > WLAN Setup > Configuration screen.
As you can see in Figure 4-18, this screen displays the 256 WLANs that are available for configuration. Remember that in normal configuration mode, you can only configure WLANs 1 through 16.

On the Wireless Edge Services zl Module, you do not create WLANs as such. The module has already created them; you configure options for and enable the WLANs. The default configuration for each WLAN is displayed in seven columns:

- **Index**—Lists the WLANs by index number. Although you will create your own name for the WLAN, this index number is important because it determines which WLAN is the primary WLAN on a BSSID, if you enable more than four WLANs. (By default, the WLAN on the BSSID with the lowest number is the primary WLAN.)
Wireless Local Area Networks (WLANs)
Configuring a WLAN

- **Enabled**—Indicates whether the WLAN has been enabled. The Wireless Edge Services zl Module does not deploy a WLAN configuration to RPs until you enable the WLAN. By default, all WLANs are disabled.
- **SSID**—Displays the WLAN's SSID. By default, this SSID simply indicates the WLAN's index number. You will change this to a network name when you configure the WLAN.
- **Description**—Describes the WLAN so that you can quickly see its purpose. For example, it might read “Internet access for guests.”
- **VLAN**—Displays the VLAN interface in which traffic received from this WLAN is forwarded. Initially, all WLANs are assigned to the default VLAN, VLAN 1. You will learn more about VLAN assignment in “Setting Basic Configuration Options: SSID and VLAN Interface” on page 4-30 and “VLAN Assignment” on page 4-80.
- **Authentication** and **Encryption**—Display the security options implemented on the WLAN.

When you want to establish a new WLAN in your network (or to alter settings of an existing WLAN), select a WLAN and click the **Edit** button at the bottom of the screen.

**Note**
You must select a WLAN with index number 1 to 16 unless you enable advanced mode configuration. See “Advanced Mode Configuration” on page 4-11.
The screen illustrated in Figure 4-19 is displayed: this is the Edit screen for the selected WLAN. On this screen, you configure settings for your WLAN.

Figure 4-19. Editing a WLAN

In the Configuration section, you create the WLAN’s basic settings.

Configure security standards in the Authentication and Encryption sections. If you choose an authentication option that requires a RADIUS server, the RADIUS Config... button is enabled, and you can configure RADIUS settings.

Optionally, you can configure advanced options in the Advanced section.

The following sections explain in more detail how to configure these settings. However, the advanced options that deal specifically with quality of service (QoS) are described in “Traffic Management (QoS)” on page 4-89.
Setting Basic Configuration Options: SSID and VLAN Interface

You must set the following options in the Configuration section of a WLAN's Edit screen:

- the SSID

  The SSID identifies the WLAN; stations associated to the same SSID are in the same WLAN regardless of the RP radio to which they have associated. The SSID is sometimes called the network name; it is the name that users see when they search for wireless networks to which to connect (as long as the WLAN operates in open system).

  Because SSIDs distinguish WLANs from each other, each WLAN must have a unique SSID.

- the VLAN interface associated with the WLAN

  It is the Wireless Edge Services zl Module's role to ready traffic received from RPs for transmission into the Ethernet network. The module removes the 802.11 header and adds an Ethernet header. This header includes a 802.1Q tag for a particular VLAN. In other words, the module assigns stations in the WLAN to a VLAN.

  By default, the module places all wireless traffic in VLAN 1. If your network only uses one subnetwork, this configuration is adequate. Many networks, however, include multiple subnetworks, of which VLAN 1 is sometimes the management VLAN. Because of security, as well as other concerns, you should often assign the WLAN a new VLAN ID.

  You can tag wireless traffic for one of your network's user VLANs, or you can create a separate VLAN entirely dedicated to wireless stations. If you choose the second option, of course, you must ensure traffic can reach its destination. For example, configure the Wireless Edge Services zl Module to route traffic. You might also need to configure Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) services on the VLAN. See “Reserving VLANs for Wireless Users” on page 1-19 of Chapter 1: “Introduction” for more explanation.

  Your network might include a RADIUS server that assigns users to VLANs based on their identities. Enable dynamic VLANs to allow the module to enforce these assignments. (The VLAN ID that you configure manually remains the default for users not assigned to a dynamic VLAN.)

  You can also enter a description, but this setting is optional.
To configure these options, follow these steps:

1. Access the Edit screen for the WLAN, as described in “Configuring a WLAN” on page 4-26.

2. Under Configuration, in the SSID field, enter the SSID that you have selected for this WLAN.

When you enable the WLAN, the Wireless Edge Services zl Module automatically configures this SSID on all adopted RP radios (as long as you are using normal mode). For more information on how the module does this, see “Normal Mode Configuration” on page 4-4.

3. In the Description field, enter information about this WLAN to remind you and other administrators of its purpose.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

For example, if this WLAN provides network access for sales representatives in conference rooms, you could enter “Sales/Conference Rooms.” (This information is for reference only and is not sent to the RPs nor broadcast to wireless stations.)

4. In the VLAN ID field, specify the VLAN to which the module maps wireless traffic. The VLAN ID can be a value from 1 to 4096.

![Image](Figure 4-21. Setting the VLAN ID)

5. Check the Dynamic Assignment box to enable the Wireless Edge Services 2L Module to apply dynamic (or user-based) VLAN assignments received from a RADIUS server.

Do not use dynamic VLAN assignment when the WLAN requires Layer 3 mobility.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

If the WLAN uses Web-Auth set the DHCP lease for the WLAN’s static VLAN very low. This allows the station to request a new IP address in the dynamic VLAN after the user authenticates.

6. Continue configuring the WLAN. See “Configuring Security Options” on page 4-33. (Or click OK to apply the settings and close the Edit screen.)

Necessary Configurations on the Wireless Services-Enabled Switch

The VLAN for which the Wireless Edge Services zl Module tags WLAN traffic is called an uplink VLAN. If you decide to have your Ethernet infrastructure devices route traffic from the wireless stations, you must tag the module’s uplink port for the stations’ VLAN. You make this configuration from the wireless services-enabled switch. (See the Wireless Edge Services zl Module Supplement to the 6200yl/5400zl/3500yl Management and Configuration.) Alternatively, you can have the Wireless Edge Services zl Module route wireless traffic and perform other necessary services for the wireless stations’ VLAN. In this case, no further configuration on the wireless services-enabled switch is necessary.

Configuring Security Options

From the Network Setup > WLAN Setup > Edit screen, you can also configure authentication and encryption options.

The security provided by a WLAN is one of its most important functions. All RPs in a WLAN must use the same security options and, for some security options, static keys. Therefore, the Wireless Edge Services zl Module, which automatically deploys the same WLAN configuration to all adopted RPs, simplifies establishing a WLAN throughout a wireless network. Remember, however, that if your network includes more than one Wireless Edge Services zl Module, you must configure exactly the same security options for identical WLANs on different modules.

Configuring Authentication

For the best security, you should enable some form of authentication on every WLAN. Authentication protects your network resources from unauthorized access; it can also protect wireless stations from connecting to a rogue access point (AP).
Wireless Local Area Networks (WLANs)
Configuring a WLAN

The Wireless Edge Services zl Module supports three types of authentication:
- 802.1X Extensible Authentication Protocol (EAP)
- Web authentication (Web-Auth)
- Media Access Control (MAC) authentication

You configure authentication methods as part of each individual WLAN's settings, and, as far as that WLAN is concerned, they are mutually exclusive. For example, a WLAN can require stations to authenticate using 802.1X or using Web-Auth, but not both. However, one WLAN can require 802.1X and a different WLAN, Web-Auth.

The MAC authentication configured on a WLAN is MAC authentication to a RADIUS server. That is, the module forwards stations' MAC addresses to be checked against accounts stored on a network server.

The Wireless Edge Services zl Module can also enforce de facto local MAC authentication, using globally configured filters, or MAC standard access control lists (ACLs), that are applied to the WLAN. You can combine these filters with another type of authentication: first, the MAC ACLs filter association requests; then the WLAN's specific authentication method initiates. See “MAC Filters (Local MAC Authentication)” on page 12-75 of Chapter 12: “Wireless Network Management” to learn how to configure MAC standard ACLs.

802.1X EAP. 802.1X is the IEEE standard for wireless authentication. When a station attempts to connect to a WLAN that uses this standard, the Wireless Edge Services zl Module places the association in closed status, dropping all traffic except EAP messages. The module forwards these messages to an authentication server (RADIUS server), and the station and server verify each other's identities. During the authentication process, the station and module also receive dynamic keys for encryption.

As an alternative to a network RADIUS server, you can use the Wireless Edge Services zl Module's internal RADIUS capabilities. See Chapter 11: “RADIUS Server” for more information.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

Figure 4-22. Enabling 802.1X Authentication

To configure 802.1X authentication for a WLAN, complete these steps:

1. Click **Network Setup > WLAN Setup**.
2. Select the WLAN and click the **Edit** button.
3. Under **Authentication**, select **802.1X EAP**.
4. Optionally, click the **Config** button next to **802.1X EAP** to configure some advanced settings for the station:
Figure 4-23. Specifying 802.1X EAP Settings

a. Enter a value in the **Station Timeout** field to control how long the module will wait for a station to authenticate itself.

   The **Station Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

b. Enter a value in the **Station Retries** field to control how many times the module will reissue a challenge to the station.

   The setting for **Station Retries** can be from 1 to 10; the default setting is 3.

c. Click the **OK** button. You return to the WLAN’s **Edit** screen.

5. 802.1X requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.
6. In the **Radius Configuration** screen, under **Server**, specify settings for your network’s RADIUS servers.

   Enter settings for your primary server in the fields in the **Primary** column:
   a. In the **RADIUS Server Address** field, specify the IP address of your network's primary RADIUS server.

      To use the module's internal server, enter 127.0.0.1.

   b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

      The default value is 1812.
c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

The RADIUS server uses the secret to identify the Wireless Edge Services zl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server's configuration.

If you are using the module's internal server, you do not need to enter a shared secret.

d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

7. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

8. Optionally, alter settings in the **Advanced** section:
   - Enter a value in the **Server Timeout** to control how long the Wireless Edge Services zl Module will wait for a reply from the RADIUS server.

   The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   - Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

   The setting for **Server Retries** can be from 1 to 10. By default, the Wireless Edge Services zl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

9. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.

   Valid values range from 0 through 63.

   a. Leave the other settings at their defaults and click the **OK** button. You will return to the WLAN's **Edit** screen.

10. You must now configure the encryption option. See “Configuring Encryption” on page 4-47.
Web-Auth. Web-Auth allows wireless stations that do not support 802.1X to authenticate to a RADIUS server. Web-Auth is an easy-to-use option that is often selected for wireless networks that provide Internet or limited network access to a broad range of users. The instructions below simply guide you through the most basic Web-Auth settings. You should refer to Chapter 5: “Web Authentication for Mobile Users” to learn how to configure more advanced options and customize Web pages.

Note
You can configure local MAC authentication for more security in a WLAN using Web-Auth. (See Chapter 12: “Wireless Network Management.”)

To enable Web-Auth on a WLAN, complete these steps:
1. Select Network Setup > WLAN Setup and click the Configuration tab.
2. Select the WLAN that you want to use Web-Auth, and then click the Edit button. The Edit screen is displayed.

![Figure 4-25. Enabling Web-Auth](image-url)
Wireless Local Area Networks (WLANs)
Configuring a WLAN

3. Under **Authentication**, select **Web-Auth**.

**Note**

On the configuration screens that appear in this procedure, you can quickly get the WLAN running by completing these minimal steps. (Learn more about the process in Chapter 5: "Web Authentication for Mobile Users").

4. Click the **Config** button next to **Web-Auth**. The **Web-Auth** screen is displayed.

![Figure 4-26. Configuring the Allow](image-url)
5. On the **Web-Auth** screen, under **Allow List**, add the IP addresses that *unauthorized* stations are allowed to access.

The Wireless Edge Services zl Module automatically handles traffic such as DHCP and Domain Name System (DNS) requests. Therefore, even if you do not add any IP addresses to the Allow list, Web-Auth using the internal pages functions correctly.

6. Leave other settings at their defaults and click the **OK** button.

7. Web-Auth requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.

![Radius Configuration Screen](image)
8. In the **Radius Configuration** screen, under **Server**, specify settings for your network’s RADIUS servers.

Enter settings for your primary server in the fields in the **Primary** column:

a. In the **RADIUS Server Address** field, specify the IP address of your network’s primary RADIUS server.

   To use the module’s internal server, enter 127.0.0.1.

b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

   The default value is 1812.

c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

   The RADIUS server uses the secret to identify the Wireless Edge Services zl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server’s configuration.

   If you are using the module’s internal server, you do not need to enter a shared secret.

d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

9. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

   Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

10. Optionally, alter settings in the **Advanced** section:

   • Enter a value in the **Server Timeout** to control how long the Wireless Edge Services zl Module will wait for a reply from the RADIUS server.

     The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   • Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

     The setting for **Server Retries** can be from 1 to 10. By default, the Wireless Edge Services zl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

11. Choose the protocol in which the Wireless Edge Services zl Module packages users’ credentials. Select **PAP** (the default) or **CHAP** for the **Authentication Protocol**.
12. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.
   Valid values range from 0 through 63.
13. Leave the other settings at their defaults and click the OK button.
14. You should now configure the encryption options. See “Configuring Encryption” on page 4-47.

**MAC Authentication.** The MAC Authentication option refers to RADIUS MAC authentication. When a station attempts to associate with the WLAN, the Wireless Edge Services zl Module forwards the station’s MAC address in a request to a RADIUS server. The RADIUS server decides whether the station can associate.

To configure MAC authentication, complete these steps:

1. Access the Edit screen for the WLAN:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN that should use MAC authentication and click the **Edit** button.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

Figure 4-28. Enabling MAC Authentication

2. Under **Authentication**, select **MAC Authentication**.
3. This authentication option requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.
4. In the **Radius Configuration** screen, under **Server**, specify settings for your network's RADIUS servers.

   Enter settings for your primary server in the fields in the **Primary** column:
   
   a. In the **RADIUS Server Address** field, specify the IP address of your network's primary RADIUS server.
      
      To use the module's internal server, enter 127.0.0.1.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

The default value is 1812.

c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

The RADIUS server uses the secret to identify the Wireless Edge Services zl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server's configuration.

If you are using the module’s internal server, you do not need to enter a shared secret.

d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

5. Optionally, alter other RADIUS server settings:

   • Enter a value in the **Server Timeout** to control how long the Wireless Edge Services zl Module will wait for a reply from the RADIUS server.

     The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   • Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

     The setting for **Server Retries** can be from 1 to 10. By default, the value is 3; Wireless Edge Services zl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

6. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

   Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

7. Choose the RADIUS protocol in which the Wireless Edge Services zl Module packages the MAC address. Select **PAP** (the default) or **CHAP** for the **Authentication Protocol**.

8. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.

   Valid values range from 0 through 63.
9. In the **MAC Address** section, choose the format in which the Wireless Edge Services zl Module forwards the MAC address.

The module sends the station’s MAC address as the username and the password in the RADIUS request. The username and password must match exactly those in the account against which the RADIUS server checks them. For example, if the account uses delimiters in the MAC address, the module must use delimiters in the same places.

Choose from among five options for the format:

- **No Delimiter** (xxxxxxxxxxxx)
- **Multi Colon** (xx:xx:xx:xx:xx:xx)
- **Multi Dash** (xx-xx-xx-xx-xx-xx)
- **Quad Dot** (xxxx.xxxx.xxxx)
- **Single Dash** (xxxxxx-xxxxxx)

10. Click the **OK** button.

11. If you want to use encryption, you should now configure the encryption option. See “Configuring Encryption” on page 4-47.

**Configuring Encryption**

Encryption ensures the privacy of data sent through the wireless medium. Even if hackers intercept packets, they cannot decrypt them without the correct key.

The WLANs controlled by the Wireless Edge Services zl Module can support any of these encryption standards, listed from least secure to most secure:

- Wired Equivalent Privacy (WEP) with a 64-bit
- WEP with a 128-bit key
- Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Integrity Protocol (TKIP)
- WPA2 with Advanced Encryption Standard (AES)

No matter which type of authentication you select, you can select any type of encryption. You can select both WPA/WPA2-TKIP and WPA2-AES at the same time. However, all other encryption options are mutually exclusive.

If your WLAN does not use authentication, the encryption option enforces a de facto authentication: the user must enter the correct encryption key in order to connect to the WLAN. However, this form of authentication is less secure, particularly when used with WEP.
Wireless Local Area Networks (WLANs)

Configuring a WLAN

Table 4-2 displays the names that this management and configuration guide uses for combinations of authentication and encryption options.

Table 4-2. Encryption and Authentication Options

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Encryption</th>
<th>Called</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>WEP (64-bit or 128-bit)</td>
<td>Static WEP</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2 TKIP</td>
<td>WPA/WPA2 with preshared keys (PSK)</td>
</tr>
<tr>
<td></td>
<td>WPA2 AES</td>
<td>WPA2-PSK</td>
</tr>
<tr>
<td>MAC authentication</td>
<td>None</td>
<td>RADIUS MAC authentication</td>
</tr>
<tr>
<td></td>
<td>WEP (64-bit or 128-bit)</td>
<td>RADIUS MAC authentication and static WEP</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2 TKIP</td>
<td>RADIUS MAC authentication and WPA/WPA2-PSK</td>
</tr>
<tr>
<td></td>
<td>WPA2 AES</td>
<td>RADIUS MAC authentication and WPA2-PSK</td>
</tr>
<tr>
<td>802.1X</td>
<td>WEP (64-bit or 128-bit)</td>
<td>Dynamic WEP</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2 TKIP</td>
<td>WPA/WPA2 with 802.1X</td>
</tr>
<tr>
<td></td>
<td>WPA2 AES</td>
<td>WPA2 with 802.1X (802.11i standard)</td>
</tr>
<tr>
<td>Web-Auth</td>
<td>None</td>
<td>Web-Auth</td>
</tr>
<tr>
<td></td>
<td>WEP (64-bit or 128-bit)</td>
<td>Web-Auth and static WEP</td>
</tr>
<tr>
<td></td>
<td>WPA/WPA2 TKIP</td>
<td>Web-Auth and WPA/WPA2-PSK</td>
</tr>
<tr>
<td></td>
<td>WPA2 AES</td>
<td>Web-Auth</td>
</tr>
</tbody>
</table>

Configuring Static WEP Encryption (No Authentication). If you enable WEP encryption without authentication, WEP keys both encrypt wireless traffic and provide rudimentary authentication. You set the WEP key manually; wireless users must enter the same key before they can connect to the WLAN. This security option is sometimes called static WEP because you set the key manually.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

**Note**
By default, all WLANs use open-key authentication for WEP, which means that all stations can associate. However, the Wireless Edge Services zI Module quietly drops any incorrectly encrypted frames, ensuring that only stations that have the correct key can forward data and truly connect to the WLAN.

An alternative to open-key authentication, shared-key authentication, has been denigrated because it leaks information about the WEP key. You should only use this option if required by your stations. See “Configuring Global WLAN Settings” on page 4-75 for information on enabling shared-key authentication.

To configure static WEP, complete these steps:

1. Access the **Edit** screen for the WLAN that is to use static WEP:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)
2. Under **Authentication**, select **No Authentication**.
3. Under **Encryption**, check either the **WEP 64** or **WEP 128** box.
4. Click the corresponding **Config** button. The **WEP 64** or **WEP 128** screen is displayed.
5. Specify the static key.

The Wireless Edge Services zl Module provides several options for configuring static keys:

- It can automatically generate four hex keys from a manually entered pass key.

Enter a string from 4 to 32 characters in the **Pass Key** field and click the **Generate** button.

As shown in Figure 4-31, the Wireless Edge Services zl Module then creates four different keys, which automatically appear in the **Key** fields. Note that these keys are in hexadecimal. Wireless users can enter the keys in this form, or you can convert the hex number to an ASCII string and tell users that string.

- You can manually enter up to four hex keys.
- You can manually enter up to four ASCII keys.

If you want to set one or more of the four keys yourself, simply move your cursor to the field for that key and enter the key. You can enter the key in hexadecimal (the first field) or in ASCII (the second field). If you want, you can specify some keys in hexadecimal and others in ASCII. You can also generate four keys from a pass key, and then change one or more of the keys.
The number of characters for the key depends on the WEP key length and on the format in which you enter the key. Table 4-3 summarizes these requirements.

**Table 4-3. Key Length for Static WEP Keys**

<table>
<thead>
<tr>
<th>Key Length</th>
<th>Format</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>Hexadecimal</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>ASCII</td>
<td>5</td>
</tr>
<tr>
<td>128-bit</td>
<td>Hexadecimal</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>ASCII</td>
<td>13</td>
</tr>
</tbody>
</table>

The key next to the selected circle (Key 1 in Figure 4-31) is the key that currently encrypts and decrypts data. For greater security, remember to periodically change which key is in use.

**Note**

The more often an encryption key is used, the more vulnerable it is to hackers. Even when administrators diligently rotate and change WEP keys, this form of WEP is significantly less secure than WEP with 802.1X authentication or WPA/WPA2.

6. If you want to return this WLAN to the default static WEP keys, click the **Restore Default WEP Keys** button.

   Another screen is displayed, asking you to confirm the return to the default keys. If you are sure, click **Yes**. You still have one more chance to change your mind. The keys do not return to the defaults until you click the **OK** button and close the screen. You can view the default values for WEP keys through the CLI by entering this command: `show running-config include-factory`.

7. After you set the key, click the **OK** button. Then click the **OK** button on the WLAN's **Edit** screen to apply the settings.

**Configuring WEP Encryption with 802.1X Authentication (Dynamic WEP).** WEP with 802.1X authentication is also called dynamic WEP because 802.1X helps to distribute encryption keys automatically. The Wireless Edge Services Z1 Module and stations encrypt and decrypt data with WEP keys; however, instead of every station using the same key, stations first identify themselves to a network authentication server. When a station passes the authentication test, the station and the authentication server generate a unique WEP key for that session alone, which the server passes to the module.
To configure this type of security for a WLAN, complete these steps:

1. Access the Edit screen for the WLAN that is to use dynamic WEP:
   a. Select Network Setup > WLAN Setup and click the Configuration tab.
   b. Select the WLAN and click the Edit button. The Edit screen is displayed. (See Figure 4-30.)

2. Enable 802.1X authentication and specify the RADIUS server. (See “802.1X EAP” on page 4-34.)

3. On the WLAN's Edit screen, under Encryption, check either the WEP 64 or WEP 128 box, as shown in Figure 4-32.

![Figure 4-32. Specifying WEP Encryption with 802.1X Authentication (Dynamic WEP)](image-url)
Do not select the Config button to configure the WEP key; the RADIUS server automatically generates and sends the dynamic WEP keys to successfully authenticated users.

If you click the Config button, the message in Figure 4-33 is displayed. The message does not indicate a problem: it simply informs you that you have completed all necessary steps for configuring encryption on this WLAN.

Figure 4-33. No Need to Configure WEP Keys When the WLAN Uses 802.1X

Configuring WPA/WPA2 with 802.1X. WPA and WPA2 are similar standards, both of which provide more robust encryption than WEP and rely on 802.1X authentication. Both standards generate hierarchies (or sets) of encryption keys. In the key hierarchy, each station has its own pairwise key, which the Wireless Edge Services Module also knows. All stations in the same WLAN use the same group key for multicast and broadcast traffic. WPA uses TKIP for the key hierarchy and WPA2 uses CCMP with AES encryption.

To configure WPA/WPA2, you must select the protocol: TKIP, AES, or both. AES is the most secure form of encryption and the one specified by WPA2 and 802.11i. However, not all stations support AES encryption.

In the Edit screen for a WLAN, as shown in Figure 4-34, the two options for WPA/WPA2 encryption are listed as:

- WPA/WPA2-TKIP
- WPA2-AES
Table 4-4 displays the types of stations supported by each option. It also lists which protocols each option uses to generate group (multicast and broadcast) keys and to generate pairwise (per-session) keys.
Wireless Local Area Networks (WLANs)

Configuring a WLAN

Table 4-4. Options for WPA/WPA2

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Multicast and Broadcast Keys</th>
<th>Per-Session Keys</th>
<th>Supported Stations</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA/WPA2 TKIP</td>
<td>TKIP</td>
<td>TKIP</td>
<td>• WPA-enabled stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• WPA2-enabled stations</td>
</tr>
<tr>
<td>WPA2 AES</td>
<td>AES</td>
<td>AES</td>
<td>• WPA-enabled stations with support for AES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• WPA2-enabled stations</td>
</tr>
<tr>
<td>WPA/WPA2 TKIP and WPA2 AES</td>
<td>TKIP</td>
<td>TKIP or AES</td>
<td>• WPA-enabled stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• WPA2-enabled stations</td>
</tr>
</tbody>
</table>

Note that WPA2-enabled stations can connect to a WLAN that uses any of these options. By default, WPA2 stations can use TKIP to associate to a WLAN. You can turn off this option in the CLI, but typically should not.

WPA-enabled stations can only connect to a WPA2 AES WLAN if they have software to support AES encryption.

To configure WPA/WPA2 encryption, complete these steps:

1. Access the **Edit** screen for the WLAN that is to use WPA/WPA2 with 802.1X:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)

2. Under **Authentication**, select **802.1X EAP**.

3. Under **Encryption**, select your encryption protocol:
   - To use TKIP, check the **WPA/WPA2-TKIP** box.
     The Wireless Edge Services zl Module and wireless stations will use TKIP for all encryption. Note that both WPA and WPA2 stations can connect, but WPA2 stations will use TKIP.
   - To use AES, check the **WPA2-AES** box.
     This option forces all wireless stations to use AES, the most secure algorithm used for wireless encryption.
   - To allow both protocols (mixed-mode), check both boxes.

4. If you want, you can also configure advanced options:
   a. Click the **Config** button in the WPA section of the **Edit** screen. The **WPA/WPA2** screen is displayed.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

Figure 4-35. Advanced Options for WPA/WPA2

<table>
<thead>
<tr>
<th>Key Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Broadcast Key Rotation</strong></td>
</tr>
<tr>
<td><strong>Update broadcast keys every</strong></td>
</tr>
<tr>
<td><strong>ASCII Passphrase</strong></td>
</tr>
<tr>
<td><strong>Enter 9-63 ASCII characters</strong></td>
</tr>
<tr>
<td><strong>256-bit key</strong></td>
</tr>
<tr>
<td><strong>Enter 16 hex characters in each field</strong></td>
</tr>
<tr>
<td><strong>Fast Roaming (802.1x only)</strong></td>
</tr>
<tr>
<td><strong>PMIC Caching</strong></td>
</tr>
</tbody>
</table>

b. If you want, check the **Broadcast Key Rotation** box.

Because all stations must use the same broadcast key, this key is clearly more vulnerable to hackers than the per-session keys. Periodically changing the broadcast key helps to protect your WLAN.

By default, the Wireless Edge Services zl Module does not rotate the broadcast key. However, if you enable the feature, the default rotation period is every 7,200 seconds (two hours).

In the **Update broadcast keys every** field, you can enter any value from 60 seconds (one minute) through 86,400 seconds (one day). The shorter the rotation period, the more secure, but also the more overhead added by the key redistribution.

c. You can also enable fast roaming features (to speed roaming with 802.1X).

A station might roam back and forth between several RPs. Ideally, such roaming is hidden from the wireless user, who need not know when he or she connects to a new RP, but only that the wireless connection remains good.
Fast roaming speeds authentication to a new RP, which can be the most time-consuming phase of the roam, so it only applies to WLANs that use 802.1X authentication.

Check these boxes to enable the Wireless Edge Services zl Module’s fast roaming capabilities:

- **PMK Caching**—The RP and the wireless station agree on a PMK identifier for their session, which each stores even after the station disassociates. If the wireless station roams back to the RP, the two can quickly exchange the PMK identifier and renegotiate necessary keys, instead of completing the entire authentication process.

**Note** When PMK caching is enabled, a WPA2 station that roams is no longer controlled by any dynamic ACLs configured with IDM. If you use IDM to assign ACLs to users with WPA2 connections, you should disable PMK caching.

- **Opportunistic Key Caching**—This capability further speeds roaming between RPs that are connected to the same module. The wireless station can use the same PMK to associate to any RP that connects to the module.

- **Pre-Authentication**—Pre-authentication speeds roaming for stations that move from an RP on a different Wireless Edge Services to an RP on this module.

  The station must also support pre-authentication. It listens for beacons from other RPs that support its SSID and authenticates to them before it roams. The station sends its EAP messages through its current RP, and that RP’s module broadcasts the EAP messages throughout the wired network. Pre-authentication allows your module to listen for and respond to EAP messages destined to its RPs.

  After you have configured all the advanced options that you desire, click the **OK** button.

5. Click the **OK** button.

**Configuring WPA/WPA2-PSK.** As noted above, WPA/WPA2 typically requires 802.1X authentication. However, for networks that do not have a RADIUS server, you can set a password, or preshared key, instead of enforcing 802.1X. All users must enter this same preshared key to connect to the WLAN.

Although a preshared key is less secure than 802.1X authentication, the WPA/WPA2 encryption is still quite strong. WPA/WPA2-PSK is a far better option than static WEP for small to medium networks.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

For more information on WPA/WPA2 encryption, see the introduction to “Configuring WPA/WPA2 with 802.1X” on page 4-54. To configure WPA/WPA-PSK on a WLAN complete these steps:

1. Access the Edit screen for the WLAN that is to use WPA/WPA2-PSK:
   a. Select Network Setup > WLAN Setup and click the Configuration tab.
   b. Select the WLAN and click the Edit button. The Edit screen is displayed. (See Figure 4-30.)

2. Under Authentication, select No Authentication.

3. Under Encryption, select your encryption protocol:
   - To use TKIP, check the WPA/WPA2-TKIP box.
     The Wireless Edge Services zl Module and wireless stations will use TKIP for all encryption. Note that both WPA and WPA2 stations can connect, but WPA2 stations will use TKIP.
   - To use AES, check the WPA2-AES box.
     This option forces all wireless stations to use AES, the most secure algorithm used for wireless encryption.
   - To allow both protocols (mixed-mode), check both boxes.

4. Specify the preshared key that users must enter to connect to the WLAN.
   a. Click the Config button next to the WPA encryption options. The WPA/WPA2 screen is displayed.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

Figure 4-36. Configuring a Key for WPA/WPA2 Encryption with No Authentication

b. Enter the preshared key.

As always, you should select a key that conforms to the highest security standards. The longer the key and the more special characters it contains, the more secure it is. (The key must be at least 22 characters to withstand a brute force attack.)

You can enter the key in one of two ways:

– Select ASCII Passphrase, and then enter a password of from 8 to 63 characters. Users must enter the same characters to access the WLAN.

– Select 256-bit key, and then enter the key manually in hexadecimal. Enter 16 characters in each of the four fields.

5. If you want, check the Broadcast Key Rotation box.

Because all stations must use the same broadcast key, this key is clearly more vulnerable to hackers than the per-session keys. Periodically changing the broadcast key helps to protect your WLAN.

By default, the Wireless Edge Services 2 Module does not rotate the broadcast key. However, if you enable the feature, the default rotation period is every 7,200 seconds (two hours).
In the **Update broadcast keys every** field, you can enter any value from 60 seconds (one minute) through 86,400 seconds (one day). The shorter the rotation period, the more secure, but also the more overhead added by the key redistribution.

6. Click the **OK** button to apply your settings and close the **WPA/WPA2** screen.

7. Click the **OK** button in the WLAN’s **Edit** screen to apply your settings.

### Configuring Encryption for a WLAN that Uses MAC Authentication.

A WLAN that enforces MAC authentication to a network server can also provide wireless encryption. In this case, a wireless user must pass two tests to connect to the WLAN: the user’s station must pass MAC authentication, and the user must enter the correct WEP or WPA/WPA2 key.

This section explains how to add encryption to a WLAN already configured for RADIUS MAC authentication. See “MAC Authentication” on page 4-43 for instructions on configuring the authentication.

After selecting **MAC Authentication** in a WLAN’s **Edit** screen, you have several choices for which boxes in the **Encryption** section to check. Table 4-5 summarizes these options and refers you to section that explains how to configure the second security option.

### Table 4-5. Encryption Options for RADIUS MAC Authentication

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Security Option</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP 64</td>
<td>static WEP</td>
<td>“Configuring Static WEP Encryption (No Authentication)” on page 4-48</td>
</tr>
<tr>
<td>WEP 128</td>
<td>static WEP</td>
<td>“Configuring Static WEP Encryption (No Authentication)” on page 4-48</td>
</tr>
<tr>
<td>WPA/WPA2-TKIP</td>
<td>WPA/WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
<tr>
<td>WPA2-AES</td>
<td>WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
<tr>
<td>WPA/WPA2-TKIP and WPA2-AES</td>
<td>WPA/WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
</tbody>
</table>
Configuring Encryption for a WLAN that Uses Web-Auth. Web-Auth occurs after a station connects to the WLAN and, by itself, provides no encryption.

To protect the users’ data within the wireless network, you can add WEP or WPA/WPA2 encryption. In this case, users must first enter a WEP or WPA key to connect to the WLAN. Then, when they attempt to access a Web site, they must submit their username and password for Web-Auth.

See “Web-Auth” on page 4-39 or Chapter 5: “Web Authentication for Mobile Users” for instructions on configuring the authentication. After selecting Web-Auth in a WLAN’s Edit screen, you have several choices for which boxes in the Encryption section to check. Table 4-6 summarizes these options and refers you to section that explains how to configure the second security option.

**Table 4-6. Encryption Options for Web-Auth**

<table>
<thead>
<tr>
<th>Encryption Option</th>
<th>Security Option</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP 64</td>
<td>static WEP</td>
<td>“Configuring Static WEP Encryption (No Authentication)” on page 4-48</td>
</tr>
<tr>
<td>WEP 128</td>
<td>static WEP</td>
<td>“Configuring Static WEP Encryption (No Authentication)” on page 4-48</td>
</tr>
<tr>
<td>WPA/WPA2-TKIP</td>
<td>WPA/WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
<tr>
<td>WPA2-AES</td>
<td>WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
<tr>
<td>WPA/WPA2-TKIP and WPA2-AES</td>
<td>WPA/WPA2-PSK</td>
<td>“Configuring WPA/WPA2-PSK” on page 4-58</td>
</tr>
</tbody>
</table>

**Configuring Advanced WLAN Settings**

In the Advanced section of a WLAN’s Edit screen, you can establish more specialized settings for a WLAN.

This section will explain how to configure:

- control over inter-station traffic
- closed system operations
- inactivity timeouts
You will learn how to configure other advanced settings, which deal with QoS capabilities, in “Traffic Management (QoS)” on page 4-89.

Controlling Inter-Station Traffic

Often, a wireless network serves simply to connect mobile users to your Ethernet network or to the Internet. In this case, wireless stations primarily need to communicate with the Wireless Edge Services zl Module and servers in the wired network; they do not need to communicate with other wireless stations. However, by default they are allowed to do so (albeit through their RPs since infrastructure mode requires that wireless stations send all traffic to the RP).

For increased security, you can prevent two wireless stations in a particular WLAN from communicating with each other. You have three options for controlling wireless station-to-station traffic in a particular WLAN:

- allow all inter-station traffic
  When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services zl Module forwards the packet toward the second station's RP.

- drop all inter-station traffic
  When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services zl Module drops the packet.

- forward inter-station traffic through the switch
  This option allows inter-station traffic but ensures that it complies with your network policies. When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services zl Module forwards the traffic into the wired network in the VLAN configured for that WLAN (or in the user's dynamic VLAN). The wireless services-enabled switch enforces any applicable access controls and sends the packet back to the module to be forwarded to toward the second station's RP.

To enable inter-station blocking on a WLAN, complete these steps:

1. Access the Edit screen for the WLAN:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The Edit screen is displayed.
2. In the **Inter-station Traffic** drop-down menu under **Advanced**, choose how the module treats inter-station traffic:
   - Drop packets
   - Allow Packets
   - Forward through switch

   The default setting is to allow inter-station traffic.

   **Figure 4-37. Controlling Inter-Station Traffic**

3. Click the **OK** button.
Remember that this setting applies to a WLAN; it does not apply to an RP as a whole, which might associate with stations in several WLANs. If you want to prevent the Wireless Edge Services zl Module from forwarding traffic between wireless stations in different WLANs, you must configure this option for both WLANs.

**Note**
Remember to consider whether a RPs must forward traffic between devices such as Voice-over-WLAN (VoWLAN) phones.

### Enabling Closed System Operations

Wireless stations have two ways that they can discover the SSID for a WLAN:
- RPs send beacons that include the SSID for the WLAN. All wireless stations listen for beacons.
- RPs answer probes from stations requesting the RP to send all SSIDs that it supports.

RPs can only beacon the SSIDs for the four primary WLANs (with normal configuration, WLANs 1 through 4). This second option allows some wireless stations to automatically discover the SSID for the other WLANs as well.

To configure a WLAN to operate truly in closed system—that is prevent wireless stations from discovering the WLAN’s SSID—you must disable both of the functions described above.

In the past, organizations have used closed system as a rudimentary security measure. However, widely available wireless sniffer software can detect SSIDs in management frames with already associated stations. Therefore, closed system deters only the most casual of unauthorized users. For true security, enable authentication and encryption as described in “Configuring Security Options” on page 4-33.

To configure a WLAN to operate in closed system, complete these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

2. In the Advanced section, check the Closed System box.

3. Uncheck the Answer Broadcast ESS box to prevent RPs from telling wireless stations the SSID in response to probes.

4. Click the OK button.
Configuring the Inactivity Timeout

Users do not always bother to disconnect from wireless connections when they turn off or leave their stations. Although the user is no longer truly connected, the Wireless Edge Services zl Module continues to store the station’s association. On an RP nearing its maximum number of stations, an unterminated association can prevent a new station from connecting to the wireless network. The unterminated association can also be a security risk, as an unauthorized user may access the station, and through it, the authorized user’s connection.

The Wireless Edge Services zl Module forces stations that have been idle for a certain period of time to reassociate.

**Note**

Stations handle the reassociation in the background; users may not even notice the process.

The inactivity timeout, which is the time that a station can be idle before reassociating, is configured for all stations on a particular WLAN. To set this time, complete these steps:

1. Access the Edit screen for the WLAN:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The Edit screen is displayed.
Wireless Local Area Networks (WLANs)

Configuring a WLAN

Figure 4-39. Setting the Inactivity Timeout

2. Under Advanced, in the Inactivity Timeout field, enter a value from 60 seconds (one hour) through 86400 seconds (one day).

   The default timeout is 1800 seconds (30 minutes).

   In Figure 4-39, the administrator has lowered the timeout to 300 seconds (five minutes).

3. Click the OK button.

Configuring Accounting on a WLAN

The Wireless Edge Services zl Module can implement accounting on a WLAN—that is, track users’ activity and consumption of network resources. Your company might analyze logs for security auditing and traffic management. Or your company might submit the reports to a billing server in order to charge users for wireless access.
You can configure the module to use these types of accounting:

- **syslog**—The Wireless Edge Services zl Module forwards logs about stations in this WLAN to a syslog server.

- **RADIUS**—The Wireless Edge Services zl Module sends messages to a RADIUS accounting server when a station connects or disconnects and, optionally, at universally throughout the connection. The messages include information such as the station’s MAC address, the duration of the connection, and the network resources consumed.

  The RADIUS accounting server can be an external server or the Wireless Edge Services zl Module’s own internal RADIUS server. See Chapter 11: “RADIUS Server” for more information about this server.

  The WLAN on which you enable RADIUS accounting must also enforce authentication to a RADIUS server.

### Enabling Logging to a Syslog Server on a WLAN

Follow these steps to enable the Wireless Edge Services zl Module to log WLAN activity to a syslog server:

1. Select **Network Setup > WLAN Setup > Configuration**.
2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.
3. In the Advanced section, in the Accounting Mode field, use the drop-down menu to select Syslog.

4. Click the Syslog Config button. The Accounting screen is displayed.
5. In the *Syslog Server IP* field, specify the Syslog server's IP address.

6. In the *Syslog Server Port* field, enter your server's UDP port or keep the default 514.

7. Click the **OK** button.

8. In the WLAN's **Edit** screen, click the **OK** button.

9. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**Enabling RADIUS Accounting on a WLAN**

To activate RADIUS accounting on a WLAN, follow these steps:

1. Select **Network Setup > WLAN Setup > Configuration**.

2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.
3. In the Advanced section, in the Accounting Mode field, use the drop-down menu to select Radius.

   Users must authenticate to a RADIUS server for RADIUS accounting to function. Select 802.1X EAP, Web-Auth, or MAC Authentication for the authentication method.

4. Click the Radius Config button. The Radius Configuration screen is displayed.
To enforce RADIUS accounting, the WLAN must use 802.1X authentication, Web-Auth, or MAC authentication for the **Authentication** mode.

5. Configure settings for the primary accounting server in the **Primary** column of the **Accounting** section.

   a. Specify the server’s IP address in the **Accounting Server Address** field.

      To use the Wireless Edge Services zl Module’s internal server for accounting, enter 127.0.0.1.

   b. Enter your RADIUS accounting server’s port in the **Accounting Port** field.

      Typically, leave the default port: 1813.
c. In the Accounting Shared Secret field, enter a string up to 127 characters long. (The string can include alphanumeric and special characters.)

The accounting server uses the shared secret to verify that reports are from a legitimate source. The key you specify must match the key configured for the module in the accounting server’s configurations.

If you are using the module’s internal server, you don’t need to specify a key.

6. Optionally, configure settings for a secondary server by completing the fields in the Secondary column of the Accounting section.

7. Optionally, alter the value in the Accounting Timeout field.

This setting determines the length of time in seconds that the Wireless Edge Services zl Module waits for an acknowledgement from the accounting server. The default is five seconds, and the valid range is from 1 to 300 seconds. Raise the timeout if your network or accounting server is frequently busy.

8. Optionally, alter the value in the Accounting Retries field.

If the module does not receive an acknowledgement from the accounting server, it resends the report. The default number of retries is 6, and the valid range is from 1 to 100.

Re-sending reports ensures that users’ activity is logged correctly—particularly important if your company charges for wireless service.

9. From the Accounting Mode drop-down menu, choose when the Wireless Edge Services zl Module sends a report:

- Start-Stop—when a station connects to this WLAN and when it disconnects
- Stop-Only—only when a station disconnects
- Start-Interim-Stop—when a station connects to this WLAN, periodically for as long as the connection persists, and when the station closes the connection

10. If you have selected Start-Interim-Stop for the Accounting Mode, enter a value in the Interval field.

This setting determines how often, in seconds, the module sends periodic reports on user activities. (It applies only when you select Start-Interim-Stop.) The default value is 60 seconds, and the valid range is from 60 to 3600 seconds (1 hour).
11. Click the OK button.
12. In the WLAN's Edit screen, click the OK button.
13. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

Configuring Global WLAN Settings

The ProCurve Wireless Edge Services zl Module also supports these features:

- **Proxy ARP**—With this feature enabled, the Wireless Edge Services zl Module responds to ARP requests on behalf of its wireless stations, reducing overhead in the wireless network.

- **Shared-key authentication**—Open and shared-key authentication apply to WLANs that use WEP encryption.

  Open-key authentication, which is the default for all WLANs on the module, allows stations to immediately associate to the RP. (However, they still must have the correct WEP key to properly send and receive data.)

  Shared-key authentication is an obsolete form of authentication requiring stations to prove that they have the WEP key before associating to the RP. This option is not recommended because it leaks information about the key.

You enable and disable these features for all WLANs on the Wireless Edge Services zl Module.

To configure global WLAN settings, complete these steps:

1. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
2. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.
Wireless Local Area Networks (WLANs)
Configuring a WLAN

3. Check the boxes for the features that you want to enable.

**Note**
The **Advanced Configuration** selection refers to how SSIDs are assigned to RP radios; see “Advanced Mode Configuration” on page 4-11.

4. Click the **OK** button.

**Enabling the WLAN**

RPs in your wireless network will not support the WLAN until you enable it.

To enable the WLAN, complete these steps:

1. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
2. Select the WLAN that you want to enable. You can use the **<Ctrl>** key to select multiple WLANs.
3. Click the **Enable** button.

   The icon in the **Enabled** column should change from a red X to a green check mark, as shown in Figure 4-45.
Figure 4-45. Enabling a WLAN

As long as you are operating in normal mode, all radios on all RPs that the Wireless Edge Services zl Module has adopted or will adopt support the enabled WLANs.

You can confirm that RPs are actually supporting the enabled WLANs by selecting **Network Setup > Radio** and checking the **WLAN Assignment** tab. Select an RP radio to view which SSIDs are mapped to that radio’s BSSIDs.

The radio also adds the enabled WLANs to the WLAN assignment for default radio adoption configurations, which you can view by selecting **Network Setup > Radio Adoption Defaults** and clicking the **WLAN Assignment** tab.

For example, Figure 4-46 shows the default configuration after you enable the five WLANs shown in Figure 4-45.
The radio supports all five WLANs. However, some of the WLANs share a BSSID. For example, when BSS 1 is selected in the section on the left, the section on the right shows the two WLANs that share this BSSID. See Figure 4-47.
To review how the Wireless Edge Services zl Module assigns WLANs to RP radios, see “Normal Mode Configuration” on page 4-4.
VLAN Assignment

The instructions for configuring a WLAN include the basic mechanics for assigning all traffic from a WLAN to a VLAN.

This section will explain in more depth when and why you would assign one WLAN to one VLAN and another WLAN to another VLAN. You will also learn about the ability of the Wireless Edge Services zl Module to assign individual wireless users to VLANs—an ability that provides a high degree of flexibility and control at the edge of the network.

To understand the importance of the VLAN assignment, consider role of the Wireless Edge Services zl Module as the guard between the wireless and wired portions of your network. RPs encapsulate wireless traffic with Ethernet headers so wireless users can access the wired network, but the module controls this traffic so that wireless users receive the appropriate network access.

In a traditional Ethernet network, one of the primary ways in which administrators control network rights is by assigning users to various subnetworks, or VLANs. Traditionally, administrators used hardware-based rules to enforce these assignments: they plugged a user's workstation into a switch port configured to carry traffic on the appropriate VLAN. However, you cannot control mobile users in a wireless network in this way, because wireless users do not connect through a set port. Instead:

- Users may connect through different ports at different times.
- Traffic from many different users may arrive on the same port.

When you configure VLAN assignment on a Wireless Edge Services zl Module, you enable the module to take over, for wireless stations, the role of assigning users to the correct VLANs. In other words, you establish the foundation for control over mobile users’ network rights. The module acts as an intelligent door to your network, opening on the correct subnetwork for each wireless user.

You have a choice about how to treat the VLANs to which the module assigns wireless traffic. If you want your wired infrastructure devices to handle this traffic, make sure that on the wireless-services enabled switch you tag the module’s internal uplink port for these VLANs. If you want the Wireless Edge Services zl Module to route the wireless traffic into VLANs used on the wired network, you should not tag the internal uplink port for the VLANs for wireless
users. On the other hand, you might tag the port for the wired VLANs (depending on whether the module has VLAN interfaces for those VLANs or simply knows routes to them).

The Wireless Edge Services zl Module determines the VLAN to which to assign incoming wireless traffic based on one of two criteria:

- the wireless user’s identity
- the wireless station’s WLAN

You configure WLAN-based VLAN assignments manually. (See “Setting Basic Configuration Options: SSID and VLAN Interface” on page 4-30.)

Identity or user-based VLAN assignments are dynamic and received from an authentication server. This server can be either the Wireless Edge Services zl Module’s internal RADIUS server on an external RADIUS server. You must activate dynamic VLANs on a WLAN in order for the module to enforce dynamic VLAN assignments. (See “Setting Basic Configuration Options: SSID and VLAN Interface” on page 4-30.)

Note that the Wireless Edge Services zl Module can use both kinds of assignment on the same WLAN, but dynamic settings always take precedence when dynamic VLANs are enabled. For example, you manually assign WLAN 1 to VLAN 10. Users A, B, and C connect to WLAN 1; however, the RADIUS database only includes a VLAN assignment for users A and B. When user C connects to the WLAN, the module forwards its traffic in VLAN 10. When user A connects to the WLAN, the authentication server sends users’ VLAN assignment, and the module forwards user A’s traffic in VLAN 20. (See Figure 4-48.)

![Figure 4-48. WLAN Versus Identity-Based VLAN Assignment](image-url)
WLAN-Based VLAN Assignment

You configure WLAN-based VLAN assignment by manually assigning the WLAN to a VLAN.

Typically, you complete this step at the same time that you configure the SSID and security settings, as described in “Setting Basic Configuration Options: SSID and VLAN Interface” on page 4-30 and as shown in Figure 4-49.

You can quickly change the interface assignment for multiple WLANs by selecting the VLAN Assignment tab on the Network Setup > WLAN Setup screen, as shown in Figure 4-50.
Wireless Local Area Networks (WLANs)

VLAN Assignment

Figure 4-50. Network Setup > WLAN Setup > VLAN Assignment Screen

In the first two columns, the **Network Setup > WLAN Setup > VLAN Assignment** screen shows this information for each WLAN:

- **Description** (if configured)
- **SSID**

All the VLANs to which at least one WLAN has been assigned compose the subsequent columns, as shown in Figure 4-50.

The check mark indicates to which interface the WLAN has been assigned.

For example, Figure 4-50 shows the **Network Setup > WLAN Setup > VLAN Assignment** screen for a Wireless Edge Services zl Module on which five WLANs have been configured and enabled. These WLANs have been assigned to a variety of VLANs. You can change the VLAN assignment for any of the WLANs simply by checking the box in the new column. Note that because a WLAN can only be *manually* assigned to a single VLAN, the check mark in the previous column automatically disappears.
Wireless Local Area Networks (WLANs)
VLAN Assignment

See “Identity-Based, or Dynamic, VLAN Assignment” on page 4-87 for an explanation of how the Wireless Edge Services zl Module can dynamically match WLAN traffic to multiple VLANs.

Considerations for WLAN-Based VLAN Assignment

By default, all WLANs are mapped to VLAN 1. In some networks that use multiple VLANs, this VLAN is reserved for the management VLAN. Just as you might prevent a switch port from carrying traffic in VLAN 1 before connecting a user to this port, you might want to remove a WLAN from VLAN 1 and place it in a different VLAN.

In addition, just as you might create several VLANs to isolate users from each other and direct them toward the appropriate resources, you might create several WLANs and assign different VLANs to these WLANs to control wireless users’ network rights.

When determining how many WLANs to create and which VLANs to assign to these WLANs, consider these issues:

■ What type of network access will users connecting to the wireless network require?

For example, if the users need the wireless connection exclusively for Internet access, then they probably will not need to be part of any specific subnetwork. You could create a single WLAN and map that WLAN to any user VLAN in your network. Remember, however, that the wireless users will then receive the same sort of network rights as users in that VLAN, which is not ideal in many cases. It might be a better idea to create a new VLAN, such as VLAN 100, that is exclusively for wireless users; network administrators could limit traffic in that VLAN to such applications as DHCP, DNS, and HTTP.

You can then either:

• Add that VLAN to the Ethernet network—completing all necessary steps such as tagging switch ports for the VLAN and configuring a DHCP server to provide addresses in the appropriate subnetwork range.

• Terminate that VLAN on the Wireless Edge Services zl Module and configure the module to route traffic, act as a DHCP server, and perform NAT.

For more information on these options, see “Determining the Layer 3 Services Your Wireless Edge Services zl Module Should Provide” on page 1-18 of Chapter 1: “Introduction.”
Wireless Local Area Networks (WLANs)
VLAN Assignment

- Who will be connecting to this WLAN?
  - **Guests**—In this case as well, you could assign the WLAN to a VLAN reserved for wireless users. Network administrators could then control traffic from that VLAN appropriately—for example, limiting wireless users to Internet access or to certain network servers.
  
  - **Employees who will use the wireless connection exclusively**—You can use the same policies to assign new employees to a VLAN that you would use if the employees used traditional, wired connections. Then simply assign the WLAN to that VLAN.

  If you want to assign different employees to different VLANs, then you must configure a separate WLAN for each employee category and ensure that the employees connect to the correct VLAN. Dynamic VLAN assignment offers a more elegant solution and will be discussed later in “Identity-Based, or Dynamic, VLAN Assignment” on page 4-87.

  - **Employees who will use the wireless connection as well as a traditional connection**—In this case particularly, you should focus on the type of network access that the employees will require. If, for example, the employees only need to check their email and access the Internet, then you could group them all together in a WLAN and VLAN that has been configured to allow such limited access.

  If, on the other hand, the employees need access equivalent to wired connections, then you must configure the Wireless Edge Services zl Module to place each employee in the VLAN in which that employee operates in the Ethernet network. In a network with a single user VLAN, the process is straightforward enough: simply create a WLAN and assign it to that VLAN.

  However, to replicate, for wireless users, wired access to a network with multiple VLANs, you must:
  i. Determine the user VLANs to which mobile employees belong.
  ii. Create one WLAN for each user VLAN, mapping each WLAN to a different VLAN.
  iii. Configure security on each WLAN such that only the employees that should be placed in the corresponding VLAN can connect to the WLAN.

  Dynamic VLAN assignment, described in “Identity-Based, or Dynamic, VLAN Assignment” on page 4-87, greatly simplifies this process, while providing finer control.
Note

When the Wireless Edge Services zl module places traffic in a VLAN, it tags it for that VLAN. You must remember to tag the module's uplink port for each VLAN to which you manually assign a WLAN. (For more on configuring the wireless services-enabled switch, see the Wireless Edge Services zl Module Supplement to the ProCurve 6200yl/5400zl/3500yl Management and Configuration.)

Figure 4-51 illustrates how a station connects a WLAN and receives an address in the appropriate subnetwork from the network's DHCP server.

Figure 4-51. Assigning a Wireless Station to a VLAN
Wireless Local Area Networks (WLANs)
VLAN Assignment

Identity-Based, or Dynamic, VLAN Assignment

The Wireless Edge Services zl Module can also divide traffic from wireless users into VLANs based on those users’ identities. This capability (variously called user-based VLANs or identity-based VLANs, as well as dynamic VLAN assignment) allows you to:

- configure one WLAN for your wireless network with a single SSID and unified wireless security policy
- simultaneously retain granular control over the network rights of each wireless user

In order for your Wireless Edge Services zl Module to implement dynamic VLAN assignment in a WLAN, stations must authenticate to a RADIUS server. This server can be either the module’s internal server or an external network server.

You must also manually enable dynamic VLAN assignment on the WLAN.

You should not use dynamic VLANs in certain circumstances:

- You must place the WLAN in a Layer 3 mobility domain—Dynamic VLANs disable Layer 3 mobility on the WLAN. See Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility” for guidelines on when a network requires Layer 3 mobility.
- The WLAN requires Web-Auth—Dynamic VLANs are actually a possibility with Web-Auth. However, they can cause complications because the Web-Auth station receives an IP address before it authenticates. Take care to set the DHCP lease for the static VLAN very low if you allow dynamic VLAN assignment.

On the Wireless Edge Services zl Module, to enable dynamic VLAN assignment on a WLAN, complete these steps:

1. Access the Edit screen for the WLAN:
   a. Select Network Setup > WLAN Setup and click the Configuration tab.
   b. Select the WLAN and click the Edit button. The Edit screen is displayed.
2. Verify that the WLAN uses 802.1X EAP, Web-Auth, or MAC authentication.
3. Check the Dynamic Assignment box.
4. Click the OK button.
5. On the RADIUS server, configure users’ VLAN assignments.
   a. See “Creating a Group” on page 11-12 in Chapter 11: “RADIUS Server” to learn how to configure VLAN assignments on the Wireless Edge Services zl Module’s internal RADIUS server.
   b. One of the easiest ways to configure the assignment on an external server itself is via an Identity Driven Management (IDM) agent installed on the server. In this case, you would configure the assignment through ProCurve IDM and its Policy Manager. You would:
      – Configure communities that include the wireless users.
      – Create policies that match these communities to the appropriate VLANs.
      – Deploy the policies to the RADIUS server that the Wireless Edge Services zl Module uses to authenticate wireless users.

In either case, when a user connects to a WLAN and authenticates to the RADIUS server, the RADIUS server sends the VLAN assignment configured for that user’s community to the Wireless Edge Services zl Module. The module then tags all traffic from that user for that VLAN.

6. On the wireless services-enabled switch, you might need to tag the module’s uplink port for the user-based VLANs just as you might if you had configured the VLAN assignment manually. (See the Wireless Edge Services zl Module Supplement to the ProCurve 6200yl/5400zl/3500yl Management and Configuration Guide.)

**Note**

Remember that the Wireless Edge Services zl Module can receive other identity-based settings from an external RADIUS server, including:

- access control lists (ACLs)
- a rate limit on traffic from the wireless station

If you are using IDM, simply configure these settings in the IDM Policy Manager at the same time that you configure the VLAN assignment. Refer to the ProCurve Identity Driven Manager User’s Guide for more detailed instructions on how to configure identity-based settings. (You can download this guide from [http://www.procurve.com](http://www.procurve.com).)
Traffic Management (QoS)

Contemporary users demand more from wireless connections—more bandwidth and more multimedia applications—but they also demand less jitter and fewer dropped calls.

The ProCurve Wireless Edge Services zl Module helps RPs to deliver a high QoS for voice, video, and other high-priority or time-sensitive traffic.

The Wireless Edge Services zl Module and adopted RPs support protocols designed to improve QoS over the radio medium:

- SpectraLink Voice Priority (SVP)
- Wireless Multimedia (WMM)

In addition, the Wireless Edge Services zl Module can use voice prioritization to mark traffic destined to VoWLAN devices for priority handling in both the Ethernet and wireless network.

Using WLAN prioritization and weighted fair queuing (WFQ), the Wireless Edge Services zl Module queues traffic outbound to RPs according to the WLAN to which it is destined. The module allocates relatively more bandwidth to the queues for WLANs with a higher priority.

Figure 4-52 displays where these various QoS mechanisms affect traffic.
SVP

SVP maintains a high QoS specifically for VoWLAN devices that are SVP-capable. SVP is implemented in wireless phones, wireless APs, and SpectraLink servers. This IEEE 802.11-compliant mechanism minimizes latency for voice traffic by providing priority queues reserved for voice packets and by increasing the probability that all voice packets are transmitted in a predictable and timely manner.

SVP devices access the medium without waiting the default 802.11 interframe spacing (IFS) interval. In addition, SVP-enabled RPs and phones transmit voice packets in a coordinated fashion, thereby eliminating the need for a random backoff time and the attendant delays.
The Wireless Edge Services zl Module can configure RPs to support SVP—that is, to recognize SVP frames, place them in priority queues, and transmit them with a zero backoff time. If your network includes a SpectraLink server and SVP-capable phones, you should enable this support in the WLAN that includes these phones.

To enable SVP support, complete these steps:

1. Access the Edit screen for the WLAN that includes voice devices:
   a. Select Network Setup > WLAN Setup and click the Configuration tab.
   b. Select the WLAN and click the Edit button. The Edit screen is displayed.
2. Under Advanced, check the Enable SVP box.
3. Click the OK button.

**Note**

Remember that you are enabling SVP support on the WLAN, not on a particular RP. Because an RP may carry traffic for several WLANs, it might support SVP for some stations and not for others.

In other words, all ProCurve RPs can support SVP, but they actually do so only on the WLANs for which you have enabled such support.

**WMM**

A wireless network uses a shared medium (a radio). To avoid collisions, 802.11 specifies that all stations and RPs use distributed coordination function (DCF), which is similar to Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

When a wireless device wants to transmit, it selects a random backoff time and then listens for contention. After the medium has been free for an entire IFS interval (3 ms in DCF), the device counts down its backoff timer and transmits. Because all devices compete for the medium on the same footing, the QoS for time-sensitive applications can be seriously degraded.

WMM is a Wi-Fi protocol that prioritizes wireless traffic, ensuring that the most important and the most time-sensitive traffic receives a high QoS. WMM is similar to Enhanced Distributed Channel Access (EDCA), which is the prioritization method specified in the IEEE 802.11e standard.

Support for WMM is particularly important when mobile users use VoWLAN applications. It will become increasingly crucial as users demand for a wide array of applications the same quality of network access that they receive over Ethernet connections.
Prioritization with WMM

WMM improves QoS by dividing traffic into priority queues, one for each of four access categories (ACs). The higher the AC, the higher the QoS the traffic requires.

The Wireless Edge Services zl Module can use WMM to prioritize the following traffic:
- traffic sent from RP radios to wireless stations
- traffic sent from wireless stations to RP radios

**Priority Queuing and ACs.** Table 4-7 shows the ACs into which RPs and wireless stations can divide traffic.

<table>
<thead>
<tr>
<th>Queue Number</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Best Effort</td>
</tr>
<tr>
<td>3</td>
<td>Video</td>
</tr>
<tr>
<td>4</td>
<td>Voice</td>
</tr>
</tbody>
</table>

Each AC queue is defined by different parameters, which include:
- the IFS—now called the arbitration IFS number (AIFSN)
- the minimum contention window (CW Min)—the maximum value for the initial random backoff time
- the maximum contention window (CW Max)—the maximum value for the random backoff time in a network experiencing collisions
- the transmit opportunity (Transmit Ops)—the continuous time during which a device that has won control of the radio can retain control

When devices use different parameters to transmit different types of traffic, the most time-sensitive traffic can receive the QoS that it needs. For example, the queue for voice traffic uses a smaller contention window, so VoWLAN devices on average choose smaller backoff times and win control of the medium more quickly.

When you enable WMM, traffic is assigned to an AC (and WMM queue) according to its QoS mark. Table 4-8 shows how QoS marks map to ACs, by default. You can customize these mappings for traffic transmitted by RP radios. (See “Customizing How QoS Marks Map to ACs” on page 4-108.)
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Table 4-8. Priority Values for WMM ACs

<table>
<thead>
<tr>
<th>Queue Number</th>
<th>AC</th>
<th>802.1p Priority</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
<td>1, 2</td>
<td>8-23</td>
</tr>
<tr>
<td>2</td>
<td>Best Effort</td>
<td>0, 3</td>
<td>0-7, 24-31</td>
</tr>
<tr>
<td>3</td>
<td>Video</td>
<td>4, 5</td>
<td>32-47</td>
</tr>
<tr>
<td>4</td>
<td>Voice</td>
<td>6, 7</td>
<td>48-63</td>
</tr>
</tbody>
</table>

By default, the module uses 802.1p priority to place traffic in a queue. You can choose DSCP instead; see “Customizing Station WMM Parameters” on page 4-102.

Priority Queuing on Traffic Transmitted from RPs to Wireless Stations. Remember that all traffic on a radio shares the same medium. So an RP radio may queue traffic for multiple WLANs together. By default, RPs queue traffic according to the classification of the WLAN to which it belongs. Because, by default, this classification is normal for all WLANs, all traffic receives the same handling.

One way to configure RPs to prioritize the traffic they transmit is to assign different classifications to traffic in different WLANs. See “Manually Classifying a WLAN’s Traffic” on page 4-111.

For more precise prioritization, you can enable WMM on a WLAN. WMM allows RPs to queue traffic destined the WLAN according to each frame’s QoS mark. In other words, the RP uses an 802.1p or DSCP value to assign traffic to an AC. The RP creates one queue for each AC on each of its radios. The radio then transmits traffic in that queue using the RP WMM parameters (such as AIFS) for that AC. (For more information about the RP WMM parameters for wired to wireless traffic, see “Viewing and Customizing RP WMM Parameters” on page 4-105.)

In this way, traffic with a higher priority receives more bandwidth, as shown in Figure 4-53. The RP radio continues to provide all wired to wireless traffic belonging to non-WMM WLANs with normal QoS.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

![Diagram showing WMM prioritization](image)

Figure 4-53. Using WMM to Prioritize Traffic Transmitted from RPs to Wireless Stations

**Priority Queuing on Traffic Transmitted from Wireless Stations to RPs.** Only when you enable WMM on a WLAN, WMM-enabled stations also implement priority queuing on traffic they transmit.

RPs broadcast station WMM parameters throughout the WLAN. WMM-enabled stations queue traffic according to 802.1p or DSCP value, using the WMM parameters to determine how to handle traffic in each queue. (Non-WMM stations continue to handle all traffic normally.) Figure 4-54 illustrates the affect of WMM on wireless station to RP traffic.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Figure 4-54. Using WMM to Prioritize Traffic Transmitted From Wireless Stations to RPs

Note that the station WMM parameters can differ from the RP WMM parameters.

Enabling WMM on a WLAN

Enabling WMM on a WLAN, enables the following:

- RP radios use QoS marks (802.1p, by default) to queue traffic destined to stations in this WLAN
  Radios grant better QoS to high priority queues by using different parameters to transmit traffic in those queues.
- WMM-enabled stations in the WLAN use QoS marks to queue traffic destined to their RPs
  Adopted RP radios broadcast WMM parameters for the four ACs. Wireless stations that are WMM-enabled queue and transmit traffic accordingly. Non-WMM-enabled stations continue to use standard settings for all traffic, which match those for the Best Effort AC (queue 1).

To enable WMM prioritization, complete these steps:

1. Access the Edit screen for the WLAN that includes voice devices:
   a. Select Network Setup > WLAN Setup and click the Configuration tab.
   b. Select the WLAN and click the Edit button. The Edit screen is displayed.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Figure 4-55. Enabling WMM on a WLAN

2. Under **Advanced**, in the **Access Category** drop-down menu, select **Automatic/WMM**.

3. Click the **OK** button.

The next section explains how to make some advanced configurations for WMM.
Changing the Protocol that Prioritizes Traffic and Enabling Admission Control

As discussed earlier, when you enable WMM, wireless devices queue frames according to QoS marks. The default protocol for the QoS mark is 802.1p. However, you can change the protocol to DSCP by accessing advanced WMM parameters.

Another advanced WMM parameter is admission control, a feature available for Video and Voice queues. The more stations that use high priority settings, the less effect those settings have. Admission control restricts the number of stations in a wireless cell that can use the high priority settings by forcing stations to check with the RP first.

To configure these advanced options, follow these steps:

1. Select **Network Setup > WLAN Setup** and click the **WMM** tab.

   As you can see in Figure 4-56, the WMM enabled column displays the WLANs for which you have set the **Access Category** to **Automatic/WMM**.
2. Select the queue for which you want to alter the settings, and then click the **Edit** button. The **Edit WMM** screen is displayed.

---

**Figure 4-56. Station EDCA (WMM) Parameters**
3. Select the prioritization protocol used by your wireless stations:
   - 802.1p is a Layer 2 protocol that marks traffic in the VLAN tag for one of eight priorities.
   - DSCP is a Layer 3 protocol that marks traffic in the IP header for one of 64 priorities.

Wireless devices queue frames according to the priority marked by the selected protocol. For example, if you select 802.1p, a wireless device transmits a frame with priority value of 5 in its VLAN tag, using the parameters for the Video AC. A frame with a DSCP value in the IP header, but no 802.1p value, is transmitted according to the Best Effort AC.

Refer to Table 4-8 on page 4-93 to review to which ACs various priority values map. See “Customizing How QoS Marks Map to ACs” on page 4-108 to change which values map to which ACs.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

**Note**

If you change the protocol for one queue, the setting automatically changes in the other three queues for the WLAN; in other words, the setting applies to the WLAN as a whole. (It does not make sense to use 802.1p to queue some traffic, but queue other traffic according to DSCP.)

4. To restrict the number of stations allowed to use the settings for this queue, check the Admission Control box and enter a value from 1 to 255.
   
   This option is only available for the Voice and Video ACs.

5. Click the **OK** button.

**Viewing Station WMM Parameters**

From the **Network Setup > WLAN Setup > WMM**, you can also view the station WMM parameters, which determine how WMM-enabled stations in a WMM-enabled WLAN handle traffic placed in various ACs.
Wireless Local Area Networks (WLANs)  
Traffic Management (QoS)

Figure 4-58. Station WMM Parameters

Figure 4-58 shows the default settings for WMM queues. As you can see, each WLAN has its own four queues. This is because RPs broadcast one set of station parameters to all stations in a WLAN. They can broadcast another set of station parameters to all stations in another WLAN (if that WLAN uses WMM).

TheIdxcolumn lists the WLAN and the queue number. For example, the first row displays the settings for queue 1 on WLAN 1. To see the AC for this queue, look at theAccesscolumn. For example, queue 1 is the Background queue.

TheSSIDandDescriptioncolumns further identify the WLAN in question.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

A green check mark in the **WLAN Enabled** column indicates that RPs in your network currently support this WLAN; a green check mark in the **WMM Enabled** column indicates that RPs are allowed to send the WMM parameters to stations (*Access Category* is **Automatic/WMM**.) In Figure 4-58, four WLANs are active and enabled. However, only two (MyWLAN and Test) implement WMM prioritization on wireless station to RP traffic.

The final four columns list the station WMM parameters for the queue in this row. The default settings grant lower latency for the queues with higher numbers.

Typically, no further configuration is necessary. You only need to know that by accepting these settings from the RPs, wireless stations can improve QoS for certain types of traffic.

For example, if a wireless station is transmitting a voice frame, the station will compete for the radio using the advantageous settings that the RP has specified for such frames. However, the station must meet these requirements for the prioritization to take effect:
- The station must support WMM.
- The traffic must be marked by an application on the wireless station for the higher AC.

**Customizing Station WMM Parameters**

If you have a great deal of experience working with WMM and other QoS protocols, you can customize the queue settings to the needs of your environment.

**Note**

Because the Wireless Edge Services zl Module automatically defines settings such that traffic in a higher-priority queue receives lower latency, the default station WMM parameters settings are usually adequate. Also, because incorrect settings can adversely affect network performance, ProCurve Networking generally recommends that you do **not** change these parameters.

To customize station WMM parameters, complete these steps:

1. Select **Network Setup > WLAN Setup** and click the **WMM** tab.
Figure 4-59. Station WMM Parameters

2. Select the queue for which you want to alter the settings, and then click the Edit button. The Edit WMM screen is displayed.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Figure 4-60. Editing Station EDCA (WMM) Parameters

3. View the SSID and Access Category settings to verify that you are configuring the correct queue. In Figure 4-60, the Best Effort queue (queue 1) in MyWLAN is being customized.

4. Enter the desired values in the AIFSN, Transmit Ops, CW Minimum, and CW Maximum fields.

The values for the AIFSN and Transmit Ops are in ms. The CW Min and CW Max values are determined by raising 2 to the power of the value in the corresponding field and subtracting one. For example, if you enter 4 in the CW Minimum field, the CW Min value is 15. (Setting the CW Min and CW Max values in this way forces you to specify values allowed by WMM.)
Again, take great care in establishing these settings. ProCurve Networking cannot guarantee any behavior. However, you can keep these tips in mind:

- The lower the AIFSN and the CW minimum values, the lower the latency for traffic in the queue, and in a congested network, the higher the throughput. In a congested network, raising the AIFSN or the CW minimum of low-priority queues can improve QoS for high-priority. Raising the AIFSN value a certain amount sometimes has a more dramatic effect than raising the CW value the same amount. However, raising either value too high can starve out low-priority traffic.
- By default, high-priority queues on the RP use an AIFSN value of 1 ms; high-priority queues on stations use an AIFSN value of 2 ms. You might want to reserve the 1-ms AIFSN for RPs.
- When you grant a queue a Transmit Ops, you allow a station that wins access to the radio continued access to the medium for that length of time. If you set this value excessively high, then lower-priority traffic, and even other high-priority traffic, may be unacceptably delayed. Although the Web browser interface lists the maximum value as 65,535, generally the Transmit Ops is set in terms of tens, or at the most, hundreds of milliseconds—not thousands. In several seconds, applications can time out, frustrating users throughout your network.
- In a network with many users and high congestion, increasing CW Maximum values can decrease the number of collisions.
- The CW Maximum value must always be higher than the CW Minimum value.

**Viewing and Customizing RP WMM Parameters**

As discussed earlier, RPs handle traffic as dictated by the WMM parameters (AIFSN and so forth) for the traffic's AC. Also as discussed earlier, the Wireless Edge Services zl Module assigns traffic to an AC according to the WLAN setting or, if the AC is set to automatic/WMM, according to priority value.

The ProCurve 210, 220, and 230 RPs use default parameters that work for nearly all applications. (For example, the parameters are such that voice frames more quickly and more often win access to the medium.)

**Note**

Because the Wireless Edge Services zl Module automatically defines settings such that traffic in a higher-priority queue receives lower latency, the default radio WMM settings are usually adequate. Incorrect settings can adversely affect network performance; ProCurve Networking strongly recommends that you do not change these parameters.
Like other radio settings, you can alter:

■ the WMM queue parameters that the Wireless Edge Services zl Module sends to newly adopted radios
■ the WMM queue parameters used by particular radios

To customize the RP WMM parameters, complete these steps:

1. Choose whether you are configuring parameters for any newly adopted radio or for a particular radio:
   • To configure settings for any newly adopted radio, select **Network Setup > Radio Adoption Defaults**.
   • To configure settings for particular radios, select **Network Setup > Radio**.

2. Click the **WMM** tab. On the screen that is displayed (see Figure 4-62), queues are listed depending on the configuration type:
   • For the radio adoption default configurations, queues are listed on the screen by radio type and access category—for example, **802.11a** and **Background**.
   • If you are configuring WMM settings for particular radios, queues are indexed according to radio number and queue number. For example, in Figure 4-62, the **Voice** queue for radio 1 would be indexed 1/4.
To change the parameters for a particular queue, select the queue and click the **Edit** button. The **Edit WMM** screen is displayed.

![Network Setup > Radio > WMM Screen](image)
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

4. To change the AIFSN value, enter a new value between 0 and 15 in the **AIFSN** field. This value is in ms.

5. To change the Transmit Ops value, enter a new value between 0 and 65,535 in the **Transmit Ops** field. This value is in ms.

6. To change the CW Min, enter a new value between 0 and 15 in the **CW Minimum** field. The CW Min is 2 to the power of this value, minus 1, in ms. For example, if you enter 3, then the CW Min is 7 ms.

7. To change the CW Max, enter a new value between 0 and 15 in the **CW Maximum** field. The CW Max is 2 to the power of this value, minus 1, in ms.

8. Click the **OK** button.

Customizing How QoS Marks Map to ACs

As discussed earlier, enabling WMM on a WLAN allows wireless devices to queue traffic according to either an 802.1p or DSCP. Table 4-9 shows the default mapping of values to priority queues.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Table 4-9. Priority Values for WMM ACs

<table>
<thead>
<tr>
<th>Queue Number</th>
<th>AC</th>
<th>802.1p Priority</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
<td>1, 2</td>
<td>8-23</td>
</tr>
<tr>
<td>2</td>
<td>Best effort</td>
<td>0, 3</td>
<td>0-7, 24-31</td>
</tr>
<tr>
<td>3</td>
<td>Video</td>
<td>4, 5</td>
<td>32-47</td>
</tr>
<tr>
<td>4</td>
<td>Voice</td>
<td>6, 7</td>
<td>48-63</td>
</tr>
</tbody>
</table>

The mapping of priority value to AC occurs as traffic is prepared for transmission in a WLAN. For traffic traveling the opposite direction—from the WLAN to the Ethernet—the Wireless Edge Services zl Module reverses the operation, marking traffic that arrives in a particular AC with a priority value.

You can change the mapping to customize your network’s queues. Follow these steps:
1. Select Network Setup > WLAN Setup and click the WMM tab.
2. Click the QoS Mappings button. The QoS Mappings screen is displayed.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Figure 4-63. Customizing QoS Mappings

3. Use the **Access Category to 802.1p** section to configure the Wireless Edge Services zl Module, to mark incoming wireless traffic with a QoS value for priority handling in the wired network.

   Click a field in the **802.1p Prioritization** column. Then enter a value between 0 and 7. The module marks traffic that arrives in this AC with this 802.1p value.

4. If you are using 802.1p to prioritize traffic in at least one WLAN, configure the QoS mappings in the **802.1p to Access Category** section.

   To select the AC to which a particular 802.1p value maps, click the **Access Category** column in the row for that value. Then choose **Best Effort**, **Background**, **Video**, or **Voice** from the drop-down menu.
5. If you are using DSCP to prioritize traffic in at least one WLAN, configure the QoS mappings in the **DSCP to Access Category** section.

   To select the AC to which a particular DSCP maps, click the **Access Category** column in the row for that value. Then choose **Best Effort**, **Background**, **Video**, or **Voice** from the drop-down menu.

6. Click the **OK** button.

**Manually Classifying a WLAN’s Traffic**

By default, the Wireless Edge Services Zl Module and RPs treat traffic destined to stations in any WLAN equally. However, you can manually assign all traffic in a particular WLAN to a specific AC. Traffic then receives QoS according to the relative priority of that AC. For example, you could configure a WLAN for traditional data traffic and a WLAN for voice traffic. To prioritize traffic sent to the voice wireless devices, you would manually set the entire voice WLAN to the Voice AC.

**Note**

With WMM, RPs automatically prioritize different types of traffic. Enabling WMM on a WLAN also allows WMM-capable stations to prioritize traffic automatically according to QoS values. See “WMM” on page 4-91 and “Enabling WMM on a WLAN” on page 4-95.

To set a WLAN’s AC manually, follow these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

![WLAN Setup screenshot](image)

**Figure 4-64. Setting a WLAN's AC**

2. Choose the name of an AC from the **Access Category** drop-down menu in the **Advanced** section.

By default, RPs handle traffic as follows, from traffic that receives the highest priority to traffic that receives the lowest:

- **Voice**
- **Video**
- **Normal**
- **Low**
Enabling Prioritization of Voice Traffic

Voice prioritization improves the QoS for traffic destined to VoWLAN devices. The Wireless Edge Services zl Module configures RPs to monitor all packets from stations in a WLAN; if the IP type in a packet's header indicates that it is a voice packet, the module marks all traffic destined to the packet's source as high-priority voice packets.

Traffic destined to the VoWLAN device thus receives priority handling both in the Ethernet network (from the wireless services-enabled switch to the RP) and in the wireless network (from the RP to the VoWLAN device). The wireless services-enabled switch forwards the traffic in its high-priority queue, and the RP uses its Voice queue settings.

Voice prioritization thus helps to maintain QoS for VoWLAN devices that do not support WMM on their own.

To enable the Wireless Edge Services zl Module to prioritize traffic to voice stations in a particular WLAN, complete these steps:

1. Access the **Edit** screen for the WLAN that includes voice devices:
   a. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
2. Under **Advanced**, check the **Use Voice Prioritization** box.
3. Click the **OK** button.

Specifying Multicast Addresses for Voice Traffic

VoWLAN devices often send and listen for traffic on a specific multicast address. When you specify this address in a WLAN's settings, the Wireless Edge Services zl Module prioritizes this traffic.

To specify multicast addresses for voice traffic, complete these steps:

1. Select **Network Setup > WLAN Setup** and click the **Configuration** tab.
2. Select the WLAN that includes voice devices, and then click the **Edit** button. The **Edit** screen is displayed.
Wireless Local Area Networks (WLANs)
Traffic Management (QoS)

Figure 4-65. Setting the Multicast Address

3. Under Advanced, in the MCast Addr 1 field, enter the address for voice traffic.
4. If you want, enter a second address in the MCast Addr 2 field.
5. Click the OK button.
Web Authentication for Mobile Users

Contents

Overview ................................................................. 5-2
The Web-Auth Process ........................................... 5-3
Authentication Through a RADIUS Server ............... 5-5
Web Pages for the Login Process .............................. 5-6
Allow List ............................................................... 5-8
Creating a VLAN Interface for the Web-Auth VLAN 5-9
Configuring Web-Auth ............................................. 5-10
Configuring Basic Options and Accessing the Web-Auth Screen ... 5-11
Configuring Internal Web-Auth Pages ..................... 5-16
Configuring Web-Auth to an External Web Server ........ 5-24
Loading Custom Pages onto the Wireless Edge Services
z1 Module's Internal Server (Advanced) .................. 5-26
Configuring the Allow List ..................................... 5-28
Configuring Encryption for a Web-Auth WLAN ........ 5-30
Copying Logo Files to the Module's Flash ................. 5-33
Configuring Custom Web-Auth Pages ..................... 5-36
Configuring the CGI Commands for the Login Page .... 5-36
Configuring the CGI Commands for the Welcome Page ... 5-38
Overview

With the ProCurve Wireless Edge Services zl Module, you can require mobile users to authenticate by entering their login credentials on a Web page. Like other authentication methods, Web authentication (Web-Auth) is verified through a Remote Access Dial In User Service (RADIUS) server.

You can use Web-Auth to provide limited network services for mobile users who visit your company's office. For example, you might want to provide Internet access so that these users can browse the World Wide Web or establish a virtual private network (VPN) to their company's network. Through the security provided over a VPN, users can access the applications (such as email) and the data that they need to do their jobs.

In addition to using Web-Auth to provide network services for visitors, you can use Web-Auth to provide authenticated access for employees who are using stations that do not support 802.1X. Because Web-Auth is easy to configure and provides an easy access method for users, you may also want to use this authentication method for employees who need limited network services.

Note

With Web-Auth, mobile users roam seamlessly between RPs adopted by the same Wireless Edges Services zl Module. To have stations roam at Layer 2 between RPs adopted by different modules, you must place the modules in a redundancy group. (See Chapter 10: “Redundancy Groups.”) To have stations roam between modules at Layer 3, you must place the modules in a Layer 3 mobility domain. (See Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility.”)

However, the redundancy group, like the module, is limited to adopting 48 RPs. Consider having a single module adopt all RPs. (You can install RPs in a different subnetwork than the Wireless Edge Services zl Module that adopts them. See “Network Requirements for Layer 3 Adoption” on page 2-62 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)
Web Authentication for Mobile Users

Overview

The Web-Auth Process

To provide limited network access to mobile users through Web-Auth, you set up a Dynamic Host Configuration Protocol (DHCP) server and instruct the users to configure their stations to receive a dynamic IP address from this server. (This DHCP server can be an external server or the Wireless Edge Services zl Module's internal server.) When a mobile user tries to associate with a wireless LAN (WLAN) that is configured for Web-Auth, the user's station requests an IP address from the DHCP server. (See Figure 5-1.)

![Figure 5-1. The Station Receives an IP Address from a DHCP Server](image)
Web Authentication for Mobile Users

Overview

After a station successfully receives an IP address and associates with the WLAN, the station enters the Web-Auth state. (See Figure 5-2.) In this state, the station can access only the network devices that you have added to the Web-Auth Allow list. This list includes the IP address of any device that you want unauthenticated users to be able to access. (When you add the IP address of a device to the Allow list, that device is publicly available: it can be accessed by any user. For more information, see “Allow List” on page 5-8.)

Associating with the WLAN is the first step. A mobile user must then open a Web browser and attempt to access a valid URL that can be reached through your company’s network. The Wireless Edge Services zl Module intercepts this request and redirects the user’s Web browser to the Web-Auth login page, which prompts the user to enter a username and password.

When the user enters a username and password, the Wireless Edge Services zl Module submits these login credentials to the RADIUS server. If the RADIUS server verifies the user’s login credentials, the login attempt is successful, and the module displays the Web-Auth welcome page. At this point, the user’s station enters the authentication state, and the mobile user can access the network resources to which he or she has rights. (You can control access to network resources through the RADIUS server or through ProCurve Identity Driven Management [IDM]. For information about ProCurve IDM, visit the ProCurve Networking Web site at http://www.procurve.com.)

In addition to reporting that the login was successful, the Web-Auth welcome page includes a Disconnect link. When the user no longer needs to access your company’s network services, he or she can click this link to end the session. (The Disconnect link is provided for the user’s convenience. The user does not need to keep the Web-Auth welcome page open or use this link to disconnect from your network services.)

If the user enters an invalid username and password, the RADIUS server denies access, and the Wireless Edge Services zl Module displays the Web-Auth failed page. In this case, the user’s station remains in the unauthenticated state, and the user can access only the devices that you have added to the Allow list.
Web Authentication for Mobile Users

Overview

Figure 5-2. The Web-Auth Process

Authentication Through a RADIUS Server

To allow mobile users to access the Internet and selected services on your company's network, you configure Web-Auth as the authentication method for a WLAN and define a RADIUS server that verifies each user's login credentials. You can specify both a primary RADIUS server and a secondary RADIUS server, ensuring high availability. If the primary RADIUS server is unavailable, the Wireless Edge Services zl Module contacts the secondary RADIUS server.

The Wireless Edge Services zl Module provides an internal RADIUS server, which you can use for Web-Auth. See Chapter 11: “RADIUS Server” for more information.
Web Pages for the Login Process

To enable authentication through the Web, the Wireless Edge Services z1 Module provides three default Web pages that guide users through the login process:

- **Login page**—When users associate with a WLAN that is configured for Web-Auth and try to access a valid Web site, their Web browser is redirected to the login page, and they are prompted to enter a username and password. (See Figure 5-3.)

```
Network Login

Please enter your username and password

Username
Password

Login

Contact the network administrator if you do not have an account
```

Figure 5-3. Default Login Page

- **Welcome page**—If users enter a valid username and password, a welcome page is displayed, reporting that the login attempt was successful. The welcome page also provides a link that users can click to disconnect from the network services that your company provides through the Wireless Edge Services z1 Module. (See Figure 5-4.)
Web Authentication for Mobile Users
Overview

Authentication Success.

You now have network access.
Click the disconnect link below to end this session.

Disconnect

Time Elapsed:
5 seconds

Figure 5-4. Default Welcome Page

■ Failed page—If users do not enter a valid username and password on the login page, the failed page is displayed. This page includes a link back to the Login screen. (See Figure 5-5.)

Authentication Failed.

Either the username and password are invalid, or service is unavailable at this time

Try Again

Contact the network administrator if you do not have an account

Figure 5-5. Default Failed Page

You can use the default Web pages as they are, or you can modify them for your environment. You can change the text that displays and add your organization's logo.
Web Authentication for Mobile Users

Overview

Table 5-1 shows the location of these pages in the Wireless Edge Services zl Module’s file system. When you enable Web-Auth and choose to use these pages, the OS copies them to a directory for that WLAN. For example, if you use Web-Auth on WLAN 1, the login page is saved as flash:/hotspot/wlan1/login.html. In Table 5-1, X indicates the WLAN’s index number.

Table 5-1. Internal Web-Auth Pages

<table>
<thead>
<tr>
<th>Web Page Name</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Web page to which unauthenticated users are redirected in order to log in</td>
<td>flash:/hotspot/wlanX/login.html</td>
</tr>
<tr>
<td>Welcome</td>
<td>Web page that users see after they successfully authenticate</td>
<td>flash:/hotspot/wlanX/welcome.html</td>
</tr>
<tr>
<td>Failed</td>
<td>Web page that users see if they fail authentication</td>
<td>flash:/hotspot/wlanX/fail.html</td>
</tr>
</tbody>
</table>

Note

When you configure Web-Auth, make sure that your Wireless Edge Services zl Module’s flash memory has sufficient space to store the Web pages.

If you prefer, you can create your own Web pages and use them instead of the default pages. You can store these pages:

- on an external server, such as your company’s Web server
- in the Wireless Edge Services zl Module’s flash memory (advanced configuration)

When you build these Web pages, you must include certain Common Gateway Interface (CGI) commands:

- code that returns the necessary login credentials to the module
- code that issues the disconnect command to the module

See “Configuring Custom Web-Auth Pages” on page 5-36 for instructions on programming the CGI code.

Allow List

When a user associates with a WLAN that is configured for Web-Auth, the user’s station cannot, by default, access any device until the user authenticates to the RADIUS server. When you add a device’s IP address to the Allow list, that device is available to any user. Only allow devices that offer services that should be available to anyone who comes within range of your RPs at anytime.
The Wireless Edge Services zl Module automatically permits certain station traffic, even when the destination is not on the Allow list:

- **DHCP requests**—The station must receive an IP address before it can access the Web login page and authenticate.

- **Domain Name System (DNS) requests**—The station must attempt to reach a valid IP address in order for the Wireless Edge Services zl Module to redirect the browser to the login page. The DNS requests allows the station’s Web browser to resolve a Web site URL to a valid IP address.

So you do not need to add the IP addresses of your DHCP and DNS servers to the allow list.

The only necessary IP address on the Allow list is that of the Web server—when you store the Web-Auth login, welcome, and failed pages on an external Web server. On the other hand, if these pages are stored on the Wireless Edge Services zl Module, you do not have to add the module’s IP address to the Allow list. In fact, to protect management access to the module, you should not.

You can add a maximum of 10 IP addresses to the Allow list.

### Creating a VLAN Interface for the Web-Auth VLAN

The Wireless Edge Services zl Module requires an IP address on the static VLAN to which the Web-Auth WLAN maps. See Chapter 6: “IP Services—IP Settings, DHCP, and DNS” for information on creating the VLAN interface and assigning it an IP address.

You can apply access control lists (ACLs) to the VLAN interface in order to continue to control traffic from the wireless stations, even after they authenticate. You can also apply dynamic Network Address Translation (NAT) to traffic from wireless users, protecting the IP addresses used in your private network. (See Chapter 7: “Access Control Lists (ACLs)” and Chapter 8: “Configuring Network Address Translation (NAT).”)

You can also, if you so desire, have the module place users in dynamic VLANs after they authenticate. With Web-Auth, however, stations initially receive IP addresses in the static VLAN. To allow stations to receive IP addresses in the dynamic VLAN after users authenticate, set the lease time in the DHCP configuration for the static VLAN very low.
The Wireless Edge Services zl Module automatically allows unauthenticated stations access to the IP address on the static VLAN for the Web-Auth WLAN. (Such access is necessary for the stations to complete Web-Auth.) Even though management access to the module is protected by a password, you might want to protect such access further. Make sure to assign the Web-Auth WLAN to a different VLAN than the module’s management VLAN. Then activate secure management. See “Viewing VLAN Interfaces and Enabling Secure Management” on page 6-4 of Chapter 6: “IP Services—IP Settings, DHCP, and DNS.”

Configuring Web-Auth

To configure a WLAN, you must set the service set identifier (SSID) and the VLAN in which traffic will be forwarded. Typically, you will want the SSID for the Web-Auth WLAN to be broadcast (beaconed), so you must configure WLAN 1, 2, 3, or 4 to use Web-Auth. For more information about SSIDs and WLANs, including which SSIDs are broadcast by the Wireless Edge Services zl Module, see Chapter 4: “Wireless Local Area Networks (WLANs).”

By default, the Wireless Edge Services zl Module places all wireless traffic in VLAN 1. If your network has only one subnetwork, this configuration may be adequate. Often, however, you will want to use a separate VLAN for the Web-Auth WLAN. If so, you must assign this VLAN an IP address. See Chapter 6: “IP Services—IP Settings, DHCP, and DNS.”

You must also set the security options, which specify the authentication method and the encryption standard for the WLAN. In this case, you will select Web-Auth as the authentication method. See “Configuring Encryption for a Web-Auth WLAN” on page 5-30 to learn about encryption options.

In addition to configuring these settings, you can configure advanced settings for individual WLANs, which include inter-station blocking, closed system operations, and inactivity timeouts. You can also configure settings for all WLANs. For more information about configuring these additional settings, see Chapter 4: “Wireless Local Area Networks (WLANs).”
Configuring Basic Options and Accessing the Web-Auth Screen

To configure a WLAN to use Web-Auth, complete these steps:

1. Select **Network Setup > WLAN Setup > Configuration**.

---

**Network Setup > WLAN Setup**

<table>
<thead>
<tr>
<th>Index</th>
<th>Enabled</th>
<th>SSID</th>
<th>Description</th>
<th>VLAN / Tunnel</th>
<th>Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x</td>
<td>SSID 1</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>x</td>
<td>SSID 2</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>x</td>
<td>SSID 3</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>x</td>
<td>SSID 4</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>5</td>
<td>x</td>
<td>SSID 5</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>6</td>
<td>x</td>
<td>SSID 6</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>7</td>
<td>x</td>
<td>SSID 7</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>8</td>
<td>x</td>
<td>SSID 8</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>9</td>
<td>x</td>
<td>SSID 9</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>x</td>
<td>SSID 10</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>11</td>
<td>x</td>
<td>SSID 11</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>12</td>
<td>x</td>
<td>SSID 12</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>13</td>
<td>x</td>
<td>SSID 13</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>14</td>
<td>x</td>
<td>SSID 14</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>15</td>
<td>x</td>
<td>SSID 15</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>16</td>
<td>x</td>
<td>SSID 16</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>17</td>
<td>x</td>
<td>SSID 17</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>18</td>
<td>x</td>
<td>SSID 18</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>19</td>
<td>x</td>
<td>SSID 19</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>20</td>
<td>x</td>
<td>SSID 20</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>21</td>
<td>x</td>
<td>SSID 21</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>22</td>
<td>x</td>
<td>SSID 22</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>23</td>
<td>x</td>
<td>SSID 23</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>24</td>
<td>x</td>
<td>SSID 24</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>25</td>
<td>x</td>
<td>SSID 25</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>26</td>
<td>x</td>
<td>SSID 26</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>27</td>
<td>x</td>
<td>SSID 27</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>28</td>
<td>x</td>
<td>SSID 28</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>29</td>
<td>x</td>
<td>SSID 29</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>30</td>
<td>x</td>
<td>SSID 30</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>31</td>
<td>x</td>
<td>SSID 31</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>32</td>
<td>x</td>
<td>SSID 32</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Filtering is disabled

---

Figure 5-6. Network Setup > WLAN Setup > Configuration Screen
2. Select the WLAN that you want to use Web-Auth, and then click the **Edit** button. The **Edit** screen is displayed.

![WLAN Edit Screen](image)

**Figure 5-7. WLAN Edit Screen**

3. Under **Configuration**, enter an SSID for this WLAN in the **SSID** field.

4. In the **Description** field, you can enter information that will help you identify this WLAN. This field is optional.

5. By default, the Wireless Edge Services zl Module places all wireless traffic in VLAN 1. If you want to assign this WLAN to a different VLAN, enter the number in the **VLAN ID** field.

   Make sure that either your module or another infrastructure device is configured to assign wireless stations DHCP addresses in this VLAN.
5. Under **Authentication**, select **Web-Auth**.
6. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.

![Radius Configuration Screen](image)

**Figure 5-8. Radius Configuration Screen**

---

**Note**

For more information about configuring SSIDs, VLANs, and advanced configuration options, such as interstation blocking and voice prioritization, see Chapter 4: “Wireless Local Area Networks (WLANs).”
8. In the fields in the **Server** area, define the primary RADIUS server under the **Primary** heading.
   a. In the **RADIUS Server Address** field, enter the IP address of the RADIUS server that authenticates users.
      Enter 127.0.0.1 if you are using the Wireless Edge Services zl Module’s internal RADIUS server.
   b. In the **RADIUS Port** field, leave the port number at the default value (1812) unless your RADIUS server uses a different port.
   c. In the **RADIUS Shared Secret** field, enter the shared secret that the RADIUS server uses to identify the Wireless Edge Services zl Module as a valid RADIUS client (or network access server [NAS]).
      You do not need to set the secret if you are using the module’s internal RADIUS server. (If you have previously set the secret, clear the field.)
9. If you have a backup RADIUS server, repeat step 8 in the fields under the **Secondary** heading.
10. In the **Server Timeout** field, enter a timeout value in seconds.
    This setting determines how long the module waits for a reply from the RADIUS server. The default setting is 5 seconds.
11. In the **Server Retries** field, enter the number of times that the Wireless Edge Services zl Module should re-attempt to contact the RADIUS server.
    The default setting is 3, which means that the module attempts to contact the server up to four times.
12. In the **Advanced** section, choose the authentication protocol that the Wireless Edge Services zl Module uses to forward the username and password to the RADIUS server.
    You can choose **PAP** or **CHAP**. Match the setting allowed in the RADIUS server's policy. The module's internal RADIUS server supports both protocols. However, if you choose PAP, users' passwords display in plaintext in logs. Generally, you should choose CHAP for higher security.
13. Click the **OK** button to apply the settings and close the screen.
14. On the WLAN **Edit** screen, under **Authentication**, click the **Config** button next to **Web-Auth**. The **Web-Auth** screen is displayed.
15. Select the location for the Web-Auth Web pages from the drop-down menu at the top of the screen.

You can select one of three options for these Web pages:

- **Internal**—three default pages stored on the Wireless Edge Services zl Module
- **External**—three pages stored on an external Web server
- **Advanced**—pages that you have loaded onto the Wireless Edge Services zl Module's flash memory

16. Configure the Web pages as described in the following sections:

- “Configuring Internal Web-Auth Pages” on page 5-16
- “Configuring Web-Auth to an External Web Server” on page 5-24
- “Loading Custom Pages onto the Wireless Edge Services zl Module's Internal Server (Advanced)” on page 5-26
Configuring Internal Web-Auth Pages

At its factory default settings, the Wireless Edge Services zl Module includes three pages for Web-Auth. See “Web Pages for the Login Process” on page 5-6 for descriptions and illustrations of these default pages.

You can customize the text and add your company’s logo to the default pages.

Follow these steps:

1. Complete the steps described in “Configuring Web-Auth” on page 5-10.
2. You should be in the Web-Auth screen for the WLAN. Select Internal from the drop-down menu at the top of the screen.
3. Under Internal (Generated) Web Page, click the Login tab to configure the login page, which users see when they try to access your network services. (See Figure 5-9.)
   a. In the Title Text field, accept the default text shown on the screen, or enter the text that you want to use.
   b. In the Header Text field, accept the default text shown on the screen, or enter the text that you want to be displayed at the top of the login page. (See Figure 5-10.)

**Note**

If you customize the Header Text, Footer Text, or Descriptive Text fields, you can enter a maximum of 1,024 characters.

- In the Footer Text field, accept the default text shown on the screen, or enter the text that you want to be displayed at the bottom of the login page. (See Figure 5-10.) For example, you might want to enter:

  **Call the IT department at ext. 1253 to receive a valid username and password.**

- In the Small Logo URL field, enter the name of a logo file to include a small logo on the login page. (See Figure 5-10.) You must copy this logo to the flash on the Wireless Edge Services zl Module. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module’s Flash” on page 5-33.)
e. In the **Main Logo URL** field, enter the name of a logo file to include a logo at the top of the login page. (See Figure 5-11.) You must copy this logo to the flash on the Wireless Edge Services zl Module. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module's Flash” on page 5-33.)

f. In the **Descriptive Text** field, accept the default text shown on the screen, or enter the text that you want to use. (See Figure 5-11.) For example, you might enter:

   **Enter the username and password you were assigned. Remember that both the username and password are case sensitive.**
4. Configure the welcome page, which mobile users see if they enter a valid username and password and the RADIUS server authenticates them.
   a. Click the **Welcome** tab. (See Figure 5-12.)
b. In the **Title Text** field, accept the default text shown on the screen, or enter the text that you want to use.

c. In the **Header Text** field, accept the default text shown on the screen, or enter the text that you want users to see when they log in. (See Figure 5-13.)

**Note**  
If you customize the **Header Text**, **Footer Text**, or **Descriptive Text** fields, you can enter a maximum of 1,024 characters.

d. In the **Footer Text** field, enter the text that will be displayed at the bottom of the welcome page. By default, this field is empty.
Web Authentication for Mobile Users  
Configuring Web-Auth

e. In the **Small Logo URL** field, enter the name of a logo file to include a small logo on the welcome page. (See Figure 5-13.) You must copy this logo to the flash on the Wireless Edge Services zl Module. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module’s Flash” on page 5-33.)

![Authentication Success](image)

**Figure 5-13. Displaying a Small Logo on the Web-Auth Welcome Page**

f. In the **Main Logo URL** field, enter the name of a logo file to display a logo at the top of the welcome page. (See Figure 5-14.) You must copy this logo to the flash on the Wireless Edge Services zl Module. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module’s Flash” on page 5-33.)

g. In the **Descriptive Text** field, accept the default text shown on the screen, or customize the text as needed. (See Figure 5-14.)
5. Configure the failed page, which mobile users see if they enter an invalid username and password.
   a. Click the **Failed** tab. (See Figure 5-15.)
Web Authentication for Mobile Users
Configuring Web-Auth

Figure 5-15. Configuring the Failed Page

b. In the **Title Text** field, accept the default text shown on the screen, or change the text as needed.

c. In the **Header Text** field, accept the default text shown on the screen, or enter the text that you want users to see if they fail to log in. (See Figure 5-16.)

**Note**

If you customize the **Header Text**, **Footer Text**, or **Descriptive Text** fields, you can enter a maximum of 1,024 characters.

d. In the **Footer Text** field, accept the default text shown on the screen, or enter the text that you want to be displayed at the bottom of the failed page. (See Figure 5-16.) For example, you may want to add the extension that users should call if they cannot log in.
Web Authentication for Mobile Users
Configuring Web-Auth

e. In the **Small Logo URL** field, enter the name of a logo file to include a small logo on the failed page. (See Figure 5-16.) You must copy this logo to the module’s flash. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module’s Flash” on page 5-33.)

![Figure 5-16. Displaying the Small Logo on the Web-Auth Failed Page](image)

f. In the **Main Logo URL** field, enter the name of a logo file to include a large logo on the failed page. (See Figure 5-17.) You must copy this logo to the flash on the Wireless Edge Services zl Module. (For instructions on how to copy the logo file to flash, see “Copying Logo Files to the Module's Flash” on page 5-33.)

![Figure 5-17. Displaying the Large Logo on the Web-Auth Failed Page](image)

g. In the **Descriptive Text** field, accept the default text shown on the screen, or customize the text as needed. (See Figure 5-17.)
Web Authentication for Mobile Users
Configuring Web-Auth

6. Configure the Allow list as described in “Configuring the Allow List” on page 5-28.

Configuring Web-Auth to an External Web Server

The Wireless Edge Services zl Module can implement Web-Auth using pages stored on an external Web server. While you can link as many pages together as you want, the fundamental Web-Auth process still relies on three basic pages: the login page, the welcome page, and the failed page. You map these pages to the URL of the corresponding page on the external Web server. For example, if you map www.CompanyXYZ.com/success.html to the welcome page, the module directs successfully authenticated users to this page.

To configure Web-Auth to an external Web server, complete these steps:

1. Create at least three Web pages (one each for the login, welcome, and failed pages) and load them on your external server. The Web pages can be as simple or complex as you want, but they must include certain commands that are described in “Configuring Custom Web-Auth Pages” on page 5-36.

2. Complete the steps described in “Configuring Web-Auth” on page 5-10.

3. You should be on the Web-Auth screen for the WLAN. Select External from the drop-down menu at the top of the screen. (See Figure 5-18.)

Figure 5-17. Displaying the Main Logo on the Web-Auth Failed Page
Web Authentication for Mobile Users
Configuring Web-Auth

Figure 5-18. Specifying the URL for Web-Auth Pages That Are Stored on an External Web Server

4. Under **External Web Pages**, specify the correct URL for each page.
   a. In the **Login Page URL** field, specify the URL of the login page, which users see when they try to access a Web site. For example, you might enter a URL such as `http://192.168.1.1/login.html` or `http://www.yourcompany.com/login.html`.
   b. In the **Welcome Page URL** field, specify the URL of the welcome page that users see if they log in successfully.
   c. In the **Failed Page URL**, specify the URL of the page that users see if they do not enter a valid username and password or if a RADIUS server is unavailable.

5. Configure the Allow list as described in “Configuring the Allow List” on page 5-28.
Loading Custom Pages onto the Wireless Edge Services zl Module’s Internal Server (Advanced)

As discussed earlier, the Wireless Edge Services zl Module can act as the Web server for Web-Auth. As an alternative to using the module’s default (pre-configured) Web-Auth pages, you can load your own pages onto the module. This advanced option gives you greater freedom in designing your Web pages than simply customizing the text on the default pages.

For advanced Web-Auth configuration, you install an entire directory (.tar) on the module. The directory holds the Web-Auth pages and can include subdirectories as well. The Web pages can be as simple or complex as you like, but must include at least these three pages:

- login.html
- welcome.html
- fail.html

These pages must contain certain commands which are described in “Configuring Custom Web-Auth Pages” on page 5-36.

When you install the directory, the Wireless Edge Services zl Module copies the pages in that directory to this location: flash:/hotspot/wlanX. X is replaced by the index number of the WLAN that you are configuring.

1. Create custom Web-Auth pages and group them in a tar file.
2. Load the directory that you have created onto a File Transfer Protocol (FTP) or Trivial FTP (TFTP) server.
3. Complete the steps described in “Configuring Basic Options and Accessing the Web-Auth Screen” on page 5-11.
4. You should be on the Web-Auth screen for the WLAN. Select Advanced from the drop-down menu at the top of the screen. (See Figure 5-19.)
5. In the **File** field, enter the name of the directory that contains the custom Web pages.

6. Select the type of server that stores the directory (FTP or TFTP) from the **Using** drop-down menu.

7. Enter the server's IP address and port in the **IP Address** and **Port** fields.
   The default port for FTP is 21, and the default port for TFTP is 69.

8. If you are using FTP, enter your username and password in the **User ID** and **Password** fields.
9. In the **Path** field, specify the name of the server directory in which the file that you are loading is stored.

   If the file is stored in the server’s base directory, leave the field empty. For some FTP servers, you might need to enter `/`. To specify a directory within the base directory, include `/`—for example, `/MyDirectory`.

10. Click the **Install** button.

    The file immediately copies to the module's flash.

11. Configure the Allow list as described below.

**Configuring the Allow List**

The Allow list determines the devices that stations can access before they are authenticated by the RADIUS server. The Allow list can contain up to 10 IP addresses. (For more information about which devices should be included on the Allow list, see “Allow List” on page 5-8.)

Follow these steps to configure the Allow list:

1. Complete the steps in “Configuring Basic Options and Accessing the Web-Auth Screen” on page 5-11.
2. You should be on the Web-Auth screen for the WLAN. In the Allow List section on the right side of the screen, add up to 10 IP addresses.
   a. If you have specified External for the Web-Auth page type, enter the IP address of the external Web server:
      i. Under the Allow List heading, select one of the 0.0.0.0 addresses.
      ii. In the Change field, enter the address for the Web server.
      iii. Click the Change button.
   b. Follow the same process to enable access to any other devices providing services to unauthenticated users.

   You do not need to allow the IP addresses of your DHCP and DNS servers. Access to these services is automatically permitted.
Web Authentication for Mobile Users
Configuring Web-Auth

**Note**
When you add a device’s IP address to the Allow list, that device is publicly available; no network authentication is required to access the device. Any user can access the device—unless that device (like the Wireless Edge Services zl Module) has its own authentication requirements.

3. Verify that you have configured the Web pages as described in earlier sections of this chapter.

4. Click the **OK** button to apply your settings and close the Web-Auth screen.

5. If you want, configure encryption for the WLAN. See “Configuring Encryption for a Web-Auth WLAN” on page 5-30.

6. Otherwise, click the **OK** button on the Edit screen and the **Save** link at the top of the screen.

### Configuring Encryption for a Web-Auth WLAN

By itself, Web-Auth ensures that only the proper wireless users can access your private network. However, it does not protect data transmitted over the wireless network. For data privacy, you must enable encryption on the WLAN.

You can configure one of the following encryption options:
- Wired Equivalent Privacy (WEP) with 64-bit keys
- WEP with 128-bit keys
- Wi-Fi Protected Access (WPA)/WPA2-Temporal Key Integrity Protocol (TKIP)
- WPA2-Advanced Encryption Standard (AES)
- both WPA/WPA2-TKIP and WPA2-AES

If you select a WEP option, the WLAN enforces static WEP. If you select a WPA option, the WLAN enforces WPA with preshared keys (WPA-PSK). This security takes effect before users connect to the wireless network and complete Web-Auth.

Follow these steps:

1. Access the Web-Auth WLAN’s Edit screen:
   a. Select **Network Setup > WLAN Setup > Configuration**.
   b. Select the WLAN that uses Web-Auth and click the **Edit** button.
2. In the Encryption section, check the box for your selection.

3. If you have selected a WEP encryption type, click its Config button and specify the WEP keys.

You can enter up to four keys. The currently selected key acts as the password. See “Configuring Static WEP Encryption (No Authentication)” on page 4-48 of Chapter 4: “Wireless Local Area Networks (WLANs)” for more information on configuration options.
4. If you have selected a WPA encryption type, click its **Config** button and specify the preshared key.

See “Configuring WPA/WPA2-PSK” on page 4-58 of Chapter 4: “Wireless Local Area Networks (WLANs)” for more information on configuring the preshared key.

5. Click the **OK** button to close the WLAN **Edit** screen and save your configuration changes to the running-config. You are returned to the **Network Setup > WLAN Setup > Configuration** screen.

---

**Network Setup > WLAN Setup**

<table>
<thead>
<tr>
<th>Index</th>
<th>Enabled</th>
<th>SSID</th>
<th>Description</th>
<th>VLAN / Tunnel</th>
<th>Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>Company</td>
<td>VLAN 1</td>
<td>None</td>
<td>TKIP-RC4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>MyCompany</td>
<td>VLAN 1</td>
<td>TKIP-RC4</td>
<td>TKIP-RC4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✗</td>
<td>web-Auth</td>
<td>VLAN 1</td>
<td>Web-Auth</td>
<td>WEB-2K</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>✗</td>
<td>SSID 4</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✗</td>
<td>SSID 5</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>✗</td>
<td>SSID 6</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>✗</td>
<td>SSID 7</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>✗</td>
<td>SSID 8</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>✗</td>
<td>SSID 9</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>✗</td>
<td>SSID 10</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>✗</td>
<td>SSID 11</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>✗</td>
<td>SSID 12</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>✗</td>
<td>SSID 13</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>✗</td>
<td>SSID 14</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>✗</td>
<td>SSID 15</td>
<td>VLAN 1</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5-22. Network Setup > WLAN Setup > Configuration Screen**

6. Activate the WLAN that you have configured by selecting the WLAN and clicking the **Enable** button.

7. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.
Copying Logo Files to the Module's Flash

If you want to display your company's logo on the Web-Auth login, welcome, or failed page, you must copy the logo file to the appropriate directory on the Wireless Edge Services zl Module's flash.

The module's flash contains a hotspot directory that, in turn, contains a subdirectory for each WLAN on the module. To display a logo on one of the Web-Auth pages, you must copy the logo file to the hotspot subdirectory for the WLAN that you are configuring. For example, if you are configuring Web-Auth as the authentication method for WLAN 2, you must copy your company's logo file to the /hotspot/wlan2 directory in the module's flash. If you are configuring Web-Auth for WLAN 1, you must copy your company's logo file to the /hotspot/wlan1 directory.

To copy the logo file to the appropriate directory for the WLAN that you are configuring, you can use either an FTP or TFTP server. Copy the logo file to the FTP or TFTP server, and then complete these steps:

1. Select Management > System Maint.—Config Files.
2. Click the Transfer Files button at the bottom of the screen. The Transfer screen is displayed. (See Figure 5-23.)
3. Specify the source for the file transfer:
   a. In the From field under Source, use the drop-down menu to select Server.
   b. In the File field, enter the name of the logo file.
   c. In the Using field, use the drop-down menu to select either FTP or TFTP.
   d. In the IP Address field, enter the IP address of the FTP or TFTP server.
   e. If you are using an FTP server, enter the login credentials.
      i. In the User ID field, enter the username for the FTP server.
      ii. In the Password field, enter the password for this username.
   f. In the Path field, enter the path where the configuration is saved on the server. If you are using an FTP server and the logo file is saved at the server’s root level, enter a period followed by a slash (./). If the logo file resides at a different level on the FTP server, enter the complete path. (If you are using a TFTP server, this field may not be required.)

4. Specify the destination as the Wireless Edge Services zl Module:
   a. In the To field under Target, use the drop-down menu to select Wireless Services Module.
   b. In the File field, enter the hotspot directory, the WLAN subdirectory, and the name of the logo file. Use the following syntax:

      /hotspot/<WLAN subdirectory>/<logo filename>

   Replace <WLAN subdirectory> with the subdirectory for the WLAN that you are configuring, and replace <logo filename> with the filename that contains your company’s logo. For example, if you are configuring Web-Auth as the authentication method for WLAN 3, you would enter:

      /hotspot/wlan3/logo.gif
5. Click the **Transfer** button. In the **Status** area at the bottom of the screen, a message is displayed, reporting whether the transfer was successful.
Configuring Custom Web-Auth Pages

You can design your own Web-Auth pages and either store them on an external server or upload them to the Wireless Edge Services zl Module's flash memory (advanced configuration). The custom Web-Auth pages must include a login page, a welcome page, and a failed page. However, in addition to those pages, you can configure links to as many other pages as you desire.

To enable Web-Auth support, you must incorporate specific CGI code on both the login page and the welcome page:

- **Login page**—You must include CGI code that allows users to enter their login credentials and then send these credentials to the Wireless Edge Services zl Module. The module, in turn, submits this information to the RADIUS server.

- **Welcome page**—You must include CGI code that disconnects the user's station from your company's network services and displays the login page again.

You do not need to include any specific CGI commands on the failed page; however, you might want to include a link back to the login page, as the default failed page does.

Configuring the CGI Commands for the Login Page

When you create the login page, you can include any text and graphical elements that you want as long as you include the CGI code shown in Figure 5-25 (for an external page) or Figure 5-26 (for a custom page stored on the module). The required code includes the commands that submit the user's login credentials to the Wireless Edge Services zl Module. When the page is stored on an external server, you must specify the IP address of the module before the reference to the CGI commands. When you are using pages that you have loaded to the module's flash memory with advanced configuration, the IP address is unnecessary.

In addition, the CGI code shown in Figure 5-25 and Figure 5-26 configures a small form that includes a username field and a password field. You can customize the font and the appearance of the form as needed to fit the other design elements on your company's login page.
Web Authentication for Mobile Users
Configuring Custom Web-Auth Pages

Figure 5-25. CGI Code Required for a Login Page Stored on an External Server

```html
<form action="https://192.168.1.50:444/cgi-bin/hslogin.cgi" method="POST">
  <p>
    <label><font face="Arial, Helvetica, sans-serif">Username:</font>
    <input type="text" name="f_user" />
    <font face="Arial, Helvetica, sans-serif">Password:</font>
    <input type="password" name="f_pass" />
    <input type="submit" name="submit" value="Log In" />
  </label>
</p>
</form>
```

You must change the IP address in this code to the IP address for the Wireless Edge Services zl Module on your network.

This code provides the fields for entering login credentials and sends the credentials to the Wireless Edge Services zl Module.

Figure 5-26. CGI Code Required for the Login Page Stored on the Module

```html
<form action="/cgi-bin/hslogin.cgi" method="POST">
  <p>
    <label><font face="Arial, Helvetica, sans-serif">Username:</font>
    <input type="text" name="f_user" />
    <font face="Arial, Helvetica, sans-serif">Password:</font>
    <input type="password" name="f_pass" />
    <input type="submit" name="submit" value="Log In" />
  </label>
</p>
</form>
```

These commands provide the fields for entering login credentials and allow the Wireless Edge Services zl Module to submit the credentials to the RADIUS server.

The CGI code in Figure 5-25 and Figure 5-26 creates the Username field, the Password field, and the Log In button shown in Figure 5-27.

Figure 5-27. Simple Login Page Stored on an External Web Server

```
<form action="https://192.168.1.50:444/cgi-bin/hslogin.cgi" method="POST">
  <p>
    <label><font face="Arial, Helvetica, sans-serif">Username:</font>
    <input type="text" name="f_user" />
    <font face="Arial, Helvetica, sans-serif">Password:</font>
    <input type="password" name="f_pass" />
    <input type="submit" name="submit" value="Log In" />
  </label>
</p>
</form>
```

Please log in

Username: Password: Log In

Figure 5-27. Simple Login Page Stored on an External Web Server
Configuring the CGI Commands for the Welcome Page

Like the login page, the welcome page can include any text and graphical elements that you want as long as you include the CGI code that the Wireless Edge Services zl Module needs to handle Web-Auth properly. The welcome page requires just one line of CGI code, which provides a Disconnect link:

- for an external Web page—\(<a href="https://192.168.1.50:444/cgi-bin/hologout.cgi">Disconnect</a>\>
- for a custom page loaded on the module—\(<a href="/cgi-bin/hologout.cgi">Disconnect</a>\>

Again, for the external page, you must replace the IP address shown in this CGI code with the IP address of the Wireless Edge Services zl Module on your network.

You can include this Disconnect link anywhere on the welcome page. Figure 5-28 shows a basic welcome page.

![Figure 5-28. Simple Welcome Page Stored on an External Server](image)

When the user clicks the Disconnect link, the network session ends, and the login page is displayed in the user's Web browser.
IP Services—IP Settings, DHCP, and DNS

Contents

IP Settings ................................................................. 6-3
  Viewing VLAN Interfaces and Enabling Secure Management ............ 6-3
  Assigning an IP Address to a VLAN .................................. 6-5
  Deleting the IP Address Assigned to a VLAN ......................... 6-6
  Editing the IP Address Assigned to a VLAN .......................... 6-7
  Viewing Statistics for VLANs That Are Assigned IP Addresses ..... 6-7
  Viewing a Graph for VLANs That Are Assigned IP Addresses ....... 6-10

IP Routing ................................................................. 6-12
  Route Table .............................................................. 6-12
  Adding Static Routes to the Route Table ............................... 6-14
    Specifying a Default Route and Gateway ............................ 6-15
  Address Resolution Table ............................................. 6-17

DNS Client ................................................................. 6-19
  Adding DNS Servers ................................................... 6-19
  Deleting a DNS Server ................................................ 6-21
  Specifying a Default Domain Name .................................... 6-21

DHCP Server ............................................................... 6-22
  Overview ................................................................. 6-22
  Configuring the DHCP Server .......................................... 6-23
    Creating DHCP Pools ................................................ 6-23
    Excluding Addresses from a Network Pool .......................... 6-32
    Enabling the DHCP Server ......................................... 6-33
  Configuring Global DHCP Settings: Ignoring BOOTP and Setting the Ping Interval ............................................ 6-35
IP Services—IP Settings, DHCP, and DNS

Contents

Configuring Extended DHCP Options .......................... 6-37
Setting Up Global Options ................................. 6-37
Specifying the Value for an Extended Option in
a DHCP Pool ........................................ 6-39
Configuring Dynamic DNS (DDNS) ......................... 6-41
Viewing DHCP Bindings ....................................... 6-43
Configuring DHCP Relay ..................................... 6-45
IP Settings

To function as a Layer 3 device, the Wireless Edge Services zl Module requires only one IP address, usually assigned to the default management interface. (The default management interface is virtual LAN [VLAN] 1.) For some network environments, however, you may want to assign IP addresses to other VLANs. To do so, you must create VLAN interfaces.

Reasons to assign a VLAN an IP address include:

- You want the Wireless Edge Services zl Module to act as the Dynamic Host Configuration Protocol (DHCP) server for stations in that VLAN.
- You want the Wireless Edge Services zl Module to use Network Address Translation (NAT) to translate IP addresses on another VLAN to an address on this VLAN.
- The Wireless Edge Services zl Module assigns stations in a Web authentication (Web-Auth) WLAN to this VLAN.

  When you configure a WLAN to use Web-Auth, the module must have an IP address on the static VLAN. (For more information about configuring Web-Auth for a WLAN, see Chapter 5: “Web Authentication for Mobile Users.”)

- You want to enable routing between VLANs.

You can assign an IP address to a maximum of eight VLANs on the Wireless Edge Services zl Module.
IP Services—IP Settings, DHCP, and DNS

IP Settings

Viewing VLAN Interfaces and Enabling Secure Management

To view the VLANs that have been assigned IP addresses, select **Network Setup > Ethernet > Configuration**.

![Network Setup > Ethernet > Configuration Screen](image)

The following information is listed for each VLAN:

- **Name**
- **VLAN ID**
- **DHCP Enabled**
  
  This column has a green check mark if the DHCP client is enabled on this VLAN (so that the VLAN receives a dynamic address).
- **IP Address**
- **Subnet Mask**
- **Admin Status**

  This column lists the status (either up or down) of the internal uplink port.
IP Services—IP Settings, DHCP, and DNS

**IP Settings**

- **Status**
  
  This column reports whether or not the VLAN was created successfully.

- **Management Interface**
  
  Only one VLAN can be selected as the management interface, and that VLAN is identified with a green check mark. All other VLANs show a red x in the **Management Interface** field.

When secure management is enabled, you can access the Wireless Edge Services zl Module’s Web browser interface only through the IP address assigned to this VLAN. To enable secure management, click the **Enable Secure Management VLAN** button at the bottom of the screen.

**Assigning an IP Address to a VLAN**

To assign an IP address to a VLAN, complete these steps:

1. Select **Network Setup > Ethernet > Configuration**.
2. Click the **Add** button at the bottom of the screen. The **Add New** screen is displayed.

![Figure 6-2. Add New Screen](image)

3. In the **VLAN ID** field, enter the number of the VLAN.
4. Configure the IP address:
   a. Check the **Use DHCP to obtain IP Address automatically** box if you want the VLAN to receive an IP address through a DHCP server. Do not check this box if you want the Wireless Edge Service zl Module to act as the DHCP server when stations successfully associate to this VLAN. As a DHCP server, the module would, of course, require a static address on the VLAN.
   b. To configure a static address, in the **IP Address** and **Subnet Mask** fields, enter the IP address and subnet mask.

5. If you want this VLAN to be the management interface for the Wireless Edge Services zl Module, check the **Set as Management Interface** box.

6. Click the **OK** button to apply the changes to the running-config.

7. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

After you assign an IP address to a VLAN, the route for the directly connected interface is listed on the module’s route table. (See “Route Table” on page 6-12.)

**Deleting the IP Address Assigned to a VLAN**

If you assign an IP address to a VLAN and later decide to delete it, complete these steps:

1. Select **Network Setup > Ethernet > Configuration**.
2. Select the VLAN and click the **Delete** button. A prompt is displayed, asking you to verify that you want to delete the item.

   **Note**

   You are not deleting the VLAN. If you have mapped a WLAN to the VLAN, the Wireless Edge Services zl Module will continue forwarding traffic in the VLAN. You are deleting the IP address that you previously assigned to the VLAN and removing the VLAN from this Ethernet table (which lists the VLANs that have been assigned IP addresses).

3. Click the **Yes** button to delete the IP address and remove the VLAN from the table.
4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.
Editing the IP Address Assigned to a VLAN

If you need to change the IP address that is assigned to a VLAN, complete these steps:

1. Select **Network Setup > Ethernet > Configuration**.
2. Select the VLAN and click the **Edit** button. The **Configuration** screen for the VLAN interface is displayed.
3. Change the settings as needed and then click the **OK** button.
4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Viewing Statistics for VLANs That Are Assigned IP Addresses

The Wireless Edge Services zl Module tracks statistics for VLANs that are assigned IP addresses. To view these statistics, select **Network Setup > Ethernet**, and click the **Statistics** tab.
IP Services—IP Settings, DHCP, and DNS

IP Settings

### Network Setup > Ethernet

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes In</th>
<th>Packets In</th>
<th>Packets In Dropped</th>
<th>Packets In Error</th>
<th>Bytes Out</th>
<th>Packets Out</th>
<th>Packets Out Dropped</th>
<th>Packets Out Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>192231</td>
<td>1136</td>
<td>0</td>
<td>0</td>
<td>551781</td>
<td>1017</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vlan2</td>
<td>17453</td>
<td>194</td>
<td>0</td>
<td>0</td>
<td>33517</td>
<td>17</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tunnel</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

![Network Setup > Ethernet > Statistics Screen](image)

**Figure 6-4. Network Setup > Ethernet > Statistics Screen**

You can view the following information:

- **Name**—VLAN ID (also referred to as the interface).
- **Bytes In**—total number of bytes received on the interface.
- **Packets In**—total number of packets received on the interface, including packets dropped and error packets.
- **Packets In Dropped**—number of incoming packets that are dropped. Packets might be dropped if the input queue is saturated or if an overrun occurs (the interface receives packets faster than it can transfer them to a buffer).
- **Packets In Error**—number of incoming packets with errors such as:
  - Runt frames—Runt frames are smaller than the minimum Ethernet frame of 64 bytes.
  - Cyclic redundancy check (CRC) errors—CRC errors are reported if the receiving station computes a CRC value that does not match the four-byte CRC field at the end of the Ethernet frame.
  - Late collisions—A late collision occurs after the sending station sends the first 64 octets of data.
- **Bytes Out**—total number of bytes sent on the interface.
- **Packets Out**—total number of packets sent on the interface.
IP Services—IP Settings, DHCP, and DNS

IP Settings

- **Packets Out Dropped**—number of outgoing packets dropped. Conditions that result in dropped packets include:
  - The output queue assigned to the interface is saturated.
  - Collisions have occurred.
- **Packets Out Error**—number of outgoing packets with errors such as malformed packets.

To view more detailed information about a VLAN, select that VLAN and click the Details button at the bottom of the screen. The Interface Statistics screen is displayed.

![Interface Statistics Screen](Image)

---

As Figure 6-5 shows, the **Interface Statistics** screen lists additional information about the VLAN. In particular, you can use this screen to monitor the broadcast and multicast traffic being transmitted on the VLAN. The **Input NonUnicast packets** field reports the incoming broadcast and multicast traffic, and the **Output NonUnicast packets** field lists the outgoing broadcast and multicast traffic.

You can click the **Refresh** button to update the information displayed on the screen.
Viewing a Graph for VLANs That Are Assigned IP Addresses

The Wireless Edge Services zl Module can create graphs of statistics for VLANs that have been assigned an IP address. Such graphs display how the statistics change over time.

To view a graph, follow these steps:

1. Select **Network Setup > Ethernet > Statistics**.

2. Select a VLAN from the list.

3. Click the **Graph** button.
To generate a graph, you must select the statistic that you want to track. Initially, the graph shows input bytes. You can choose any of the statistics displayed in the Details screen (refer to “Viewing Statistics for VLANs That Are Assigned IP Addresses” on page 6-7 for more information about a statistic).

Select the appropriate box for the statistic you want to view.
IP Routing

As discussed in Chapter 1: “Introduction,” the Wireless Edge Services zl Module and its internal uplink port operate at Layer 3 of the Open Systems Interconnection (OSI) model. As part of this Layer 3 functionality, the Wireless Edge Services zl Module maintains a route table. You can view the route table, which automatically lists directly connected interfaces, and you can add static routes to the route table. You can also assign IP addresses to as many as eight VLANs, which then become directly connected interfaces, and you can enable routing between these VLANs.

The Wireless Edge Services zl Module’s route table is completely separate from the route table maintained by the wireless services-enabled switch. The IP addresses that you assign to VLANs on the module are stored and maintained in the module’s running-config. If you want to assign IP addresses to VLANs on the wireless services-enabled switch, you must access the command line interface (CLI), the menu system, or the Web browser interface for the switch itself.

By default, IP routing is disabled. Turning routing on enables these functions:
- DHCP relay
- the internal firewall, including IP ACLs applied to logical (VLAN or tunnel) interfaces
- Network Address Translation (NAT)

Route Table

When the Wireless Edge Services zl Module receives an IP address from a DHCP server, the address is assigned to the default management interface, which is typically VLAN 1. The module automatically recognizes the subnet network directly connected to the default management interface and lists this information in its route table. In the example shown in Figure 6-8, the default management interface (which, in this case, is VLAN 1) is directly connected to network 10.4.1.0/24.
If you assign an IP address to any other VLAN (as described in “IP Settings” on page 6-3), the Wireless Edge Services zl Module recognizes the subnetwork attached to that VLAN and lists it as a directly connected route.

To view the module’s route table, select Network Setup > Internet Protocol and click the IP Forwarding tab. (See Figure 6-8.) The following fields are provided for each route:

- **Destination Subnet**—lists the IP address of the destination subnetwork.
- **Subnet Mask**—lists the subnet mask for the destination subnetwork.
- **Gateway Address**—lists the gateway for reaching the destination subnetwork.
- **Interface**—lists the VLAN through which traffic is forwarded.
IP Services—IP Settings, DHCP, and DNS
IP Routing

- **Protocol**—lists the name of the protocol through which the route was obtained. Routes can be obtained in the following ways:
  - DHCP—Routes can be included with the IP address that the module receives from a DHCP server.
  - Static—Routes can be entered manually.
  - Connected—Routes can be directly connected to an interface.
  - Kernel/ICMP—Routes can be added to the route table if the module receives an Internet Control Message Protocol (ICMP) redirect from an intermediate router.

- **Route Metric**—used for selecting the best available path to the destination subnetwork. Routes with lower metric values are given preference.

- **Active**—indicates whether or not IP forwarding is enabled for the route.

Adding Static Routes to the Route Table

To add a static route to the Wireless Edge Services zl Module’s route table, complete these steps:

1. Select **Network Setup > Internet Protocol** and click the **IP Forwarding** tab.
2. Click the **Add** button at the bottom of the screen. The **Add static route** screen is displayed.

   ![Add Static Route Screen](image)

   **Figure 6-9. Add Static Route Screen**

3. In the **Destination Subnet** field, enter the IP address for the route.
4. In the **Subnet Mask** field, enter the subnet mask.
5. In the **Gateway Address** field, enter the IP address of the next hop.
6. Click the **OK** button to apply the change to the running-config.

7. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

To delete a route, select the route from list in the **Network Setup > Internet Protocol > IP Forwarding** screen. Then click the **Delete** button.

**Specifying a Default Route and Gateway**

A default route is a special static route that applies to all traffic for which the Wireless Edge Services zl Module does not know another route.

When you use the CLI to configure the Wireless Edge Services zl Module's default gateway, the module automatically creates a default route to that gateway. This route is listed in the **Network Setup > Internet Protocol > IP Forwarding** screen. (See Figure 6-10.)

![Network Setup > Internet Protocol](image)

**Figure 6-10. Viewing the Default Route**
Although you can add another default route manually (or, from the CLI, specify another default gateway), only one default route is active—the first route configured. To avoid confusion, ProCurve Networking recommends that you delete all but one default route.

Follow these steps to configure or to change the Wireless Edge Services zl Module’s default route:

1. Select **Network Setup > Internet Protocol** and click the **IP Forwarding** tab.
2. If the route table already lists a default route, select that route and click the **Delete** button.
3. Click the **Add** button at the bottom of the screen. The **Add static route** screen is displayed.
4. In the **Destination Subnet** field, enter 0.0.0.0.
5. In the **Subnet Mask** field, enter 0.0.0.0.
6. In the **Gateway Address** field, enter the IP address of the new default gateway.
7. Click the **OK** button to apply the change to the running-config.

8. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**Address Resolution Table**

The Wireless Edge Services zl Module maintains an address resolution table, which displays the media access control (MAC) addresses associated with particular IP addresses. The module uses this table to prepare IP packets for forwarding to the correct MAC address.

In addition, by default, the Wireless Edge Services zl Module provides proxy ARP for its wireless stations. That is, the module responds to ARP requests for the IP addresses listed in this table.

To view this table, select **Network Setup > Internet Protocol** and click the **Address Resolution** tab.
The **Interface** column lists the VLAN on which the IP address can be reached, and the **Type** column indicates how the module learned to map that IP address to that MAC address. For example, in Figure 6-13, **Dynamic** indicates that the module learned the mapping by listening to frames received from the device at 10.4.1.100.

If you want to remove an entry, select it and click the **Clear** button.

You can add manual entries to the ARP table to force the Wireless Edge Services 2l Module to respond to requests for an address that is not its own. However, you must do so through the CLI.
DNS Client

DNS is the Internet protocol for translating domain names or hostnames into IP addresses. The hostname is the familiar, alphanumeric name for a host on the Internet (for example, www.procurve.com), and the IP address is the 32-bit address that devices on a TCP/IP network use to reach each other. DNS allows users to enter more readily memorable and intuitive hostnames rather than IP addresses. In addition, DNS allows a host to keep the same hostname even if a company changes the host’s IP address.

The Wireless Edge Services zl Module can act as a DNS client. To enable the module to query a DNS server to resolve hostnames, you must define that DNS server. In addition, you can specify a default domain name—which is typically your organization’s domain name.

Adding DNS Servers

To define the DNS servers that the Wireless Edge Services zl Module should contact when it needs to resolve hostnames, complete these steps:

1. Select **Network Setup > Internet Protocol** and click the **Domain Name System** tab.
2. Click the **Add** button at the bottom of the screen. The **Add DNS Server** screen is displayed.

3. In the **Server IP Address** field, enter the IP address of the DNS server.
4. Click the **OK** button. The DNS server is now listed on the **Network Setup > Internet Protocol > Domain Name System** screen.
5. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.
Deleting a DNS Server

If you want to remove a DNS server that is listed on the Network Setup > Internet Protocol > Domain Name System screen, complete these steps:

1. Select Network Setup > Internet Protocol and click the Domain Name System tab.
2. Select the DNS server that you want to delete and click the Delete button at the bottom of the screen. A prompt is displayed, asking if you want to delete the item.
3. Click the Yes button to remove the DNS server.
4. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

Specifying a Default Domain Name

To specify a default domain name, complete these steps:

1. Select Network Setup > Internet Protocol and click the Domain Name System tab.
2. Click the Global Settings button. The Edit DNS Settings screen is displayed.

3. In the Domain Name field, enter your company’s domain name.
4. Click the OK button.
5. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.
DHCP Server

The Wireless Edge Services zl Module can function as a DHCP server. Although the module can provide DHCP services for your entire network, it is more appropriately used as the DHCP server for your wireless network.

Overview

A DHCP server issues dynamic configurations to stations. The DHCP server on the Wireless Edge Services zl Module can assign stations a variety of settings, or options, in the configuration. Standard options include:

- an IP address, which the module selects from a configured range of IP addresses
- a default router address
- a domain name
- primary and secondary Domain Name System (DNS) addresses
- a lease time (the time that the station can keep this configuration before requesting it again)

Other options that you can specify for the configuration include:

- broadcast addresses
- NetBIOS node type
- NetBIOS name server address
- boot file
- Bootstrap Protocol (BOOTP) server address

You can also define your own extended options.

The configuration for clients is stored in a DHCP pool, which you create and associate with a particular VLAN on your Wireless Edge Services zl Module. When the module receives a DHCP request from a station in that VLAN, it issues the configuration stored in the pool to the station, including:

- all configured options that the client requested
- an IP address selected from the range for the pool

You can also create pools that assign fixed IP addresses to particular hosts.

A list of excluded IP addresses, which the module never assigns to DHCP clients, prevents conflicts with static IP address assigned on your network.
As a DHCP server, the Wireless Edge Services zl Module can also implement dynamic DNS (DDNS), which updates a DNS server whenever a host’s IP address changes.

Finally, the Wireless Edge Services zl Module supports DHCP relay.

Configuring the DHCP Server

If you want the Wireless Edge Services zl Module to assign IP addresses to devices on your network, you must configure it as a DHCP server by following the steps outlined in the following sections. You can access all of the options necessary to configure the DHCP server from the Network Setup > DHCP Server screen in the Web browser interface.

To run the DHCP server on a VLAN, the VLAN must meet these requirements:

- It must have a static IP address. (See “Assigning an IP Address to a VLAN” on page 6-5.)
- It must not implement DHCP relay.

DHCP relay configurations take precedence over the DHCP server. In other words, if you associate a VLAN interface with a network pool and you also implement DHCP relay on that interface, the module does not respond to DHCP requests on that VLAN. Instead it relays requests to an external server.

After configuring the DHCP server, you must enable it. If the server is already enabled, any configurations you make to it take effect only after the server restarts. The DHCP server automatically restarts 30 seconds after you apply a change. You can also manually restart the server.

Creating DHCP Pools

As a DHCP server, the Wireless Edge Services zl Module requires one or more pools from which to issue configurations to devices. You can configure either a network pool or a host pool.

A network pool includes a range of IP addresses from which the DHCP server can choose as it responds to DHCP requests. The Wireless Edge Services zl Module associates each network pool with a particular VLAN. When a station in that VLAN sends a DHCP request, the module responds with one of the addresses from the associated pool.
When you use network pools, you can also specify a range of excluded addresses, which are addresses in a pool that the Wireless Edge Services zl Module is not allowed to assign. Use the excluded addresses to protect IP addresses on your network that you want to remain fixed, such as the IP addresses of routers and DNS servers.

A host pool contains a single fixed IP address and is designated to a specific device. When that device sends a DHCP request, the Wireless Edge Services zl Module recognizes its MAC address (or client identifier) and assigns the device the fixed IP address.

Use host pools for devices that require a dynamic address but also a stable address that never changes. For example, certain devices should almost always be given static addresses so that routes remain accurate, the network design remains logical and consistent, and the traffic flow remains uninterrupted. Network servers, such as Remote Access Dial In User Service (RADIUS) servers, need stable addresses so that other network devices, which are configured to query those servers, always know where to reach them.

However, sometimes a device that needs a stable IP address is also required to take a dynamic address from a DHCP server. You can configure the router to assign a fixed DHCP address to this device.

Also, when you want to assign a permanent address to a particular host, sometimes it is better to configure this address through a DHCP server, rather than through whatever application is on the host. DHCP automatically tracks addresses so that two devices are not inadvertently given the same address.

**Creating a Network Pool.** To create a network pool of IP addresses, complete these steps:

1. Select **Network Setup > DHCP Server > Configuration.**
2. Click the **Add** button. The **Add Pool** screen is displayed.
3. In the **Pool Name** field, enter a name for the pool. You can enter up to 255 alphanumeric characters (no special characters).

   The name is typically a descriptive text string that helps identify the purpose of the pool or the set of clients that it is intended to serve.

4. In the **Domain** field, enter the domain name for the network on which the Wireless Edge Services zl Module is running.
5. In the **Associated Interface** field, use the drop-down menu to select the VLAN interface that you want to associate with this network pool. This drop-down menu includes all of the Wireless Module’s configured interfaces (such as VLAN 1). The IP address and subnet mask assigned to the associated interface are automatically inserted into the appropriate fields.

6. In the **Lease Time** section, specify the lease length for IP addresses assigned by the DHCP server. Either select **Infinite** or specify a lease time (in dd:hh:mm format). The maximum number of days is 365, the maximum number of hours is 23, and the maximum number of minutes is 59. Therefore, the maximum lease time is roughly one year.

7. In the **Servers** section, specify the IP addresses of the servers that stations might need to reach to function properly.
   a. In the left column, select the server type.
   b. Click the top of the right column and specify the IP addresses for the corresponding server type. Use the **Insert** and **Remove** buttons as needed to add and delete additional servers for the server type.

   At a minimum, you should enter the IP address of the default router (default gateway) for this VLAN and at least one DNS server. You can add up to eight default routers, eight DNS servers, eight NetBIOS servers, and one BOOTP server. (NetBIOS servers are called Windows Internet Naming Service [WINS] servers. These WINS servers map devices’ names to their IP addresses.)

8. In the **Included Ranges** section, click the **Insert** button and specify the starting and ending IP addresses to be included in the address pool.

   The DHCP server will assign IP addresses only from this range. All of the IP addresses in the range must be within the subnetwork of the VLAN selected as the **Associated Interface**.

   Use the **Insert** and **Remove** buttons as needed to add and delete additional address ranges.
9. If necessary, set options for a network that uses NetBIOS:
   a. In the **NetBios Node** field, use the drop-down menu to select the NetBIOS node type.
      
      The NetBIOS node type determines how stations resolve NetBIOS names to IP addresses, whether by broadcasting messages, by using a WINS server (peer-to-peer), or by a combination of the two. You can select one of four options:
      
      – **b** (Broadcast)
      – **h** (Hybrid)
      – **m** (Mixed)
      – **p** (Peer-to-Peer)

   b. If you select a hybrid, mixed, or peer-to-peer node type, you must specify the WINS server that maps devices’ names to their IP addresses:
      
      i. In the **Servers** section, select **NetBios (WINS)** from the left column.
      
      ii. Click the top of the right column and enter the WINS server’s IP address.
      
      iii. Optionally, click the **Insert** button and add up to eight WINS servers.

10. Optionally, in the **Boot File** field, specify the name of a file (including its directory structure).

    An older device might not have its operating system (OS) loaded onto it; such a device can boot remotely from the file that you specify in this field.

11. If your network might include BOOTP clients, specify the IP address of the next server in the clients’ boot process:

    i. In the **Servers** section, select **Bootp Next** from the left column.
    
    ii. Click the top of the right column and enter the server’s IP address.

12. Click the **OK** button to apply your changes to the running-config. The new network pool is shown on the **Network Setup > DHCP Server > Configuration** screen.

13. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**Creating a Host Pool.** To create a host pool, which stores a fixed IP address for a particular device, complete these steps:

1. Select **Network Setup > DHCP Server** and click the **Host Pool** tab.
6-29

IP Services—IP Settings, DHCP, and DNS

DHCP Server

Figure 6-19. Network Setup > DHCP Server > Host Pool Screen

2. Click the **Add** button. The **Add Pool** screen is displayed.
3. In the **Pool Name** field, enter the name of the pool to which this IP address will belong. For example, you might enter the name of the device. The name can include up to 255 alphanumeric characters.

4. In the **IP Address** field, enter the fixed address for this device. You can specify an IP address that is also within a network pool: the Wireless Edge Services zl Module automatically adds the fixed address to its list of exclusions. You can view this exclusion in the **Network Setup > DHCP Server > Excluded** screen.

5. In the **Client Name** field, enter a descriptive name for the client that will receive this IP address.
6. Enter either a hexadecimal client identifier (ID) in the Client ID field or a MAC address in the Hardware Address field, but not both.

When a device sends a DHCP request, the request includes a client ID, either a customized ID or the device’s MAC address. The Wireless Edge Services zl Module uses this value to match the device to the correct host pool and fixed IP address.

A customized client ID, entered in the Client ID field, can use ASCII or hexadecimal characters. Typically, a customized client ID uses hexadecimal characters. Use colons to separate the hexadecimal characters.

7. Set up other options much as you would for a network pool:
   a. In the Servers section, specify the IP addresses of the servers that stations might need to reach to function properly.
      i. In the left column, select the server type.
      ii. In the right column, specify the IP addresses for the corresponding server type. Use the Insert and Remove buttons as needed to add and delete additional servers for the server type.

At a minimum, you should enter the IP address of the default router (default gateway) for the subnetwork on which you have placed this device. You should also enter the IP address of one or more DNS servers.

If this network uses NetBIOS or BOOTP, you should specify servers for those protocols.

b. In the Lease Time section, specify the lease length for IP addresses assigned by the DHCP server. Either select Infinite or specify a lease time (in dd:hh:mm format).

c. If this client will use NetBIOS, in the NetBios Node field, use the drop-down menu to select the NetBIOS node type.

d. If this device is a BOOTP client, in the Boot File field, enter the name of the file from which the device should boot.

8. Click the OK button to apply your changes to the running-config. The new host pool entry is shown on the Network Setup > DHCP Server > Host Pool screen.

9. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

You can create multiple host pools.
Excluding Addresses from a Network Pool

You may sometimes want to prevent the DHCP server from assigning specific IP addresses within the network pool or pools that you have configured. For example, you would not want the DHCP server to assign an IP address that is already configured statically on another network device. In such cases, simply add exclusions to the DHCP server configuration.

To exclude IP addresses from dynamic assignment, complete these steps:

1. Select Network Setup > DHCP Server and click the Excluded tab.

2. Click the Add button. The Add Range screen is displayed.

3. In the Start IP Address and End IP Address fields, enter the starting and ending IP addresses, respectively, for the range of excluded addresses.

   If you want to specify only one IP address, simply leave the End IP Address fields blank.

4. Click the OK button to apply your changes.

   The excluded range is displayed on the Network Setup > DHCP Server > Excluded screen.
5. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

You can specify multiple ranges.

**Enabling the DHCP Server**

To enable the DHCP server, complete these steps:

1. Select **Network Setup > DHCP Server > Configuration**.
2. Check the **Enable DHCP Server** box.
IP Services—IP Settings, DHCP, and DNS

DHCP Server

Figure 6-23. Enabling the DHCP Server

3. Click the Apply button.

4. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

To disable the DHCP server, uncheck the Enable DHCP Server box and click the Apply button.
Configuring Global DHCP Settings: Ignoring BOOTP and Setting the Ping Interval

Two global settings apply to the Wireless Edge Services zl Module's internal DHCP server:

- **Ignoring BOOTP requests**—BOOTP is an earlier protocol that uses the same ports as DHCP. Like DHCP, BOOTP enables stations to receive dynamic configurations, typically including the name and location of a boot file. If your network includes devices that use BOOTP, it may also include a server already configured to serve these devices. In this case, you should configure the Wireless Edge Services zl Module to ignore BOOTP requests so that they can reach the proper server.

- **Ping interval**—Before assigning an IP address to a station, the Wireless Edge Services zl Module pings the address twice to verify that the address is available. You can configure the number of seconds that the module waits in between the two pings.

To configure the global DHCP settings, follow these steps:

1. Select **Network Setup > DHCP Server > Configuration**.
2. Check the **Ignore Bootp** box to configure the module to ignore BOOTP requests.

   Checking the box allows the BOOTP requests to continue on to a BOOTP server.

3. Enter a value from 1 through 10 seconds in the **Ping time interval** field.

   The default setting is 1 second.

4. Click the **Apply** button.

---

**Figure 6-24. Configuring Global DHCP Settings**
Configuring Extended DHCP Options

The Wireless Edge Services zl Module allows you to configure extended DHCP options for both network and host pools. For example, in addition to assigning clients a DNS server address, you might want to assign them a Network Time Protocol (NTP) server address. An NTP server address is defined through option 42.

To configure extended DHCP options, you first define globally which extended option or options you will use. Next, you configure values for these options in particular network or host pools.

Setting Up Global Options

To define the extended options to be used by your DHCP server, complete these steps:

1. Select Network Setup > DHCP Server > Configuration.
2. Click the Options Setup button. The Global Options screen is displayed.

3. Click the Insert button.
4. Enter an alphanumeric string in the Name field to identify the option.

The string cannot include special characters or spaces. If you include such characters, you will receive this message when you click the OK button: Failed to save - Option name has invalid characters

Some option names are reserved for DHCP options automatically enabled on the Wireless Edge Services zl Module. You cannot use the names listed in Table 6-1.
Table 6-1. Names Not Allowed for Global DHCP Options

<table>
<thead>
<tr>
<th>Reserved Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet-mask</td>
</tr>
<tr>
<td>routers</td>
</tr>
<tr>
<td>domain-name-servers</td>
</tr>
<tr>
<td>domain-name</td>
</tr>
<tr>
<td>broadcast-address</td>
</tr>
<tr>
<td>netbios-name-servers</td>
</tr>
<tr>
<td>netbios-node-type</td>
</tr>
<tr>
<td>bootfile-name</td>
</tr>
<tr>
<td>user-class</td>
</tr>
<tr>
<td>next-server</td>
</tr>
<tr>
<td>dynamic-bootp</td>
</tr>
</tbody>
</table>

5. In the **Code** field, enter a value between 0 and 254. You should enter the standard code for the option that you are defining.

   Again, some DHCP codes are reserved for the DHCP options configured when you set up the pool. You cannot alter the codes listed in Table 6-2.

Table 6-2. Codes Not Allowed for Global DHCP Options

<table>
<thead>
<tr>
<th>Reserved Code</th>
<th>Associated Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet mask</td>
</tr>
<tr>
<td>3</td>
<td>router</td>
</tr>
<tr>
<td>5</td>
<td>name server</td>
</tr>
<tr>
<td>6</td>
<td>domain name server</td>
</tr>
<tr>
<td>15</td>
<td>domain name</td>
</tr>
<tr>
<td>28</td>
<td>broadcast address</td>
</tr>
<tr>
<td>44</td>
<td>Netbios name server</td>
</tr>
<tr>
<td>46</td>
<td>Netbios node type</td>
</tr>
<tr>
<td>67</td>
<td>bootfile</td>
</tr>
<tr>
<td>77</td>
<td>userclass</td>
</tr>
<tr>
<td>119</td>
<td>dns list</td>
</tr>
</tbody>
</table>
6. The **Type** drop-down menu includes two options: **ip** and **ascii**.

   The setting that you select determines the type of value that you enter when you actually configure the option in a pool. (See “Specifying the Value for an Extended Option in a DHCP Pool” on page 6-39.)

   In this example, you are setting up an option to specify an IP address for an NTP server, so you select **ip**. Selecting **ascii** allows you to enter alphanumeric characters for the option.

   ![Figure 6-26. Defining a Global Option for DHCP](Image)

7. Click the **Insert** button again if you need to add more options.

8. When you are finished setting up the options, click the **OK** button.

9. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

### Specifying the Value for an Extended Option in a DHCP Pool

After you set up an extended option, you must configure the value that the DHCP server assigns for that option. Like typical DHCP settings, you configure these values for particular pools.

Complete these steps:

1. Select **Network Setup > DHCP Server > Configuration**.

2. To configure an option for a network pool, complete these steps and then proceed to step 4:
   a. Select one of the pools in the **Network Pool** section. (See “Creating a Network Pool” on page 6-24 for instructions on creating the pool.)
   b. Click the **Options** button. The **Pool Options** screen is displayed.
3. To configure an option for a host pool, complete these steps and then proceed to step 4:
   a. Click the **Host Pool** tab.
   b. Select one of the pools. (See “Creating a Host Pool” on page 6-28 for instructions on creating the pool.)
   c. Click the **Options** button. The **Pool Options** screen is displayed.

4. In the **Pool Options** screen, click the **Insert** button.

![Figure 6-27. Specifying the Value for an Extended Option](image)

5. Click the **Name** field. It turns into a drop-down menu that includes the names of all of the options defined globally. (See “Setting Up Global Options” on page 6-37.)

6. In the **Value** field, enter either an IP address or an alphanumeric string, depending on whether the type specified for the global option is **ip** or **ascii**. The Wireless Edge Services zl Module sends this value for the option to DHCP clients.

7. Click the **Insert** button again to configure another option. You can configure as many options as have been defined globally.

8. Click the **OK** button.

9. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.
Configuring Dynamic DNS (DDNS)

A DNS server resolves hostnames to IP addresses. For the DNS server to function correctly, clearly its table must include the correct IP address for each hostname. However, a device that acts as a DHCP client might unexpectedly receive a new IP address, invalidating the DNS server's hostname table. DDNS addresses this problem by updating a DNS server whenever a client’s IP address changes.

The Wireless Edge Services zl Module supports DDNS as part of its function as a DHCP server. The module can either update the DNS server itself or allow clients to do so. The DNS server itself, of course, must also support DDNS (as specified in Request for Comments [RFC] 2136). Such a server is called a DDNS server. In addition, if the clients will send the updates, they must also support DDNS.

You enable and configure DDNS separately for each DHCP pool, which can be either a network pool or a host pool. Complete these steps:

1. Select **Network Setup > DHCP Server > Configuration**.
2. To configure DDNS for a network pool, complete these steps and then proceed to step 3:
   a. Select one of the pools in the **Network Pool** section. (See “Creating a Network Pool” on page 6-24 for instructions on creating the pool.)
   b. Click the **DDNS** button. The **Global Options** screen for DDNS is displayed.
3. In the **Domain Name** field, enter an alphanumeric string.
   In DDNS updates, a client’s name follows this format:
   - user class, if the client has sent such a class
   - client’s MAC address
   - the domain name that you specify in this step
   For example, an update might identify a client as follows:

4. Specify the time-to-live for updates in the **TTL** field. This setting determines the time in seconds that the Wireless Edge Services zl Module waits for a reply from the DDNS server.
   The valid range is from 1 through 65,535 seconds.
5. From the **Automatic Update** drop-down menu, select which device sends the dynamic updates:

   - Select **Server Update** to have the Wireless Edge Services zl Module send an update whenever one of its DHCP clients accepts an IP address from it.
   - Select **Client Update** to have each DHCP client send an update when it receives an IP address from the DHCP server. In this case, the client must support DDNS.
   - Select **Off** to disable automatic updates. You can still send manual updates to the DDNS server by clicking the **Send All** button.

6. Optionally, check the **Enable Multiple User Class** box.

   This setting allows users to send multiple user classes. The name in the DDNS updates includes the first class.

7. Specify the IP addresses of up two DDNS servers in the **DDNS Servers** field.

8. Click the **OK** button.

Make sure that the DHCP server is enabled, and then save your configuration.

**Viewing DHCP Bindings**

The Wireless Edge Services zl Module stores a table of the IP addresses that it has assigned to DHCP clients. You can view this table and verify that the DHCP server is issuing the correct addresses.

Select **Network Setup > DHCP Server** and click the **Status** tab.
The screen displays a list of leases, with information in these columns:

- **IP Address**—the IP address assigned to the station
- **MAC Address/Client ID**—the station’s MAC address or, if it sent a customized ID, its ID
- **Type**—the method that the Wireless Edge Services zl Module used to select the IP address
  - **Automatic** indicates that the module chose the IP address from a network pool. **Manual** indicates that the module matched the DHCP client to a host pool and assigned it a fixed IP address.
- **Expiration**—the date and time when the DHCP lease ends

The fixed IP address shown in Figure 6-29 never expires: its lease was configured as infinite.
Configuring DHCP Relay

Your network might already include a DHCP server. The Wireless Edge Services zl Module can provide DHCP relay services to this server. A DHCP server serves only clients on the same subnetwork or VLAN. DHCP relay passes DHCP requests from clients on one subnetwork to a DHCP server on a different subnetwork, eliminating the need for a DHCP server on each local network segment.

To provide DHCP relay services, a VLAN interface must have a static IP address. (The DHCP client is disabled on the VLAN interface.)

**Note**

Enabling DHCP relay on an interface overrides the DHCP server. That is, the server will not respond to requests on that interface even if you have configured a pool for it.

**Note**

The gateway interface is the interface through which the Wireless Edge Services zl Module reaches the external DHCP server. Like the interface that relays the DHCP requests, the gateway interface cannot run either the DHCP server or the DHCP client. (That is, the interface requires a static address.)

To configure DHCP relay on the Wireless Edge Services zl Module, complete these steps:

1. Select **Network Setup > DHCP Server** and click the **Relay** tab.
2. Click the **Add** button. The **Add Relay Information** screen is displayed.
3. In the **Interface** field, use the drop-down menu to select the VLAN interface that receives the DHCP requests.

4. In the **Server** fields, enter the IP addresses for up to four DHCP servers. In each applicable **Gateway** field, use the drop-down menu to specify the corresponding interfaces by which the DHCP servers may be reached. For example, if the module’s default gateway knows how to route traffic to the DHCP server, you would select the default VLAN.

5. Click the **OK** button.

6. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

The configuration is displayed on the **Network Setup > DHCP Server > Relay** screen. (See Figure 6-32.) The **Interfaces** section shows the interface from which DHCP packets will be forwarded to the DHCP server. The **Gateway Information** section shows the server IP address and the interface by which the DHCP server can be reached.
You can select the DHCP relay configuration for an interface and edit or delete it by clicking the corresponding buttons.
# Access Control Lists (ACLs)

## Contents

- Overview ............................................................... 7-2
- Stateful ACLs ....................................................... 7-2
- ACL Types ............................................................ 7-3
  - Standard IP ACLs .................................................... 7-3
  - Extended IP ACLs ..................................................... 7-3
  - MAC Standard ACLs .................................................. 7-4
  - MAC Extended ACLs .................................................. 7-4
- ACL Rules .............................................................. 7-4
  - Precedence ........................................................... 7-5
  - Filters ............................................................... 7-5
  - Operation ........................................................... 7-7
- ACL Strategies ........................................................ 7-8
- Configuring ACLs ..................................................... 7-10
  - Creating ACLs ....................................................... 7-10
  - Configuring Rules for ACLs ...................................... 7-13
    - Creating Rules for Standard IP ACLs .......................... 7-14
    - Creating Rules for Extended IP ACLs .......................... 7-17
    - Creating Rules for MAC Extended ACLs ....................... 7-23
    - Modifying ACL Rules ............................................. 7-25
- Applying ACLs to Interfaces ....................................... 7-26
- Using ACLs with DHCP Services ................................... 7-28
- Viewing ACL Statistics ............................................. 7-29
Access Control Lists (ACLs)
Overview

Overview

You can configure access control lists (ACLs) on the ProCurve Wireless Edge Services zl Module to control traffic to and from wireless stations. An ACL is an ordered list of rules that select packets according to header information and dictate whether the module should permit (forward) or deny (drop) those packets.

ACLs allow you to control wireless users’ network rights. You can configure ACLs for purposes such as:

- limiting certain groups of wireless users to Internet access only
- permitting certain groups of wireless users access to a limited list of network servers
- limiting certain groups of wireless users to certain types of applications
- restricting access to a particular private server to a select group of users only

You can also use ACLs to select traffic for Network Address Translation (NAT). See Chapter 8: “Configuring Network Address Translation (NAT)” to learn how to configure this feature of the Wireless Edge Services zl Module’s firewall.

Stateful ACLs

On the Wireless Edge Services zl Module, ACLs applied to VLAN interfaces are stateful. In other words, the module tracks traffic associated with a particular session. Once it has permitted one packet in a session, it permits all packets necessary for that session. For example, if you create a rule to permit traffic from wireless stations to an HTTP server, you do not need to create a rule to permit the HTTP server's return traffic.

ACLs applied to the physical ports, on the other hand, are not stateful. They check every packet or frame that arrives on the interface.
Access Control Lists (ACLs)

Overview

ACL Types

The Wireless Edge Services zl Module supports two basic ACL types:

- **IP ACLs**—based on the IP header (Layer 3)
  
  IP ACLs control traffic *inbound* on an interface. They can apply to the Wireless Edge Services zl Module’s virtual LAN (VLAN) interfaces or to its two physical interfaces: the internal uplink and downlink ports. If applied to a VLAN interface, the IP ACLs control *routed* traffic. If applied to a physical port, the IP ACLs control inbound traffic on *all* VLANs tagged for that interface.

- **MAC ACLs**—based on the Media Access Control (MAC) header (Layer 2)
  
  Standard MAC ACLs are used for MAC authentication. You can apply extended MAC ACLs to the module’s physical interfaces, but not to its VLAN interfaces. Like IP ACLs, the extended MAC ACLs affect *inbound* traffic.

Both types of ACLs include two subtypes: standard and extended.

Standard IP ACLs

Standard IP ACLs permit and deny traffic according to source IP addresses. They match inbound traffic based on the following IP header fields:

- **source IP address**—either any IP address, an individual (“host”) IP address, or all IP addresses in a particular subnetwork

- **WLAN index**—the index number (1 through 256) of the WLAN through which the packet arrived (for physical interfaces only)

You can apply a standard IP ACL to inbound traffic on either a logical (VLAN or tunnel) interface or a physical (internal uplink or downlink) interface. When you apply an ACL to a logical interface, the traffic must be routed to be filtered.

Extended IP ACLs

Extended IP ACLs can permit and deny traffic according to more sophisticated criteria than standard IP ACLs. They match inbound traffic based on the following IP header fields:

- **source and destination IP address**—either any IP address, an individual (“host”) IP address, or all IP addresses in a particular subnetwork

- **ICMP message type and code**
Access Control Lists (ACLs)

Overview

- **TCP and UDP source and destination ports**
- **WLAN index**—the index number (1 through 256) of the WLAN through which the packet arrived (for physical interfaces only)

You can apply an extended IP ACL to inbound traffic on either a logical (VLAN or tunnel) interface or a physical (internal uplink or downlink) interface. Again, an ACL on a logical interface only affects traffic that the Wireless Edge Services zl Module actually routes.

**MAC Standard ACLs**

MAC standard ACLs permit and deny traffic according to the source MAC address in the frame. The Wireless Edge Services zl Module uses these ACLs to implement local MAC authentication, restricting access to WLANs according to stations' MAC addresses. For more information on these ACLs, see “MAC Filters (Local MAC Authentication)” on page 12-75 of Chapter 12: “Wireless Network Management.”

**MAC Extended ACLs**

MAC extended ACLs permit and deny traffic according to the source and destination MAC addresses, as well as other information in the MAC header, such as the encapsulated protocol, the VLAN tag, or the 802.1p priority.

You can apply a MAC extended ACL to inbound traffic on a physical (internal uplink or downlink) interface.

When you apply the ACL to the uplink interface, the ACL examines the Ethernet header for traffic that arrives on the uplink port from the wired network.

When you apply the ACL to the downlink interface, the ACL examines the encapsulated 802.11 header for traffic that arrives from RPs on the downlink port. The ACL also examines the Ethernet header after the Wireless Edge Services zl Module bridges the traffic from the WLAN to the VLAN.

**ACL Rules**

An ACL consists of one or more rules, which the Wireless Edge Services zl Module processes in order. Each rule performs two functions:

- selects traffic according to the filters that you configure
- performs an operation on the selected traffic
Access Control Lists (ACLs)
Overview

For all ACL types, rules include the following specifications:
- **precedence**—the order in which the rule is processed
- **filters**—the criteria by which a rule selects packets
- **operation**—the action that the Wireless Edge Services zl Module takes on traffic selected by a rule

All ACLs include an implicit “deny any” rule at the end. In other words, if traffic does not match any of the ACLs rules, the ACL drops the traffic. MAC standard ACLs, which are configured as filters for local MAC authentication, are the exception. They include an implicit “permit any” rule at the end. See “MAC Filters (Local MAC Authentication)” on page 12-75 of Chapter 12: “Wireless Network Management.”

Precedence

An ACL’s rules are processed in ascending numeric order until a “match” is found for the packet or frame. When the Wireless Edge Services zl Module matches traffic to the rule, the rule has “selected” the traffic. The module then performs the operation defined for the rule.

Each ACL has a list of ordered rules separate from all other ACLs. For example, two ACLs can each have one rule with a precedence value of 1.

Filters

Filters specify the information that a packet’s header must match. As discussed in “ACL Types” on page 7-3, valid fields depend on the ACL type. A packet or frame must match every filter that you specify.

Rules for all ACL types can include these filters:
- **source address**, either IP or MAC address
  - The filter can select:
    - all addresses
    - a single address
    - a range of addresses, specified either by subnetwork address and prefix length (for IP ACLs) or by mask (for MAC extended ACLs)
- **WLAN index number** (from 1 through 256)
  - The traffic must arrive from this WLAN to match the rule. This setting is optional and takes effect only for ACLs applied to physical interfaces. You should only use it for the ACLs applied to the downlink port.
Access Control Lists (ACLs)

Overview

Extended IP ACL rules can include these additional filters:

- **destination IP address**
  
  The filter can select:
  
  - all addresses
  - a single address
  - a range of addresses, specified by subnetwork address and a prefix length

- **protocol**
  
  By default, a rule matches all IP packets, but you can limit the rule to a specific protocol including:
  
  - ICMP
  - TCP
  - UDP

- for ICMP packets, ICMP type and ICMP code
- for TCP and UDP packets, source and destination ports

  In this way, you can control traffic according to the application. For example, configure a rule to select Web traffic by specifying the TCP protocol and destination port 80.

Extended MAC ACL rules can include these additional filters:

- the destination MAC address, either a single address or a range of addresses (specified by a mask)
- VLAN ID—a specific VLAN ID number
- 802.1p priority—the traffic service class used for quality of service (QoS)
- EtherType—the Layer 3 protocol encapsulated in the frame:
  
  - IPv4—Internet Protocol, version 4
  - ARP—Address Resolution Protocol
  - RARP—Reverse Address Resolution Protocol
  - AppleTalk
  - AARP—AppleTalk Address Resolution Protocol
  - 802.1q—VLANs
  - IPX—Internetwork Packet Exchange
  - IPv6—Internet Protocol, version 6
Operation

The module takes one of the following actions on packets selected by a rule:
- **deny**—the module drops the selected traffic
- **permit**—the module forwards the selected traffic
- **mark**—the module marks the selected traffic for a certain type of QoS and forwards the traffic

**Permit and Deny.** These operations allow you to control users’ network access.

Remember, the operation only affects traffic that meets all of the criteria of the rule. Also, the operation is explicit. That is, the module performs the operation on selected traffic, but does not perform the opposite action on traffic that is not selected. Instead, the module attempts to match the traffic against the next rule in order of precedence.

However, all ACLs include an implicit **deny any** rule at the end, which drops all traffic not selected by other rules. In other words, traffic is permitted only if explicitly permitted by one of the ACL’s rules. Therefore, whenever you apply an ACL to an interface, make sure that you include a rule to permit all traffic that you want the Wireless Edge Services zl Module to forward.

**Mark.** Besides deny and permit, a third operation is mark, which marks traffic for a particular type of QoS or Type of Service (TOS). Marked traffic is also forwarded. The mark operation only takes effect for ACLs applied to physical interfaces.

Two protocols define QoS classes:
- **802.1p**—a mechanism for implementing QoS at Layer 2

802.1p divides traffic into different classes and provides expedited service to traffic in higher-priority classes. Eight different classes of service (0 through 7) are available. The class is indicated in three bits of an 802.1Q VLAN tag. Table 7-1 shows the type of service typically associated with each 802.1p class. However, the actual treatment for each class is left to your network implementation. The Wireless Edge Service zl Module simply marks traffic for a particular class.
Access Control Lists (ACLs)
Overview

Table 7-1. Standard QoS for 802.1p Classes

<table>
<thead>
<tr>
<th>Priority Value</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 and 2</td>
<td>lowest priority (background)</td>
</tr>
<tr>
<td>0 and 3</td>
<td>default priority (best effort)</td>
</tr>
<tr>
<td>4 and 5</td>
<td>higher priority (video and voice)</td>
</tr>
<tr>
<td>6 and 7</td>
<td>highest priority (network control traffic)</td>
</tr>
</tbody>
</table>

- **TOS**—a mechanism for implementing QoS at Layer 3
  
  The value for the IP header’s one-byte TOS field can range from 0 through 255. Typically, only values 0 through 63 are used—the six-bit Differential Services (DiffServ) Code Point (DSCP) values. (The other two bits make up the explicit congestion notification field.)
  
  Again, higher values typically receive higher priority, but the exact handling depends on your network’s implementation.

ACL Strategies

The Wireless Edge Services zl Module’s ACLs can enforce a variety of flexible policies. Within a given rule, or among the rules in a given ACL, you can combine filter criteria—for example, to filter based on a port number and source and destination addresses, or based on an Ethertype and a WLAN index value, and so on.

Example policies include:

- **limiting a particular subnetwork to accessing certain servers only**
  
  For example, your Wireless Edge Services zl Module places wireless traffic in VLAN 8 (192.168.8.0/24). You want to limit the wireless users to accessing a Web server. You would create an extended IP ACL and add a permit rule with the destination address of the Web server. The source address would be 192.168.1.0, and the prefix length would be 24.
  
  You would then apply the ACL to inbound traffic on VLAN 8. The module only forwards traffic matching the permit rule (that is, traffic destined to the Web server).

- **marking traffic destined for a particular port (or range of ports) for QoS or TOS**
You may want to mark time-sensitive traffic, which is often destined to one of UDP's real-time ports, for higher QoS. For example, to mark traffic destined for UDP port 1720 with a TOS value, you would create an extended IP ACL with a rule that includes these specifications:

- a mark operation and the desired TOS value
- the UDP protocol
- the 1720 destination port

The source and destination wildcard/masks would both be set to “any,” and you would not specify the WLAN index.

Perhaps your Wireless Edge Services zl Module places all wireless traffic in the same VLAN, VLAN 16. However, one WLAN grants guests access, and you want to prohibit guest access to VLAN 2, which include servers holding sensitive information.

When you configure the extended IP ACL to control traffic that arrives on the VLAN 16 interface, add a rule that does the following:

- denies traffic destined to the VLAN 2 subnetwork
- specifically selects traffic from the guest WLAN

Make sure that this rule has a lower precedence order than any rule that permits traffic to VLAN 2.

As you configure ACLs, remember that they always have an implicit “deny any” operation at the end; any traffic not specifically permitted by the rules within an ACL will be denied.
Configuring ACLs

To configure an ACL, you must complete these steps:

1. Create the list and select the ACL type.
2. Create a series of ordered permit, deny, or mark rules.
3. Apply the list to an interface.

Do not complete the final step if you are using a standard IP ACL for a function other than controlling traffic. These functions include:

- **NAT**—The ACL selects traffic for dynamic source NAT; you specify the ACL in the NAT configuration. See Chapter 8: “Configuring Network Address Translation (NAT).”
- **secure Network Time Protocol (NTP)**—The ACL selects which hosts are allowed to send specific types of NTP communications. See “Applying ACLs to NTP Services” on page 2-146 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”

Creating ACLs

To create an ACL, complete these steps:

1. Select **Security > ACLs > Configuration.**
2. Click the **Add** button. The **Add ACL** screen is displayed. (See Figure 7-2.)
Access Control Lists (ACLs)
Configuring ACLs

3. In the **ACL Type** field, use the drop-down menu to select either the standard IP, extended IP, or MAC extended ACL type.

4. In the **ACL ID** field, specify the ACL ID, which uniquely identifies the ACL. ACL IDs can be either an ASCII string or a numeric value. Follow these rules:
   - String names for ACL IDs can contain alphanumeric characters as well as the hyphen (-) and underline (_) characters; spaces are not allowed, but other special characters are.
   - Valid numeric ACL IDs depend on the ACL type; use the range of values listed in Table 7-2.

**Table 7-2. ACL Types and ACL ID Ranges**

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>ACL ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard IP access list</td>
<td>1-99 and 1300-1999</td>
</tr>
<tr>
<td>Extended IP access list</td>
<td>100-199 and 2000-2699</td>
</tr>
<tr>
<td>MAC extended access list</td>
<td>Any number outside of the ranges 1-199 and 1300-2699</td>
</tr>
</tbody>
</table>

The numeric value of the ACL ID does not affect the precedence of ACLs. However, precedence is important for the rules inside of a particular ACL; you will set these precedence values later when you configure ACL rules.
5. Click the OK button. The ACL is now listed in the ACLs section of the Security > ACLs > Configuration screen.

![Security > ACLs](image)

**Figure 7-3. Security > ACLs > Configuration with ACL**

**Configuring Rules for ACLs**

After you create an ACL, you must add rules to it. These rules actually select and control the traffic.

For each ACL rule, you must specify the following:

- the rule's precedence
- the operation (deny, permit, or mark) that the Wireless Edge Services zl Module performs on selected packets
- the filters that select a packet or frame according to fields in the header

You can configure up to 500 rules for each ACL, no matter what its type.
Creating Rules for Standard IP ACLs

The standard IP ACL offers a variety of options for rules. However, some of these options only take effect on certain interfaces. As you create the rule, keep in mind the interface for which you are designing this ACL. In Table 7-3, an X under the interface means that the option is supported for that interface.

Table 7-3. Valid Options for Standard IP ACLs Depending on Interface

<table>
<thead>
<tr>
<th>Option</th>
<th>VLAN/Tunnel Interface</th>
<th>Uplink Port</th>
<th>Downlink Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>permit operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mark operation</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>source IP address and mask</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WLAN index</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

To create a rule for a standard IP ACL, complete these steps:

1. On the **Security > ACLs > Configuration** screen, in the **ACLs** section, select a standard IP ACL.
2. Click the **Add** button under **Associated Rules**. The **Add Rule** screen is displayed.
3. In the **Precedence** field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services zl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on), in case you need to insert new rules “between” existing rules later.

4. In the **Operation** field, use the drop-down menu to select the operation (**deny**, **permit**, or **mark**) for the rule.

**Note**

The mark operation *only* takes effect if you apply this ACL to a physical interface.

5. Optionally, check the **Logging** box to allow the module to keep track of the number of packets matched to this rule.
Access Control Lists (ACLs)
Configuring ACLs

6. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255. Standard DSCP values are from 0 through 63.

   Remember that higher values typically mark traffic for better QoS.

7. In the **Source Wildcard/Mask** field, use the drop-down menu to select one of the following:
   - **any**—The rule will apply to traffic from any IP address. (This allows you to filter traffic based on fields other than the source IP address.)
   - **host**—The rule will apply specifically to a single source IP address. Enter this address in the **Source Address** field.
   - **numbers 1 through 31**—The rule selects traffic from an entire subnetwork with the specified prefix length. Enter the subnetwork’s network address in the **Source Address** field.

   For example, you select **24** in the **Source Wildcard/Mask** field and **192.168.8.0** in the **Source Address** field. The rule matches only the first 24 bits (three octets) of source IP addresses against the specified source address. Any packet from the 192.168.8.0/24 subnetwork is selected.

8. If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the **Wlan Index** field, specify the index number (from 1 through 256) of the WLAN from which traffic must arrive.

   If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.

   **Note**

   The WLAN filter *only* takes effect if you apply this ACL to a physical interface. However, you should *never* specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not typically marked for a WLAN, so the rule will not select any traffic.

9. Click the **OK** button to apply the rule.

   The rule is now listed in the **Associated Rules** section of the Security > ACLs > Configuration screen (when the corresponding ACL is selected).

   Remember to click the **Save** link to preserve the configuration.
Creating Rules for Extended IP ACLs

Configuring rules for an extended IP ACL is similar to configuring rules for standard IP ACLs. However, these rules can also select traffic by protocol, application, and destination IP address.

Refer to Table 7-4 to verify that a particular option is supported for the interface to which you plan to apply the ACL. An X under the interface means that the option is supported for that interface.

Table 7-4. Valid Options for Extended IP ACLs Depending on Interface

<table>
<thead>
<tr>
<th>Option</th>
<th>VLAN/Tunnel Interface</th>
<th>Uplink Port</th>
<th>Downlink Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>permit operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mark operation</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>source IP address and mask</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>destination IP address and mask</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>protocol</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>protocol options</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>WLAN index</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

To create a rule for an extended IP ACL, complete these steps:

1. On the Security > ACLs > Configuration screen, in the ACL section, select an extended IP ACL.
2. Click the Add button under Associated Rules. The Add Rule screen is displayed.
3. In the **Precedence** field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services zl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on) in case you need to insert new rules in between existing rules later.

4. In the **Operation** field, use the drop-down menu to select the operation (**deny**, **permit**, or **mark**) for the rule.
Note

The mark operation *only* takes effect if you apply this ACL to a physical interface.

5. Optionally, check the **Logging** box to allow the module to keep track of the number of packets matched to this rule.

6. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255.
     Standard DSCP values are from 0 through 63.

   Remember that higher values typically mark traffic for better QoS.

7. Under **Filter**, use the **Protocol** drop-down menu to select the protocol:
   - **icmp**
   - **ip**
   - **tcp**
   - **udp**

   The ACL rule matches traffic that uses the specified protocol. You can make the filter more specific than the protocol alone. That is, if you choose **icmp**, **tcp**, or **udp**, you should specify protocol options that select *certain types* of ICMP, TCP, or UDP traffic, based on information in the respective protocol header. If you select **ip**, the rule selects any IP packet that matches other filters, and you cannot specify special protocol options.

8. If you selected **icmp**, **tcp**, or **udp** in step 7, click the **Protocol Options** button.
   a. If you selected the ICMP protocol, the **ICMP Options** screen is displayed. (See step b on page 7-21 if you selected the TCP or UDP protocol.)

---

**Figure 7-6. ICMP Options Screen**
The **ICMP Type** and **ICMP Code** settings are based on the first 16 bits of the 32-bit ICMPv6 message packet, illustrated in Figure 7-7.

<table>
<thead>
<tr>
<th>ICMP Type</th>
<th>Type Description</th>
<th>ICMP Code</th>
<th>Code Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination Unreachable message</td>
<td>0</td>
<td>No route to destination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Communication with destination</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>administratively prohibited</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>(Not assigned)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Address unreachable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Port unreachable</td>
</tr>
<tr>
<td>2</td>
<td>Packet Too Big message</td>
<td>0</td>
<td>Set to 0 by the sender and ignored by</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the receiver</td>
</tr>
</tbody>
</table>

Click the **OK** button to return to the **Add Rule** screen and finish configuring other filters.
b. If you selected the TCP or UDP protocol, the TCP/UDP Options screen is displayed. Specify the source and destination ports for selected traffic in the respective Source Options and Destination Options sections:
   – Use the drop-down menu to select Equals (for one specific port) or Range (for a range of ports).
   – Enter the port number in the field beneath the drop-down menu.

Valid values are from 1 through 65,535. As shown in Figure 7-8, if you select Range, you must enter two port numbers: one for the low end of the range and one for the high end. The range is inclusive.
Access Control Lists (ACLs)
Configuring ACLs

You do not have to specify both source and destination ports. Set the destination port to control traffic associated with a particular VLAN. For example, set the destination port to 80 to select HTML traffic.

Click the OK button to return to the Add Rule screen and finish configuring other filters.

9. In the Source Wildcard/Mask field, use the drop-down menu to select one of the following:
   - any—The rule will apply to traffic from any IP address. (This allows you to filter traffic based on fields other than the source IP address.)
   - host—The rule will apply specifically to a single source IP address. Enter this address in the Source Address field.
   - numbers 1 through 31—The rule selects traffic from an entire subnetwork with the specified prefix length. Enter the subnetwork's network address in the Source Address field.

   For example, you select 24 in the Source Wildcard/Mask field and 192.168.8.0 in the Source Address field. The rule matches only the first 24 bits (three octets) of source IP addresses against the specified source address. Any packet from the 192.168.8.0/24 subnetwork is selected.

10. In the Destination Wildcard/Mask and Destination Address fields, specify the destination address for selected traffic in the same way that you specified the source address.

11. If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the Wlan Index field, specify the index number (from 1 through 256) of the WLAN from which traffic must arrive.

   If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.

   **Note**

   The WLAN filter only takes effect if you apply this ACL to a physical interface. You should never specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not marked for a WLAN, so the rule will not select any traffic.

12. Click the OK button to apply the rule.

   The rule is now listed in the Associated Rules section of the Security > ACLs > Configuration screen (when the corresponding ACL is selected).

   Remember to click the Save link to preserve the configuration.
Creating Rules for MAC Extended ACLs

To create a rule for a MAC extended ACL, complete these steps:

1. On the Security > ACLs > Configuration screen, in the ACL section, select a MAC extended ACL.

2. Click the Add button under Associated Rules. The Add Rule screen is displayed.

![Add Rule Screen for MAC Extended ACLs](image-url)

Figure 7-9. Add Rule Screen for MAC Extended ACLs
3. In the **Precedence** field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services zl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on) in case you need to insert new rules in between existing rules later.

4. In the **Operation** field, use the drop-down menu to select the operation (**deny**, **permit**, or **mark**) for the rule.

5. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255. Standard DSCP values are from 0 through 63.

Remember that higher values typically mark traffic for better QoS.

6. In the **Source Wildcard** field, type one of the following:
   - **any**—The rule will apply to traffic sent from any device. (This allows you to filter traffic based on fields other than the source MAC address.)
   - **host**—The rule will apply to traffic from a specific device only. Enter this device's MAC address in the **Source Address** field.
   - MAC address mask—The rule will apply to a range of MAC addresses. Enter the mask in standard six-octet MAC address format (XX-XX-XX-XX-XX-XX, in which you replace “Xs” with “Fs” to match octets and “0s” to ignore the bit).

   Then enter a MAC address in the **Source Address** field.

   For example, you enter a MAC address mask of FF-FF-FF-00-00-00 and an address of 00:C0:49:00:00:00. The rule matches source MAC addresses to the first three octets and ignores the next three octets.

7. In the **Destination Wildcard** and **Destination Address** fields, specify the destination MAC address or addresses. Use the same rules discussed in the previous step.

8. If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the **Wlan Index** field, specify the index number (from 1 through 256) of the WLAN from which traffic must arrive.

   If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.
You should *never* specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not marked for a WLAN, so the rule will not select any traffic.

9. Optionally, check the box to filter frames according to the following criteria:
   - **Vlan ID**—Select traffic with the specified VLAN ID
     Valid values range from 1 through 4,095.
   - **802.1p Priority**—Select traffic with the specified QoS class.
     Valid values range from 0 through 7.
   - **Ethertype**—Select traffic according to the encapsulated protocol. Use the drop-down menu to select:
     - **IPv4**—Internet Protocol, version 4
     - **ARP**—Address Resolution Protocol
     - **RARP**—Reverse Address Resolution Protocol
     - **AppleTalk**
     - **AARP**—AppleTalk Address Resolution Protocol
     - **802.1q**—VLANs
     - **IPX**—Internetwork Packet Exchange
     - **IPv6**—Internet Protocol, version 6

10. Click the OK button to apply the rule.

### Modifying ACL Rules

You might need to change a rule to fix a mistake or to respond to changing policies. To modify an ACL rule, complete these steps:

1. Select **Security > ACLs > Configuration**.
2. Select the ACL in the **ACLs** section.
3. Select the ACL rule in the **Associated Rules** section.
4. Click the **Edit** button. The **Edit Rule** screen is displayed.
5. Make the necessary changes.
6. Click **OK**.

The edited rule replaces the old rule in the **Associated Rules** section.
Applying ACLs to Interfaces

An ACL does not take effect on the Wireless Edge Services Z1 Module until you apply it to an interface. Although you can create and configure many ACLs, you are limited in the number of ACLs that you can apply:

- You can apply one IP ACL to each logical (VLAN or tunnel) interface. See “IP Settings” on page 6-3 in Chapter 6: “IP Services—IP Settings, DHCP, and DNS” to learn how to create a VLAN interface.
- You can apply one IP ACL and one MAC extended ACL to the module’s internal uplink port.
- You can apply one IP ACL and one MAC extended ACL to the module’s internal downlink port.

The Wireless Edge Services Z1 Module filters all traffic that is inbound to a physical (uplink or downlink) port with the ACLs applied to those ports.

On the other hand, the module filters only traffic that is inbound to a logical (VLAN or tunnel) interface and routed to another interface.

Packets inbound to a VLAN or tunnel interface include:

- packets from the wireless network that have been mapped to that interface
- packets from the wired network that arrive on that interface

The Wireless Edge Services Z1 Module has already added the Ethernet header to traffic that has been mapped to a logical (VLAN or tunnel) interface. For this reason, the following rules only take effect on ACLs applied to a physical port:

- marking traffic with an 802.1p or DSCP value
- filtering traffic according to WLAN

If you have configured these options in a rule, that portion of the rule does not take effect. Other options in the rule take effect normally.

To associate an ACL with an interface, complete these steps.

1. Select Security > ACLs and click the Attach tab.
2. Click the **Add** button. The **Add ACL Association** screen is displayed.
3. From the **Interface** drop-down menu, select one of the following interfaces:
   - **uplink**—the module’s internal uplink port
   - **downlink**—the module’s internal downlink port
   - an uplink VLAN configured on the module

4. Select the ACL to control incoming traffic on the selected interface. The options available depend on the type of interface:
   - For VLAN interfaces, select an IP-type ACL from the **IP ACL** drop-down menu.
   - For an uplink or downlink port, you can select ACLs from either the **IP ACL** drop-down menu, the **MAC ACL** drop-down menu, or both.

   When you apply both types of ACLs, the Wireless Edge Services zl Module processes the MAC extended ACL first, so a rule in the MAC ACL always takes precedence over a rule in the IP ACL. However, if a frame is not selected by any of a MAC extended ACL’s explicit rules, the module sends the frame to be processed by the IP ACL.

5. Click the **OK** button to apply the ACL.

6. Click the **Save** link to preserve your configuration.

**Using ACLs with DHCP Services**

An ACL filters all traffic as soon as it arrives on the interface to which the ACL is applied. Remember that most wireless stations have no IP address until they receive one through DHCP. If you have applied an ACL to the VLAN (or tunnel) associated with a WLAN, the module might drop stations’ DHCP requests before they have the chance to receive a valid address.

To avoid problems, check all ACLs that filter traffic on a interface on which DHCP requests might arrive: these ACLs must include a rule that permits those requests. The best way to meet this requirement is to create an extended IP ACL for the VLAN (or tunnel) in question and add a rule that permits any UDP traffic destined to the DHCP server port (67).
Viewing ACL Statistics

You should check ACLs and verify that they are selecting traffic as they should.

To view statistics for your ACLs, select Security > ACLs and click the Statistics tab. You can alternatively select Security > ACL Statistics.

ACL statistics are displayed on the screen. (If you do not see any statistics, you may need to edit your rules and check the Logging box.)

Each row provides information about one ACL rule:

- **Interface**—the interface to which the ACL rule is applied (uplink, downlink, VLAN, or tunnel interface)
- **Action**—whether the module forwards selected packets or drops them

Refer to Table 7-6 for a key to the action ID.
Access Control Lists (ACLs)

Configuring ACLs

Table 7-6. Action IDs for ACL Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>drop—a deny rule</td>
</tr>
<tr>
<td>3</td>
<td>forward—a permit or mark rule</td>
</tr>
</tbody>
</table>

- **Protocol**—protocol for selected packets

Table 7-7 provides a key for the protocols.

Table 7-7. Protocol IDs for ACL Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>IP</td>
</tr>
<tr>
<td>1</td>
<td>ICMP</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
</tr>
</tbody>
</table>

- **Low Source IP**—the lowest source IP address specified for the rule
- **High Source IP**—the highest source IP address specified for the rule
- **Low Destination IP**—the lowest destination IP address specified for the rule (always 0.0.0.0 for standard ACLs)
- **High Destination IP**—the highest destination IP address specified for the rule (always 0.0.0.0 for standard ACLs)
- **Times Used**—the number of times that the Wireless Edge Services zl Module has applied the ACL rule to traffic

The counter increments when the module drops a denied packet or when permits the first packet in a session. The Wireless Edge Services zl Module support stateful ACLs, which means that it automatically allows all traffic in the session.

Check this column periodically to ensure that ACL rules are affecting traffic. If not, you might need to reconfigure ACLs to make them more relevant to your network. You can also check for a deny rule that filters out traffic that should be allowed.

To view detailed statistics for a specific interface, select the interface and click the **Details** button. The **Details** screen is displayed.
In addition to the information that you viewed on the Security > ACLs > Statistics screen, you can monitor the traffic associated with this rule. **Total Flows** reports the total number of sessions established using this rule and typically matches the value for **Times Used**. **Active Flows** shows how many of those sessions are still active. Look at **Packets in** and **Packets out** to monitor how much total traffic this rule has permitted.

The **Rule Precedence** value is based on the precedence value you choose for the rule; however, it is displayed differently. The Wireless Edge Services zl Module processes rules with a **high** rule presentness first.

Click the **Refresh** button to update the statistics, and click the **Close** button to close the window.

On the main Security > ACLs > Statistics screen, you can export statistical information about a specific rule. Select the rule and click the **Export** button. On the screen that is displayed, specify the destination filename and location.

The logged information is saved to a comma-separated values (CSV) file on your workstation, which lets you monitor activity and looks for signs of possible security issues or problems with traffic flow.
Access Control Lists (ACLs)
Configuring ACLs
# Configuring Network Address Translation (NAT)

## Contents

- Overview .............................................. 8-3
- Translating Between an Inside and an Outside Network ........ 8-3
- Local and Global Addresses ............................. 8-4
- NAT Implementation Methods ......................... 8-5
  - Dynamic, or Many-to-One, NAT ......................... 8-5
  - Dynamic NAT for Wireless Traffic .................... 8-5
  - Dynamic NAT for Wired Traffic ....................... 8-7
  - Port Address Translation for Dynamic NAT .......... 8-8
- Static, or One-to-One, NAT ............................ 8-8
  - Static NAT on Destination Addresses ................. 8-9
  - Using Port Forwarding with Static Destination NAT ... 8-10
  - Static NAT on Source Addresses ...................... 8-12
- Understanding Local and Global Addresses ............... 8-12
- Planning the NAT Configuration ....................... 8-15
  - Consider Your Company’s Requirements for NAT ... 8-15
  - Record Necessary IP Addresses and Select the NAT Implementation Method .......... 8-17
    - Planning the Configuration for Dynamic NAT ... 8-17
    - Planning the Configuration for Static NAT ....... 8-19
Configuring Network Address Translation (NAT)

Contents

Configuring Standard ACLs for Dynamic NAT......................... 8-22
Configuring NAT ....................................................... 8-24
   Defining Interfaces as Outside or Inside ...................... 8-24
   Configuring Dynamic NAT ...................................... 8-26
   Configuring Static Translation ............................... 8-29
      Configuring Static Source NAT ......................... 8-30
      Configuring Static Destination NAT ................... 8-33
   Viewing NAT Status ......................................... 8-38
Overview

You can configure the ProCurve Wireless Edge Services zl Module to perform Network Address Translation (NAT) on traffic routed between two subnetworks—typically, traffic exchanged between the wireless and the wired network. The module can translate either the source or the destination IP address in a packet’s IP header to a new address.

The Wireless Edge Services zl Module allows you to implement NAT in several different ways. For example, you can configure the module to use a single IP address as the source address for an entire group of wireless stations when these stations transmit data to a wired network. This implementation of NAT allows users whose wireless stations have private IP addresses to access the Internet using one public IP address. NAT also adds another layer of security by concealing the actual IP addresses of wireless devices from users in the wired network.

Translating Between an Inside and an Outside Network

When implementing NAT, the Wireless Edge Services zl Module distinguishes between an inside and an outside network, and implements NAT at the border between the two networks.

When you configure NAT, you define the inside and outside networks by specifying if a given virtual LAN (VLAN) interface is inside or outside. For example, in Figure 8-1, wireless LAN (WLAN) A is assigned to VLAN 8, which has been defined as an inside interface. On the other hand, VLAN 4, which is used in the Ethernet LAN, is defined an outside interface.

The setting you select for a particular VLAN—either inside or outside—depends on how you implement NAT. (The options for implementing NAT are described in “NAT Implementation Methods” on page 8-5.)
Configuring Network Address Translation (NAT)

Overview

The Wireless Edge Services zl Module always performs NAT on traffic as the traffic arrives on an interface. Because the module can apply NAT to both inside and outside interfaces, it can perform NAT in both directions.

**Note**

When the Wireless Edge Services zl Module maps wireless traffic to a VLAN, that traffic is considered to have arrived on the VLAN interface.

**Local and Global Addresses**

In addition to identifying inside and outside networks, the Wireless Edge Services zl Module distinguishes between an IP address as it appears before and after translation. The Web browser interface and the command line interface (CLI) use two terms to make this distinction:

- **local IP address**—the IP address as it appears before translation
- **global IP address**—the IP address as it appears after translation

As mentioned earlier, the Wireless Edge Services zl Module translates the IP address in a packet’s IP header. Depending on how you implement NAT, the module can translate a packet’s source IP address or its destination IP address.
NAT Implementation Methods

On the Wireless Edge Services zl Module, you can configure:

- dynamic NAT
- static NAT

Dynamic NAT affects only source IP addresses while static NAT can translate either source or destination IP addresses.

Dynamic, or Many-to-One, NAT

Perhaps the most common implementation of NAT is dynamic NAT, sometimes called many-to-one NAT because it allows multiple stations to share the same IP address after translation. Dynamic NAT applies only to source IP addresses.

You define dynamic NAT using the following specifications:

- access control lists (ACLs), which select the source IP addresses of traffic on which the Wireless Edge Services zl Module performs NAT
- a Wireless Edge Services zl Module interface, which defines the IP address to which the source address is translated

This NAT method is considered dynamic because when you modify an ACL or interface, the corresponding NAT definition is modified accordingly.

You can apply dynamic NAT to traffic that arrives on inside interfaces, on outside interfaces, or on both. The sections below discuss some uses for dynamic NAT for wireless traffic and for wired traffic. (Whether configuring NAT on wireless traffic requires inside or outside NAT depends on how you define the VLAN interface in which the module places wireless traffic.)

Dynamic NAT for Wireless Traffic

Implementing dynamic NAT on wireless traffic allows you to create VLANs for wireless traffic only. The Wireless Edge Services zl Module assigns WLAN traffic to a VLAN reserved for wireless stations; its internal DHCP server issues wireless stations IP addresses in this VLAN. Before routing wireless traffic into the Ethernet network, the module translates these local DHCP addresses to an IP address valid in the wired network—the module's own.

This implementation also has the advantage of conserving IP addresses: instead of each wireless station having its own IP address that is valid in the wired network, all wireless stations share the Wireless Edge Services zl Module’s address.
Figure 8-2 illustrates this configuration, which allows wireless stations to use IP addresses local to the wireless network but still to open sessions with servers in the Ethernet network.

You can also implement NAT on the module to ready wireless traffic for transmission to the Internet—if you do not have another device that does so. Many companies have only one public IP address although they have many employees who need Internet access. With dynamic NAT, all these employees can share one IP address. When users on the company's wireless network send requests to the Internet, the Wireless Edge Services zl Module translates the senders' local IP addresses to a global address—the module's IP address in the wired network. After translating packets' source IP addresses, the module forwards the requests onto the Ethernet network and toward the Internet.
Dynamic NAT for Wired Traffic

You can configure dynamic NAT for traffic bound from the wired network to the wireless network. In this case, the Wireless Edge Services zl Module translates wired devices’ IP addresses to one of the module’s own IP addresses.

You might use dynamic NAT on wired traffic when your wireless network receives a great deal of public traffic. You can then conceal the IP addresses of devices in your private network from the wireless users. (See Figure 8-3.)

![Dynamic Source NAT](image)

**Figure 8-3. Dynamic Source NAT**

Again, whether you apply dynamic NAT to inside or outside traffic depends on how you have defined interfaces. In this example, you have defined the VLAN used in the wired network as an outside interface, so you configure outside dynamic NAT.

If you want to allow wireless users to access internal servers, you must configure destination NAT to translate the publicly known IP address back to the servers’ internal addresses. (See “Static NAT on Destination Addresses” on page 8-9.)
In fact, instead of configuring dynamic source NAT to conceal private addresses, you might want to configure only destination NAT. The Wireless Edge Services zl Module automatically performs source NAT on the traffic returning from the server.

Port Address Translation for Dynamic NAT

To enable multiple users to share one IP address, the Wireless Edge Services zl Module uses port address translation in conjunction with NAT. When the module translates a local IP address to a global address, it assigns each local address a unique port number, as shown in Table 8-1.

The Wireless Edge Services zl Module uses this port number to forward return traffic, which is destined to the single global IP address, to the correct local IP address. For example, Table 8-1 lists possible IP address for the network shown in Figure 8-3. In this case, the module translates all inside addresses (in the 192.168.1.0/24 subnetwork) to 10.1.1.1. If a packet arrives for 10.1.1.1 on port 4001, the module knows to forward the packet toward the station at 192.168.1.11.

<table>
<thead>
<tr>
<th>Local IP Address</th>
<th>Translated (Global) IP Address</th>
<th>Translated Port</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>10.1.1.1</td>
<td>4000</td>
<td>10.20.1.1</td>
<td>80</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>10.1.1.1</td>
<td>4001</td>
<td>172.16.1.10</td>
<td>80</td>
</tr>
<tr>
<td>192.168.1.12</td>
<td>10.1.1.1</td>
<td>4002</td>
<td>172.16.10.5</td>
<td>80</td>
</tr>
<tr>
<td>192.168.1.13</td>
<td>10.1.1.1</td>
<td>4003</td>
<td>10.45.16.1</td>
<td>80</td>
</tr>
<tr>
<td>192.168.1.14</td>
<td>10.1.1.1</td>
<td>4004</td>
<td>172.16.11.1</td>
<td>80</td>
</tr>
</tbody>
</table>

Static, or One-to-One, NAT

You can also configure static definitions for NAT. In this case, you manually specify the following information for each one-to-one NAT:

- the IP address (and optionally, port) that should be translated
- the IP address (and optionally, port) that should replace the original address

The Wireless Edge Services zl Module can perform static translation on both source IP addresses and destination IP addresses. In addition, it can apply NAT to traffic inbound from the inside network or from the outside network.
Static NAT on Destination Addresses

One reason to use destination NAT is to allow wireless users to access servers on your internal LAN, while still concealing the servers’ IP addresses. This use is particularly important when you open your wireless network to the public. Because this wireless network is much like the Internet—filled with untrusted users—you should implement the same types of security measures that you put in place for users who access your network from the Internet.

Configure destination NAT to allow wireless users to send traffic toward a server’s publicly known address. The Wireless Edge Services zl Module translates the traffic’s destination address to the correct local address. When the server replies, the module automatically translates the source address back to the address to which the traffic was originally destined, and the private address remains concealed.

For example, your company may have a Web server or an FTP server, which is housed on your internal LAN. To access this server, wireless users enter a URL, which is resolved through a Domain Name System (DNS) server to a public IP address. When your Wireless Edge Services zl Module receives a packet destined to this address, it translates the destination IP address and forwards the packet toward the correct internal device.

For example, in Figure 8-4, a Web server on the internal LAN has an IP address of 192.168.1.10. However, the IP address to which wireless stations send traffic is 10.1.1.1. When the ProCurve Wireless Edge Services zl Module receives packets with the destination address of 10.1.1.1, it translates the destination address to the private IP address of the Web server: 192.168.1.10. The source IP address is not affected. (See Figure 8-4.) Therefore, you must ensure that devices in the wired network can route traffic back to the subnetwork used in the wireless network.
Configuring Network Address Translation (NAT)

Overview

One principle to remember: on the Wireless Edge Services zl Module, you define which VLANs are inside interfaces and which are outside. Figure 8-4 shows a configuration in which the VLAN used in the Ethernet network is an outside interface. So you configure the destination NAT on inside interfaces (these interfaces receive traffic that is destined to the outside VLAN).

As mentioned earlier, you can apply destination NAT to traffic from both the inside and the outside network. In theory, you could also apply destination NAT to traffic being sent from the wired network to the wireless network. However, destination NAT is typically used to allow servers to share a public IP address and to conceal their private addresses. Your wireless network is unlikely to include such servers, so you would probably set up destination NAT in one direction.

Using Port Forwarding with Static Destination NAT

The Wireless Edge Services zl Module also supports port forwarding for static destination NAT. Port forwarding allows two or more devices on a network to share a single IP address known in the other network. For example, you could have wireless users send traffic that is destined to two different servers to the same IP address:

- your LAN's Web server
- your LAN's FTP server

Figure 8-4. Outside Destination NAT
The Wireless Edge Services zl Module would then translate the destination IP addresses of all traffic destined to port 80 to the Web server’s private IP address (the address on wired network). Likewise, the module would translate all traffic destined to port 21 to the FTP server’s private IP address.

Figure 8-5. Outside Destination NAT with Port Forwarding
Configuring Network Address Translation (NAT)
Overview

When the module translates the destination IP address, it can also perform port translation, assigning the traffic to the particular port used by the destination device.

Static NAT on Source Addresses

Static source NAT is an alternative to dynamic source NAT. However, instead of allowing many stations to share one global address, static source NAT sets up a one-to-one correspondence between a particular IP address and a translated IP address. Use this option only when relatively few devices in one network (inside or outside) need to access devices in the other network.

Understanding Local and Global Addresses

When you configure NAT on the Wireless Edge Services zl Module, you define a local address and a global address. As mentioned earlier, the local address is the pre-translation address. For source NAT, the local address is always the IP address assigned to the device for the network in which the device resides. In Figure 8-6, the local address is any address used by a device in WLAN A—the 10.1.1.0/24 subnetwork.
However, for destination NAT, the local address is actually the address as it appears across the border between inside and outside. This is because packets, pre-translation, are destined to the IP address that the originating station knows for the destination device, not the destination's actual IP address. In Figure 8-5 on page 8-11, for example, the local address is 10.1.1.1.

Table 8-2 summarizes this terminology.
### Table 8-2. Terminology for IP Addresses According to NAT Implementation

<table>
<thead>
<tr>
<th>NAT Interface Type (Inside or Outside)</th>
<th>NAT Address Type</th>
<th>Address</th>
<th>Explanation of Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside</td>
<td>Source</td>
<td>Local</td>
<td>An inside station’s IP address as it appears on the inside network</td>
</tr>
<tr>
<td>Inside</td>
<td>Source</td>
<td>Global</td>
<td>An inside station’s IP address as it appears on the outside network</td>
</tr>
<tr>
<td>Inside</td>
<td>Destination</td>
<td>Local</td>
<td>An outside station’s IP address as it appears on the inside network</td>
</tr>
<tr>
<td>Inside</td>
<td>Destination</td>
<td>Global</td>
<td>An outside station’s IP address as it appears on the outside network</td>
</tr>
<tr>
<td>Outside</td>
<td>Source</td>
<td>Local</td>
<td>An outside station’s IP address as it appears on the outside network</td>
</tr>
<tr>
<td>Outside</td>
<td>Source</td>
<td>Global</td>
<td>An outside station’s IP address as it appears on the inside network</td>
</tr>
<tr>
<td>Outside</td>
<td>Destination</td>
<td>Local</td>
<td>An inside station’s IP address as it appears on the outside network</td>
</tr>
<tr>
<td>Outside</td>
<td>Destination</td>
<td>Global</td>
<td>An inside station’s IP address as it appears on the inside network</td>
</tr>
</tbody>
</table>
Planning the NAT Configuration

Before you access the Security > NAT screen and begin to set up NAT for your wireless network, you should plan your configuration:

1. Consider your company’s network topology and security needs and determine the requirements for NAT.
   In other words, which NAT methods do you need to configure, and which traffic should be translated.
2. Record the IP addresses necessary for your NAT configuration.
3. If you are using dynamic NAT, configure the necessary standard ACLs.

The following sections outline these steps in more detail.

Consider Your Company’s Requirements for NAT

The Wireless Edge Services zl Module supports a variety of options for NAT. Use the following scenarios to determine which options you must configure:

- You want to assign wireless stations to VLANs reserved for wireless traffic (either for security or to conserve IP addresses on your LAN or both). All wireless stations will share a single IP address in your LAN—an address used by the Wireless Edge Services zl Module.

  Assign the WLAN to a VLAN not used in the Ethernet network. Use DHCP to assign addresses to wireless stations in that VLAN. (See Chapter 6: “IP Services—IP Settings, DHCP, and DNS.”)

  Define the VLAN in which the Wireless Edge Services zl Module places wireless traffic as an inside VLAN and configure dynamic NAT on inside traffic. Or, define the VLAN as an outside VLAN and configure dynamic NAT on outside traffic. (For the exact configuration steps, see “Configuring Dynamic NAT” on page 8-26.)

- You want to prepare wireless traffic for transmission on the Internet.

  This scenario is similar to the above. Define VLANs associated with wireless traffic as inside VLANs and configure dynamic NAT on inside traffic. Make sure that your Wireless Edge Services zl Module has a valid public IP address and can reach your Internet Service Provider’s (ISP’s) router.
You want to conceal IP addresses used in your LAN from wireless users.

Separate the VLANs for wired traffic from the VLANs for wireless traffic: When you specify the uplink VLANs in which the Wireless Edge Services zl Module places traffic from WLANs, choose different VLANs from those already used in the wired network.

Next, define the wired VLANs as inside interfaces and define the wireless VLANs as outside interfaces.

Configure static destination NAT on outside traffic. Each static destination NAT definition allows you to map a global IP address and destination port to a particular address used in your internal network, typically that of network servers. Create a different NAT definition for each server in the Ethernet network that users in the wireless network must access.

**Note**

The Wireless Edge Services zl Module performs at most one type of NAT on a packet. Therefore, you should typically configure source NAT for either inside or outside interfaces.

For example, your internal (wired) network might use VLAN 2, and the module might perform dynamic source NAT on all traffic from that VLAN, translating the addresses used on the Ethernet network to the module’s address on the wireless network. You might also configure static destination NAT for wireless traffic destined to certain wired servers.

Configuring dynamic NAT for wireless traffic would have no effect on traffic destined to the wired resources: when the module translates an outside packet’s destination address, it does not apply dynamic NAT.

Because wireless traffic enters the Ethernet network with its source address unchanged, the Ethernet infrastructure devices must know routes to the subnetwork for wireless traffic.
Record Necessary IP Addresses and Select the NAT Implementation Method

As part of your NAT planning, you should record:

- **local address**—the address or addresses that will be translated
- **global address**—the address that will replace the local address when the module applies NAT

You should also determine which NAT implementation method you are using. For example, if you want to conserve IP addresses on your LAN, you will probably decide to use dynamic NAT on inside traffic. If you want to allow wireless users access to private Web or FTP servers with concealed IP addresses, you will use static NAT.

Planning the Configuration for Dynamic NAT

If you are using dynamic NAT, you must use ACLs to specify which traffic the Wireless Edge Services module NATs. Consider which IP addresses these ACLs should select. For example, if you want to NAT all traffic from wireless stations in a particular WLAN, you can create an ACL that permits any IP address and specifies that particular WLAN.

You may want the Wireless Edge Services module to NAT traffic from wireless stations before that traffic enters your wired network. In this case, you would first configure the module to place wireless stations in a particular VLAN and act as a DHCP server, assigning the stations IP addresses in a corresponding subnet. Before the module forwarded this traffic to the wired network, it would NAT the traffic to a single IP address, as shown in Figure 8-7.
Configuring Network Address Translation (NAT)
Planning the NAT Configuration

Figure 8-7. Dynamic NAT on a Sample Network

For this NAT implementation, you would record the IP addresses specified in the DHCP pool and configure an ACL that selects those addresses. Table 8-3 lists the actual IP addresses that you would record for the sample network shown in Figure 8-7.

Table 8-3. Recording Addresses for Dynamic NAT on a Sample Network

<table>
<thead>
<tr>
<th>NAT Interface Type (Inside or Outside)</th>
<th>NAT Address Type</th>
<th>Local or Global Address</th>
<th>Recorded Addresses for the Sample Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside</td>
<td>Source</td>
<td>Local (stations’ IP addresses as they appear on the wireless network)</td>
<td>10.1.1.0/24 subnetwork—assigned through DHCP and specified in an ACL</td>
</tr>
<tr>
<td>Inside</td>
<td>Source</td>
<td>Global (IP address for all stations as it appears on the wired network)</td>
<td>192.168.1.10—module’s vlan 1 IP address</td>
</tr>
</tbody>
</table>
Planning the Configuration for Static NAT

For static NAT, you manually specify the IP address and port settings within each NAT configuration. You must configure a separate static definition specifically for each IP address that your Wireless Edge Services zl Module must translate.

Before configuring static destination NAT for traffic destined to network servers, collect the following information:

- the IP address that you want to advertise to wireless stations (through, for example, a DNS server)
  This will be the original destination address (local address) for incoming packets.

- the destination port for traffic that will be subject to NAT (local port) and the corresponding protocol (TCP or UDP)
  This setting is for port translation, which enables multiple internal servers to share one advertised IP address. For example, the Wireless Edge Services zl Module can select traffic destined to:
  - a Web server on port 80
  - an FTP server on port 21

- the internal device’s IP address on your LAN
  This will be the translated destination address (global address).

- the translated destination port (global port)
  This setting is also optional. If you do not specify this port, the module forwards traffic to the destination port on which it arrived.

To configure static source NAT, you must know:

- the local address to which the module must apply NAT

- the global address to which the module should translate the original address

You can optionally specify a new source port for the translated traffic.

In Figure 8-8, for example, the company wants to conceal the actual IP address of its Web server—192.168.1.25. The company has also set up its Web server to use a different port—port 51000. For this implementation, you must configure destination NAT with port translation.
In Figure 8-8, the VLAN for wireless stations is the inside interface, so the Web server is an outside device. Therefore you must set up *inside* destination NAT. You could alternatively define the Web server's VLAN as the inside interface, in which case you would configure *outside* destination NAT.

When you record the local address for destination NAT, identify the destination device’s IP address as it appears on the *source* network. On the wireless network, the Web server’s IP address appears to be 10.1.1.1. For this sample network, you would record 10.1.1.1 for the local address, as shown in Table 8-4.

When you record the global address for destination NAT, identify the inside device’s IP address as it appears in the destination network. For the sample network, the Web server’s actual IP address is 192.168.1.25. You would, therefore, record 192.168.1.25 as the global address.

Because the sample network is also using port address translation, you should record the port for the translated traffic, as shown in Table 8-4.
### Table 8-4. Recording Addresses for Outside Destination NAT

<table>
<thead>
<tr>
<th>NAT Interface Type</th>
<th>NAT Address Type</th>
<th>Local or Global Address</th>
<th>Local or Global Port</th>
<th>Recorded Addresses for the Sample Network</th>
<th>Recorded Ports for the Sample Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside</td>
<td>Destination</td>
<td>Local (outside device’s IP address as it appears on the inside network)</td>
<td>Local (port to which the inside devices originally send traffic)</td>
<td>10.1.1.1</td>
<td>80</td>
</tr>
<tr>
<td>Inside</td>
<td>Destination</td>
<td>Global (outside device’s IP address as it appears on the outside network)</td>
<td>Global (port used by the outside device)</td>
<td>192.168.1.25</td>
<td>51000</td>
</tr>
</tbody>
</table>
Configuring Standard ACLs for Dynamic NAT

To configure dynamic translation, you use a standard ACL to select the IP addresses that the Wireless Edge Services 41 Module NATs. Although you can use any ACL that you have configured, you will probably want to configure ACLs to meet the specific requirements for your NAT implementation.

Remember that depending on the types of NAT you are configuring, you might need to create several ACLs. If your module will NAT both inside and outside traffic, you must create one ACL to select IP addresses used in the inside network and one ACL that selects addresses used in the outside network.

To create ACLs, use the procedure documented in Chapter 7: “Access Control Lists (ACLs).” For NAT, you must create a standard IP ACL.

To add rules to the ACL, use the screen shown in Figure 8-9.

Figure 8-9. Add Rule Screen for Standard IP ACLs
The full procedure for adding rules to ACLs is documented in Chapter 7: “Access Control Lists (ACLs).” The following rule guidelines apply to ACLs used for NAT:

- In the Operation field, the permit operation means that traffic will be subject to NAT; the deny operation means that traffic will not be subject to NAT. (The mark operation does not apply to NAT.)
- The entries in the Filters area specify the source IP address or range of source IP addresses for which NAT will be either permitted or denied. (The Wlan Index entry is optional.)

For example, to NAT all traffic that arrives from the wireless network, you would set up a “permit any” rule. Or, to NAT all traffic from a particular subnet, the rule would specify the subnet’s IP address and subnet mask. For example, you might have mapped a particular WLAN to a VLAN, and then set up a DHCP pool for that VLAN on the Wireless Edge Services zl Module. To apply NAT to all of the wireless stations that have been assigned addresses in that VLAN, specify the VLAN’s subnet IP address and mask.

After you have created ACLs and added rules to them, you can select those ACLs when you set up NATs using dynamic translation. (See “Configuring Dynamic NAT” on page 8-26.)
Configuring NAT

To configure NAT, follow these steps:

1. Enable routing.
   
   See “IP Routing” on page 6-12 of Chapter 6: “IP Services—IP Settings, DHCP, and DNS.”

2. Define interfaces as inside or outside interfaces.
   
   When you create a NAT definition, you will select whether this definition applies to inside or outside traffic. To do so, you must know which Wireless Edge Services zl Module interfaces connect to inside networks and which to outside networks. See “Defining Interfaces as Outside or Inside” on page 8-24.

3. Configure one or both types of NATs:
   - **Dynamic translation**—based on ACLs, which permit or deny NAT based on IP addresses; as the ACL configuration changes, the NAT configuration changes as well.
   - **Static translation**—configured to specific IP addresses and ports; any configuration changes are made within the NAT configuration itself.

Defining Interfaces as Outside or Inside

NAT configurations have no effect until you map interfaces to NAT by defining particular interfaces as outside or inside. For example, when traffic arrives on an inside interface, the module applies the configurations created for inside NAT (as long as the traffic matches the specifications for that NAT definition).

**Note**

NAT applies to traffic that arrives on an interface. NAT does not affect traffic sent from an interface.

To define an interface as outside or inside, complete these steps:

1. Select **Security > NAT** and click the **Interfaces** tab.
2. Click the **Add** button. The **Add Interface** screen is displayed.

3. In the **Interfaces** field, use the drop-down menu to select an interface configured on the module.
4. In the **Type** field, use the drop-down menu to select either **Inside (Private)** or **Outside (Public)**.

5. Click the **OK** button.

The interface is now listed on the **Security > NAT > Interfaces** screen.

---

**Figure 8-12. Interface Assignment in Security > NAT > Interfaces Screen**

**Configuring Dynamic NAT**

For each NAT configuration that will use dynamic NAT, you must first set up an ACL. This ACL contains rules that select the source addresses for traffic to be translated. For information about creating this ACL, see Chapter 7: “Access Control Lists (ACLs)” and “Configuring Standard ACLs for Dynamic NAT” on page 8-22.

To configure dynamic translation, complete these steps:

1. Select **Security > NAT** and click the **Dynamic Translation** tab.
2. Click the Add button. The Add Dynamic Translation screen is displayed.
3. In the **NAT Interface** field, use the drop-down menu to select the type of interfaces to which the module applies NAT:
   - **Inside (Private)**—traffic that arrives from the inside network
     
     In other words, inside NAT applies to incoming traffic on an inside interface; typically, the inside traffic should be bound to the outside network.
     
     Internal addresses are those that you are trying to adjust for, or to conceal from, the outside world, so you will usually select this option for dynamic source NAT.
   - **Outside (Public)**—traffic that arrives from the outside network
     
     In other words, incoming traffic on an outside interface.

4. In the **NAT Address Type** field, leave the setting at **Source** (the only option permitted for dynamic translation).

   The Wireless Edge Services zl Module translates the source addresses of selected traffic.

5. In the **Access List** field, use the drop-down menu to select the ACL that you configured to select traffic.

   This ACL should permit the source addresses that you want to translate. For inside dynamic NAT, the ACL should select inside addresses as they appear locally (on the inside network). When using outside dynamic NAT, choose an ACL that selects outside address as they appear on the outside network. For example, if your outside network is a publicly used wireless network, the ACL should select traffic from the IP addresses assigned to wireless stations.

6. From the **Interface** drop-down menu, select one of the module’s VLAN or tunnel interfaces.

   The Wireless Edge Services zl Module translates the source addresses to the IP address on the specified interface. Ethernet interfaces are named vlan1, vlan2, and so on.

   If you are configuring dynamic NAT on traffic from wireless stations, make sure to choose an interface that is tagged on the module’s uplink port. In this way, return traffic from the wired network can reach the wireless stations.

   The interface you select is sometimes called the overloaded interface because many devices share its IP address.

7. Click the **OK** button.
The definition for dynamic translation is now listed on the Security > NAT > Dynamic Translation screen. Remember: the translation does not take effect unless you define an interface as the type on which you configured dynamic NAT. (See “Defining Interfaces as Outside or Inside” on page 8-24.)

<table>
<thead>
<tr>
<th>NAT Interface</th>
<th>NAT Address Type</th>
<th>Access List</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside (Private)</td>
<td>Source</td>
<td>NAT_VLAN8</td>
<td>Vlan1</td>
</tr>
</tbody>
</table>

Figure 8-15. Dynamic NAT Configuration in the Security > NAT > Dynamic Translation Screen

Configuring Static Translation

Static translation sets up a one-to-one correspondence between a source or destination IP address and a translated IP address.

The configuration steps depend on whether you configuring static source NAT or static destination NAT.
Configuring Static Source NAT

When the Wireless Edge Services zl Module stands between two networks that use different IP addresses, static source NAT allows a device in one network to reach devices in the other network. The module translates traffic’s source address so that the device that sent the traffic appears to have a valid IP address in the other network.

Note that the more typical configuration for source NAT is often dynamic NAT because it allows multiple devices to share the same translated IP address.

To configure a static source translation, complete these steps:
1. Select Security > NAT and click the Static Translation tab.

2. Click the Add button. The Add Static Translation screen is displayed.
3. In the **NAT** section, select the **Interface Type** and **Address Type**:
   a. The **Interface Type** determines to which interfaces the Wireless Edge Services zl Module applies the static NAT definition:
      - **Outside (Public)**—incoming traffic on an outside interface
      - **Inside (Private)**—incoming traffic on an inside interface
   b. For the **Address Type**, select **Source**—The module translates the packet’s source IP address.

The correct settings depend, of course, on the goal of the NAT configuration and on how you have defined interfaces in your network.

When you select **Source** for the **Address Type**, the **Interface Type** choice is relatively straightforward: choose **Inside (Private)** to apply NAT to inside devices and **Outside (Public)** to apply NAT to outside devices.

See the “Static, or One-to-One, NAT” on page 8-8 and “Planning the NAT Configuration” on page 8-15 for more guidelines on choosing these settings.

4. In the **Before Translation** section, specify the IP address of traffic to which the module should apply NAT.
   a. In the **Local Address** field, enter the IP address to be translated.
      This address depends on the choices that you made in the **NAT** section.
      Refer to Table 8-5.
Configuring Network Address Translation (NAT)

Configuring NAT

Table 8-5. Determining the IP Address for the Local Address Field

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Address Type</th>
<th>IP Address for the Local Address Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside (Private)</td>
<td>Source</td>
<td>IP address of an inside device as it appears on the inside network</td>
</tr>
<tr>
<td>Outside (Public)</td>
<td>Source</td>
<td>IP address of an outside device as it appears on the outside network</td>
</tr>
</tbody>
</table>

For example, for source NAT, enter the configured IP address assigned to a device in its own network. This address is typically allocated out of a private address space.

b. The Local Port field is not available for source NAT.

5. In the After Translation section, specify the IP address to which the Wireless Edge Services zl Module should translate the source address:

a. In the Global Address field, enter the IP address as it should appear after translation.

See Table 8-6 for guidelines on specifying this address.

Table 8-6. Determining the IP Address for the Global Address Field

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Address Type</th>
<th>IP Address for the Global Address Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside (Private)</td>
<td>Source</td>
<td>IP address of an inside device as it should appear on the outside network</td>
</tr>
<tr>
<td>Outside (Public)</td>
<td>Source</td>
<td>IP address of an outside device as it should appear on the inside network</td>
</tr>
</tbody>
</table>

Make sure to enter a valid IP address on this Wireless Edge Services zl Module. Select an address that is valid in the network to which the traffic is destined. For example, if you are configuring source NAT for a wireless device, enter an IP address on a VLAN tagged on the uplink.

b. The Global Port field is not available for source NAT. The Wireless Edge Services zl Module automatically assigns a port to the translated packet.

6. Click the OK button.

The static NAT definition is now listed on the Security > NAT > Static Translation screen. Remember: the translation does not take effect unless you define an interface as the type on which you configured static source NAT. (See “Defining Interfaces as Outside or Inside” on page 8-24.)
Configuring Network Address Translation (NAT)

Configuring NAT

Figure 8-18. Static NAT Definition in the Security > NAT > Static Translation Screen

Configuring Static Destination NAT

The Wireless Edge Services zl Module stands between two networks that use different IP addresses. Destination NAT allows clients in one network to open sessions with servers in the other network. You must configure destination NAT statically.

To configure a static destination translation, complete these steps:

1. Select Security > NAT and click the Static Translation tab.
2. Click the Add button. The Add Static Translation screen is displayed.
Configuring Network Address Translation (NAT)

Configuring NAT

3. In the **NAT** section, select the **Interface Type** and **Address Type**:
   a. The **Interface Type** determines to which interfaces the Wireless Edge Services zl Module applies the static NAT definition:
      - **Outside (Public)**—incoming traffic on an outside interface
      - **Inside (Private)**—incoming traffic on an inside interface
   b. For the **Address Type**, select **Destination**—the module translates the destination IP address in the IP header.

The correct settings depend, of course, on the goal of the NAT configuration and on how you have defined interfaces in your network.

Remember: destination NAT allows client traffic to reach servers at public IP address, and servers are typically in your wired network. If you define VLANs for wired servers as **outside** interfaces, you should define VLANs for wireless traffic as **inside** interfaces. Then select **Destination** for the **Address Type** and **Inside (Private)** for the **Interface Type**. On the other hand, you might define VLANs for wireless traffic as **outside** interfaces. In this case, select **Destination** for the **Address Type** and **Outside (Public)** for the **Interface Type**. In either case, NAT applies to traffic from wireless stations destined to wired servers.

See the “Static, or One-to-One, NAT” on page 8-8 and “Planning the NAT Configuration” on page 8-15 for more guidelines on choosing these settings.
4. Select either TCP or UDP in the Protocol drop-down menu.

This setting, which is available only for destination NAT, allows you to configure port forwarding. Choose the protocol for the application for which you are creating the NAT definition. For example, if you are setting up destination NAT to allow wireless stations to reach your Web server, select TCP.

5. In the Before Translation section, specify the IP address and port to the traffic to be translated is destined.
   a. In the Local Address field, enter the IP address to be translated.

   This address depends on the choices that you made in the NAT section. Refer to Table 8-5.

Table 8-7. Determining the IP Address for the Local Address Field

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Address Type</th>
<th>IP Address for the Local Address Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside (Private)</td>
<td>Destination</td>
<td>IP address of an outside device as it appears on the inside network</td>
</tr>
<tr>
<td>Outside (Public)</td>
<td>Destination</td>
<td>IP address of an inside device as it appears on the outside network</td>
</tr>
</tbody>
</table>

For destination NAT, the local address is actually the IP address of a host as it appears to hosts in the opposite network. So if you are using destination NAT to translate wireless requests to a wired server, enter the address known in the wireless network (typically, the Wireless Edge Services zl Module’s).

b. In the Local Port field, enter the port to which the traffic to be translated is destined. Specify a number from 1 through 65,535.

   This setting is used for port forwarding and is available only when you select Destination for the Address Type. See “Using Port Forwarding with Static Destination NAT” on page 8-10 for more information.

   For example, you are setting up NAT for traffic inbound from a public wireless network to your internal FTP server. This traffic from the public network is destined to port 21, so you enter 21 in the Local Port field.

6. In the After Translation section, specify how the Wireless Edge Services zl Module should translate the IP header:
   a. In the Global Address field, enter the IP address as it should appear after translation. In other words, enter the actual IP address of the server to which the traffic is destined.

   See Table 8-6 for guidelines on specifying this address.
In the example in which you are configuring destination NAT to allow public access to your company's FTP server, you would enter the FTP server's private address.

b. In the **Global Port** field, enter the port to which the Wireless Edge Services zl Module should forward the traffic.

This optional setting for destination NAT provides port translation.

For example, traffic arrives for your internal Web server on its public IP address and the standard HTML port 80 (which you specify in the **Local Port** field of the *Before Translation* section). The module translates the traffic to the Web server's private address and a private port, selected by your company. Enter the private address in the **Global Address** field and the private port in the **Global Port** field.

7. Click the **OK** button.

The static NAT definition is now listed on the **Security > NAT > Static Translation** screen. Remember: the translation does not take effect unless you define an interface as the type on which you configured static destination NAT. (See “Defining Interfaces as Outside or Inside” on page 8-24.)

### Table 8-8. Determining the IP Address for the Global Address Field

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Address Type</th>
<th>IP Address for the Global Address Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside (Private)</td>
<td>Destination</td>
<td>IP address of an outside device on the outside network</td>
</tr>
<tr>
<td>Outside (Public)</td>
<td>Destination</td>
<td>IP address on an inside device on the inside network</td>
</tr>
</tbody>
</table>

---
Configuring Network Address Translation (NAT)

Configuring NAT

Figure 8-21. Static NAT Definition in the Security > NAT > Static Translation Screen

Viewing NAT Status

To view current translations, select Security > NAT and click the Status tab. Alternatively, you can select Security and click the NAT Status tab. (See Figure 8-22.)
Each active session to which the Wireless Edge Services zl Module has applied NAT is displayed in a row. The screen columns show the IP addresses associated with the session:

- **Inside-Global**—the source IP address as it appears in the destination device’s network
- **Inside-Local**—the source IP address as it appears in the source device’s network
- **Outside-Global**—the destination IP address as it appears in the destination device’s network
- **Outside-Local**—the destination IP address as it appears in the source device’s network

For example, if you have configured dynamic source NAT on inside traffic, the **Inside-Local** column lists the IP address of the source device in the inside network. The **Inside-Global** column lists the translated IP address. (See the top row in Figure 8-22.)
Configuring Network Address Translation (NAT)
Configuring NAT

The number after a colon indicates the port. For example, the module has translated the source IP addresses in the first three rows to the same global source address, but different port numbers.

On the other hand, for a session using static destination NAT on outside traffic, the translation appears in the Outside-Global and Outside-Local columns. The Outside-Local column shows the IP address to which the source device actually destines the packet. The Outside-Global column shows the destination IP address after the module has translated it to the destination device’s actual address. (See Figure 8-23.)

![Security > NAT](image)

Figure 8-23. Viewing Outside NAT in the Security > NAT > Status Screen

To export statistical information about a specific session, select the row and click the Export button. On the screen that is displayed, specify the destination filename and location.
The logged information is saved to a comma-separated values (CSV) file on your workstation, which lets you:

- save information that might be important later, while keeping logs or statistics clear for future events
- send a file to support staff for troubleshooting help
- pool information from multiple devices in a central location
- track patterns of network activity
Configuring Network Address Translation (NAT)
Configuring NAT
Fast Layer 2 Roaming and Layer 3 Mobility

Contents

Overview 2
Layer 2 Roaming on a Single Wireless Edge Services zl Module . . . . . 9-2
Fast Layer 2 Roaming for WPA/WPA2 with 802.1X . . . . . . . . 9-3
Pre-authentication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-3
Layer 2 Roaming on a Web-Auth WLAN Between Different
Wireless Edge Services zl Modules . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-4
Layer 3 Mobility . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-5
Roaming Behavior . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-8
Configuring Fast Layer 2 Roaming for WPA/WPA2 with 802.1X . . . . . 9-12
Configuring Layer 3 Mobility . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-15
Configuring Layer 3 Mobility Settings . . . . . . . . . . . . . . . . . . . . . . . . . . 9-16
Specifying Layer 3 Mobility Peers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-19
Enabling Layer 3 Mobility . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-20
Verifying and Managing Layer 3 Mobility . . . . . . . . . . . . . . . . . . . . . . . . 9-22
Monitoring Peers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-22
Viewing a Station’s Status . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9-26
Overview

The type of roaming that your ProCurve Wireless Edge Services zl Modules support depends on your network topology and module configurations, as well as on other factors.

This overview has three main purposes:
- explaining when you can and should configure fast Layer 2 roaming
- explaining when Layer 3 mobility is required
- summarizing the configurations required to implement the best possible roaming behavior in various circumstances

The sections that follow the overview explain how to enable fast Layer 2 roaming and Layer 3 mobility.

Layer 2 Roaming on a Single Wireless Edge Services zl Module

The Wireless LAN System, with its coordinated AP design, facilitates fast and seamless roaming between wireless cells. A central device, the Wireless Edge Services zl Module, controls all security settings and associations with wireless stations. The module generates and encrypts 802.11 frames. In other words, the module functions much like a single, high-capability AP with many remote radios (the RPs). Therefore, when a station disassociates from one RP and reassociates with another RP adopted by the same module, the module already has in place the association, authentication, and encryption keys.

No matter which security options you have enabled on a wireless LAN (WLAN), a station can quickly roam (under 50 milliseconds) between two RPs adopted by the same module.

The Wireless Edge Services zl Module also supports 802.11i mechanisms for speeding roaming in a WLAN that requires Wi-Fi Protected Access (WPA)/WPA2 with 802.1X. These mechanisms help to speed roaming both between RPs adopted by the same module and by different modules.
Fast Layer 2 Roaming and Layer 3 Mobility

Overview

Fast Layer 2 Roaming for WPA/WPA2 with 802.1X

WPA's Temporal Key Integrity Protocol (TKIP) (and WPA2's Counter Mode CBC-MAC Protocol [CCMP]) derive encryption keys from a unique Pairwise Master Key (PMK) for each association with a wireless station. Because the PMK is necessary for the station and the Wireless Edge Services zl Module to communicate, the module must ensure that it maintains the key for a roaming station. The following mechanisms help it to do so:

- **Pairwise Master Key (PMK) caching**—Enables fast roaming back to an RP adopted by the Wireless Edge Services zl Module.

  PMK caching allows the module to store a station’s PMK after the station disassociates with one of the module’s RPs. Caching ensures that the key is still in place if the station again associates with an RP adopted by the module.

- **Opportunistic Key caching**—Facilitates fast roaming to a new RP on the local Wireless Edge Services zl Module.

  Opportunistic key caching enables the module to push PMKs down to all adopted RPs, so that the correct key is in place if a station roams to a new RP.

These mechanisms are enabled by default, although you can disable them on particular WLANs. A third mechanism, pre-authentication, completes the requirements for fast roaming between RPs adopted by different Wireless Edge Services zl Modules.

**Note**

Using pre-authentication to enable fast roaming also applies to roaming between an AP and a Wireless Edge Services zl Module.

Pre-authentication

Roaming becomes more complicated when a station roams from an RP adopted by one module to an RP adopted by another module.

The complication arises from the authentication enforced in the WLAN. Because the station has not authenticated to the second module, the second module does not know whether the station is allowed to connect. 802.1X authentication, in particular, slows down a roam because it requires several exchanges of messages, usually to a network RADIUS server.

In addition, as noted above, WPA uses 802.1X authentication to create unique encryption keys for each station. The second module does not have the correct key for the station until the station authenticates to it.
Fast Layer 2 Roaming and Layer 3 Mobility

Overview

The 802.11i standard (on which WPA is modeled) includes a section on pre-authentication, a mechanism that speeds up Layer 2 roaming. A station can associate to only one RP and Wireless Edge Services zl Module at a time. However, the station can detect beacons from other RPs—including RPs connected to other modules. A station using pre-authentication listens for such beacons and pre-authenticates to other modules while it is still connected to its original module.

Because the station is still connected to its original module, its pre-authentication messages must pass through the original module, onto the wired network, and finally to the second module. These pre-authentication messages are the Extensible Authentication Protocol (EAP) messages required by 802.1X, and the station addresses them to the Basic Service Set Identifier (BSSID) of the WLAN on the RP to which it is pre-authenticating.

Enabling pre-authentication on a Wireless Edge Services zl Module lets the module listen for EAP messages that arrive on its internal uplink port and respond to those destined to its RPs. The station authenticates to the second module, and the module and the station set in place all the encryption keys necessary for WPA, before the station ever roams. Thus, when the station does roam, it does so very quickly (in less than 50 milliseconds).

Note

The EAP pre-authentication messages do not cross VLAN borders. Therefore, the two Wireless Edge Services zl Modules must assign the WLAN to the same subnetwork (VLAN). This requirement means that Layer 3 mobility, described in the next section, is seamless, but not fast.

Layer 2 Roaming on a Web-Auth WLAN Between Different Wireless Edge Services zl Modules

Like 802.1X authentication, Web-Auth can complicate a roam between RPs adopted by different Wireless Edge Services zl Modules. The new module considers the roaming station a new, unauthenticated station, so it redirects the station’s Web browser to the login page. Because the user must reauthenticate, the roam is not seamless.

The best solution for roaming with Web-Auth is to have a single Wireless Edge Services zl Module adopt all RPs that support the WLAN in question. The RPs can range over an extensive area: Layer 3 adoption enables them to reach the module across subnetwork boundaries.

If necessary, however, you can enable seamless Layer 2 roaming for Web-Auth between different modules. Place all Wireless Edge Services zl Modules that support the Web-Auth WLAN in the same redundancy group. When a user
authenticates to one module, that module uses the redundancy group communications to transmit the user’s credentials to all modules in the group. The other modules cache the credentials so that they are ready to be sent to the RADIUS server should the user later roam to one of these modules.

Note that the redundancy group solution does not enable the Web-Auth WLAN to include any more RPs than the single module solution: a redundancy group, just like a single module, has a 156 RP limit. The only reason to have multiple Wireless Edge Services zl Modules support the WLAN would be to add capacity to the system.

Layer 3 Mobility

A station can roam seamlessly between two RPs adopted by the same Wireless Edge Services zl Module (as long as both RPs support the WLAN). Likewise, a station can roam seamlessly between two RPs adopted by different modules as long as those RPs support the same WLAN. However, two modules that do not support the same virtual LANs (VLANs) complicate the roaming process: the station’s IP address is no longer valid, so it loses its active sessions.

Wireless Edge Services zl Modules use Layer 3 mobility to solve this problem. You must enable Layer 3 mobility to support roaming between modules that have these characteristics:

- The modules support the *same* WLAN (or WLANs).
- Each module places traffic from that WLAN in a *different* subnetwork. For Layer 3 mobility to function correctly, the different subnetworks must use different VLAN IDs.

Figure 9-1 illustrates a network that requires Layer 3 mobility. The module on the left places wireless stations in WLAN A in VLAN 1 while the module on the right places stations in WLAN A in VLAN 20.
Fast Layer 2 Roaming and Layer 3 Mobility
Overview

To implement Layer 3 mobility, Wireless Edge Services zl Modules perform these functions:

- The modules support a Layer 3 mobility domain.

The area in which stations can roam freely (no matter which subnetworks are supported in that area of the wired network) is the Layer 3 mobility domain. The Wireless Edge Services zl Modules in the roaming domain are referred to as peers. A domain can include up to 12 peers, each of which can support up to 500 stations.
The modules store information about all stations associated to any module in the Layer 3 mobility domain.

The Wireless Edge Services zl Module responsible for handling a station’s traffic is that station’s home module (HM). All the peers in the Layer 3 roaming domain must track all stations’ HM and HM VLAN. A module can then recognize when a station that roams to it requires a Layer 3 roam: the station’s HM VLAN is different from the VLAN supported on that module.

When a Layer 3 roam is necessary, a module tunnels traffic back to the station’s original module.

Each peer in the Layer 3 mobility domain maintains a Generic Routing Encapsulation (GRE)-like tunnel to each other peer. (The peers automatically configure the tunnel when you enable Layer 3 mobility.) When a station roams, the module tunnels all traffic to and from the station, including Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) requests, to the station’s HM.

As you plan Layer 3 roaming, keep in mind that a Layer 3 roaming domain should be contiguous with the following two domains. (See Figure 9-2.)

The Radio Frequency (RF), or Layer 2, roaming domain

Layer 3 roaming takes place in the background on top of RF roaming. That is, at both Layer 2 and Layer 3, stations always roam within a WLAN. (Moving to a new WLAN requires the user to select a new wireless network.) Therefore, all Wireless Edge Services zl Modules in the Layer 3 roaming domain must support the WLAN in question.

In addition, you must not divide a WLAN into multiple Layer 3 roaming domains.

A ProCurve Identity Driven Manager (IDM) location domain

If you use IDM to assign network rights, best practices dictate that devices in the same Layer 3 roaming domain are also in the same location domain.

Note, however, that you cannot use dynamic VLAN assignments with Layer 3 mobility.

For seamless Layer 2 roaming for WLANs that use Web-Auth, you must place all Wireless Edge Services zl Modules in the same redundancy group. So, if you want to enable Layer 3 mobility as well, you should place modules in the same redundancy group and Layer 3 mobility domain.
Roaming Behavior

This section summarizes which features you must configure on your Wireless Edge Services zl Modules to enable the best possible roaming behavior in various circumstances. Keep in mind that this section discusses the behavior the modules support. Stations’ capabilities also affect roaming. For example, the station’s wireless network interface card (NIC) determines when the station will actually roam, and the station’s operating system (OS) determines how long the station holds the IP stack if it loses the radio signal—even temporarily.
The previous sections have introduced you to different types of roaming, which are defined briefly as follows:

- **Fast roaming**—A fast roam is under 50 milliseconds. Fast roaming, as a standard, refers to pre-authentication as specified by 802.11i, which applies only to WPA/WPA2 with 802.1X. However, other types of roaming might be under 50 milliseconds. When a roam is described as fast, it also is assumed to be seamless.

- **Seamless roaming**—The defining feature of a seamless roam is not speed, but preservation of the user's authentication, IP address, and active sessions. The user does not need to re-login, and a user browsing the Internet probably would not notice a seamless roam; a user accessing a real-time application may detect a slight lag.

- **Not seamless roaming**—If a roam is not seamless, the user must log in again so that his or her station can re-authenticate or change its IP address.

A Wireless Edge Services zl Module handles roaming between its own RPs automatically—this roaming is always fast. To enable the best possible roaming between RPs adopted by different modules, however, you may need to take some additional steps.

If you configure and group your modules correctly, you can always enable at least seamless, and sometimes fast, roaming. Table 9-1 explains how to enable the best possible roaming depending on the WLAN’s security and on whether the roam occurs at Layer 2 or Layer 3.
Overview

Table 9-1. Enabling the Best Roaming Between Different Wireless Edge Services zl Modules

<table>
<thead>
<tr>
<th>WLAN Security Option</th>
<th>Layer 2 Roam Without Special Configuration</th>
<th>Best Layer 2 Roam</th>
<th>Requirements for Best Layer 2 Roam</th>
<th>Layer 3 Roam Without Special Configuration</th>
<th>Best Layer 3 Roam</th>
<th>Requirements for Best Layer 3 Roam</th>
</tr>
</thead>
<tbody>
<tr>
<td>open authentication</td>
<td>seamless</td>
<td>seamless</td>
<td>none</td>
<td>not seamless</td>
<td>seamless</td>
<td>modules in the same Layer 3 mobility domain</td>
</tr>
<tr>
<td>authentication with a static key (static Wired Equivalent Privacy [WEP] or WPA-preshared key [PSK])</td>
<td>seamless</td>
<td>seamless</td>
<td>none</td>
<td>not seamless</td>
<td>seamless</td>
<td>modules in the same Layer 3 mobility domain</td>
</tr>
<tr>
<td>Web-Auth</td>
<td>not seamless</td>
<td>seamless</td>
<td>156 RP limit, either:</td>
<td>not seamless</td>
<td>seamless</td>
<td>modules in the same Layer 3 mobility domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• a single module adopts all RPs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• modules in the same redundancy group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dynamic WEP or RADIUS MAC authentication</td>
<td>seamless</td>
<td>seamless</td>
<td>none</td>
<td>not seamless</td>
<td>seamless</td>
<td>modules in the same Layer 3 mobility domain</td>
</tr>
<tr>
<td>WPA/WPA2 with 802.1X</td>
<td>seamless</td>
<td>fast</td>
<td>• PMK caching</td>
<td>not seamless</td>
<td>seamless</td>
<td>modules in the same Layer 3 mobility domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• pre-authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In summary, follow these guidelines:

- The Wireless Edge Services zl Module automatically enables fast Layer 2 roaming between RPs on the same module. (Layer 3 roaming is not a concern for roaming on a single module.)

- Except when using Web-Auth, modules automatically handle seamless (but not necessarily fast) Layer 2 roaming between RPs on different modules.

- Fast roaming between modules at Layer 2 requires extra configuration and is possible in a WLAN that requires WPA/WPA2 with 802.1X. See “Configuring Fast Layer 2 Roaming for WPA/WPA2 with 802.1X” on page 9-12.
- When a WLAN enforces Web-Auth, you must configure a redundancy group for seamless Layer 2 roaming between RPs on different modules. See Chapter 10: “Redundancy Groups” to learn how to create such a group.

- You must configure a Layer 3 mobility domain for Layer 3 roaming. Layer 3 roaming is seamless, but not fast. See “Configuring Layer 3 Mobility” on page 9-15.

In some networks, you must enable Layer 2 roaming between some Wireless Edge Services zl Modules and Layer 3 roaming between others. Keep these rules in mind as you plan relationships between Layer 3 mobility domains and redundancy groups:

- A Layer 3 mobility domain can include multiple redundancy groups or no redundancy groups at all.
  
  You can divide a Layer 3 mobility domain into multiple redundancy groups, or you can place all modules in the domain in the same group. Although modules in the same redundancy group usually map a WLAN to the same VLAN, as long as you place the modules in the same Layer 3 mobility domain, this is not a requirement. Roaming behavior is not typically affected by how you group modules into redundancy groups.

- Best practices dictate that two Wireless Edge Services zl Modules in the same redundancy group either be in the same Layer 3 mobility domain or in no mobility domain at all (for a network that does not require Layer 3 roaming).

In other words, a Layer 3 mobility domain can include members in multiple redundancy groups, but a redundancy group can include members in at most one Layer 3 mobility domain.
Configuring Fast Layer 2 Roaming for WPA/WPA2 with 802.1X

Fast roaming facilitates roaming in a WLAN that requires WPA/WPA2 with 802.1X authentication. That is, it speeds the process of a station connecting to a new RP and possibly a new Wireless Edge Services module:

- putting necessary encryption keys in place
- when necessary, completing 802.1X authentication

If your network includes only one Wireless Edge Services module or if your network requires roaming only between RPs adopted by the same module, you do not need to configure fast Layer 2 roaming. The module supports it by default.

However, in a network in which stations might need to roam between RPs adopted by different modules, you must enable fast roaming for WLANs that enforce WPA with 802.1X authentication. Follow these steps:

1. Select **Network Setup > WLAN Setup > Configuration**.
2. Select the WLAN on which you want to enable fast roaming.
3. Click the **Edit** button.
4. Configure the WLAN settings, making sure to select **802.1X EAP** for authentication and **WPA/WPA2-TKIP** or **WPA2-AES** for encryption.

   For more information about configuring WLANs, see Chapter 4: “Wireless Local Area Networks (WLANs).”
5. Click the **Config** button next to the encryption standard. A screen for editing the encryption options is displayed.
6. Check the box for **Pre-authentication**.

   Remember that pre-authentication messages do not cross subnetwork (VLAN) boundaries, so the module receives them only from modules or APs that assign the WLAN to the same subnetwork.

7. By default, **PMK Caching** and **Opportunistic Key Caching** are enabled and you should leave them so.

   PMK caching *must* be enabled for pre-authentication. (PMK caching allows the module to store the station’s encryption key until the station actually roams to it.) Although opportunistic key caching is optional for pre-authentication, ProCurve Networking recommends that you accept the default setting, which enables this option. Opportunistic key caching facilitates fast roaming between RPs adopted by the same module.

**Note**

When PMK caching is enabled, a WPA2 station that roams is no longer controlled by any dynamic ACLs configured with IDM. If you use IDM to assign ACLs to users with WPA2 connections, you should disable PMK caching.
8. Click the **OK** button.
9. Click the **OK** button in the **Edit** screen for the WLAN.
10. Remember to save your configuration.

---

**Configuring Layer 3 Mobility**

You must complete these tasks to configure Layer 3 mobility:

1. Configure Layer 3 mobility settings for the local Wireless Edge Services zl Module:
   - IP address
   - WLANs on which Layer 3 mobility is enabled
2. Specify the peers' IP addresses.
3. Enable Layer 3 mobility.
4. Save the configuration and complete these steps on all other Wireless Edge Services zl Modules in the Layer 3 mobility domain.

It is assumed that you have completed the configurations outlined in Table 9-2.

---

**Note**

You cannot use user-based, or dynamic, VLANs in a WLAN assigned to the Layer 3 mobility domain. In other words, the **Dynamic Assignment** box in the WLAN's **Edit** screen must be unchecked.
Fast Layer 2 Roaming and Layer 3 Mobility
Configuring Layer 3 Mobility

Table 9-2. Other Configurations Necessary for Layer 3 Roaming

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Necessary Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN configuration (for each WLAN on which Layer 3 mobility is enabled)</td>
<td>• SSID and security settings are the same as peers’ settings.</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID is different from at least some peers’ VLAN settings. Different subnetworks must have different VLAN IDs.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic VLAN assignment is disabled.</td>
</tr>
<tr>
<td>IP configuration on the local module</td>
<td>• The module can reach peers.</td>
</tr>
<tr>
<td></td>
<td>• The peers can reach the module.</td>
</tr>
<tr>
<td>IP configuration for stations</td>
<td>• DHCP is provided through either:</td>
</tr>
<tr>
<td></td>
<td>– local DHCP pool for the VLAN mapped to the WLAN</td>
</tr>
<tr>
<td></td>
<td>– external DHCP server</td>
</tr>
</tbody>
</table>

Configuring Layer 3 Mobility Settings

The first step in establishing a Layer 3 mobility domain is configuring local Layer 3 mobility settings on your Wireless Edge Services zl Module. You must specify:

- the IP address that the module uses in the mobility domain:
  - an IP address configured on the local Wireless Edge Services zl Module
  - an IP address reachable by all peers
    In other words, the VLAN with this IP address must be tagged on the module's uplink port. Network infrastructure devices must also be able to route to this address.

- the local WLANs that can use Layer 3 roaming

  Stations do not roam between these WLANs. Stations only roam between RPs that support the same WLAN. Wireless Edge Services zl Modules create a separate Layer 3 mobility domain for each WLAN.

To configure the Layer 3 mobility settings, complete these steps:

1. Select **Network Setup > Layer 3 Mobility > Configuration.**
2. Specify a valid IP address on this Wireless Edge Services zl Module. You have two options:
   - Select **Use Default Management Interface** to use the address on the management VLAN.
   - Select **Use this Local Address** and manually enter an IP address.

3. Optionally, change the value in the Roam Interval field.

4. A station that roams at Layer 3 must maintain its association with its HM. The roam interval specifies how long the Wireless Edge Services zl Module stores a station's association after it loses contact with the station—giving the station's traffic time to tunnel back to it after a Layer 3 roam.

   The roam interval is added to the station timeout for the WLAN in question. If you have set this value low and if your Ethernet network is somewhat congested, you might need to increase the roam interval.

   You can set the interval from between 1 and 300 seconds. The default setting is 5 seconds.
5. The section at the bottom on the screen displays all WLANs on this module. Check the boxes for the WLANs on which you want to enable Layer 3 mobility.

Enabled WLANs are displayed in boldface.

You can use the **All WLANs On** and **All WLANs Off** buttons to quickly select and deselect WLANs.

You might see the screen shown in Figure 9-6 when you attempt to check a WLAN's box.

![Figure 9-6. Dynamic VLAN Error](image)

Dynamic VLAN assignment is incompatible with Layer 3 mobility. If the WLAN requires Layer 3 mobility, you must access the WLAN's **Edit** screen and uncheck the **Dynamic Assignment** box. (See “Setting Basic Configuration Options: SSID and VLAN Interface” on page 4-30 of Chapter 4: “Wireless Local Area Networks (WLANs).”)

6. Click the **Apply** button.

Figure 9-7 displays an example configuration.
Specifying Layer 3 Mobility Peers

Other Wireless Edge Services zl Modules in the Layer 3 mobility domain are called peers. To specify their addresses, complete these steps:

1. Select **Network Setup > Layer 3 Mobility** and click the **Peer List** tab.
2. Click the **Add** button.
Fast Layer 2 Roaming and Layer 3 Mobility
Configuring Layer 3 Mobility

Figure 9-8. Adding a Layer 3 Mobility Peer

3. Enter the peer's IP address in the Add screen.
4. Click the OK button.

Repeat steps 2 through 4 to add multiple peers (up to 11).

Enabling Layer 3 Mobility

After configuring your Layer 3 mobility settings and specifying peers, you enable Layer 3 mobility by completing these steps:

1. Select Network Setup > Layer 3 Mobility and click the Configuration tab.
2. Check the Enable Mobility box.
3. Click the **Apply** button.

4. Click the **Save** link to write the configuration to the startup-config.
Verifying and Managing Layer 3 Mobility

To verify that Layer 3 mobility is functioning correctly, check the following:

- The local Wireless Edge Services zl Module begins communicating with its peers.
- Stations that roam to an RP adopted by a Wireless Edge Services zl Module on a different VLAN preserve their IP addresses and active sessions.

Monitoring Peers

Select Network Setup > Layer 3 Mobility and click the Peer List tab to view each peer’s current status. You should see the Established status, as shown in Figure 9-10, which indicates that the local module and the peer are communicating.

```
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Session Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4.2.30</td>
<td>Established</td>
</tr>
</tbody>
</table>
```

Figure 9-10. Viewing a Peer’s Status
Fast Layer 2 Roaming and Layer 3 Mobility
Verifying and Managing Layer 3 Mobility

The Idle status indicates that the local Wireless Edge Services zl Module has not enabled Layer 3 roaming. Even if the Enable Mobility box is checked, the module does not enable Layer 3 mobility until you specify a valid local IP address.

A Wireless Edge Services zl Module that remains at the Active-Connecting or Passive-Connecting status also cannot connect to the peer. Usually, one of two problems has occurred:

- The local Wireless Edge Services zl Module and the peer cannot reach each other.
  
  Make sure that each module can ping all other members of the Layer 3 mobility domain. The local IP addresses must be on VLANs that are tagged on the uplink VLAN. And either the modules themselves or the modules' default gateways must know the necessary routes.

- The peer has not enabled Layer 3 mobility.

You should also check that this module and the peer enable mobility on the same WLAN (or WLANs). Even when they do not, the peers can establish a connection; however, but Layer 3 mobility will not function correctly on the WLAN in question.

Tracking Peer Communications

Layer 3 mobility peers that have established a relationship exchange these messages:

- **Join Events**—A Wireless Edge Services zl Module sends a Join Event when a station first associates with it. This message, which informs all peers that the station has joined the Layer 3 mobility domain, contains the station’s MAC address, IP address, and HM VLAN. The HM (the module responsible for handling the station’s traffic) is typically the module that sends the Join Event message.

- **Leave Events**—A module informs its peers when a station disassociates from the WLAN completely. (This is different from roaming to a new RP or module.)

- **L2-Roams**—A station performs a Layer 2 roam when it reassociates to a new RP but its HM VLAN remains the same. Wireless Edge Services zl Modules track only Layer 2 roams that occur between modules. Because the new module supports the station’s HM VLAN, the new module does not need to tunnel traffic back to the original HM. Instead, the new module becomes the station’s new HM, sending out an L2-Roam message to notify peers of the change.
Fast Layer 2 Roaming and Layer 3 Mobility
Verifying and Managing Layer 3 Mobility

- **L3-Roams**—When a Wireless Edge Services zl Module receives a reassociation request from a station with a different HM VLAN than the module uses, it determines that a Layer 3 roam is necessary. The new module becomes the station’s current module (CM), sends an L3-Roam message to the HM, and begins tunneling the station’s traffic back to the HM.

Track the messages described above to verify that your Wireless Edge Services zl Modules send the correct messages when your station completes the roams illustrated in Figure 9-11.

---

**Figure 9-11. Difference Between a Layer 2 Roam and a Layer 3 Roam**
To track the messages, select **Network Setup > Layer 3 Mobility** and click the **Peer Statistics** tab. A screen displays all peers, which are identified by their IP address. (See Figure 9-12.) Columns display:

- the number of Join Events sent to and received from that peer
- the number of Leave Events sent to and received from that peer
- the number of L2-Roams sent to and received from that peer
- the number of L3-Roams sent to and received from that peer

<table>
<thead>
<tr>
<th>Peer IP</th>
<th>JOIN Events sent/recv</th>
<th>LEAVE Events sent/recv</th>
<th>L2-ROAMS sent/recv</th>
<th>L3-ROAMS sent/recv</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.30</td>
<td>12/6</td>
<td>12/6</td>
<td>0/10</td>
<td>0/2</td>
</tr>
</tbody>
</table>

Figure 9-12. Viewing Peer Statistics

Click the **Clear Statistics** button to erase the current statistics and start the counters over again.
Fast Layer 2 Roaming and Layer 3 Mobility
Verifying and Managing Layer 3 Mobility

Viewing a Station’s Status

A successful Layer 3 roam should meet these criteria:

- The station roams seamlessly at Layer 2—that is, the station reassociates and re-authenticates in the background.
- The station maintains its IP address.
- The Wireless Edge Services zl Module that supports the station’s new RP becomes the station’s CM and tunnels traffic back to the station’s HM.

To test Layer 3 roaming, move a station from one RP’s cell to the cell of an RP supported by a different Wireless Edge Services zl Module. Verify that the station’s IP address remains the same and sessions remain active.

You can also verify a Layer 3 roam from your module’s Web browser interface.

To view information about stations, select Network Setup > Layer 3 Mobility and click the Station Status tab. You can also view this information by selecting Device Information > Wireless Stations and clicking the Layer 3 Mobility-Station Status tab.
### Fast Layer 2 Roaming and Layer 3 Mobility
### Verifying and Managing Layer 3 Mobility

#### Figure 9-13. Viewing a Station's Status

The screen displays the following information for every station associated with any Wireless Edge Services zl Module in the Layer 3 mobility domain:

- **Station MAC**—station MAC address
- **Station IP**—station IP address
- **Home Module IP**—HM IP address
- **Home Module VLAN**—HM VLAN ID
- **Curr Module IP**—CM IP address
- **Roam**—This column tracks Layer 3 roams. The station is considered to be in a roaming state (green check mark) if its CM differs from its HM.

<table>
<thead>
<tr>
<th>Station MAC</th>
<th>Station IP</th>
<th>Home Module IP</th>
<th>Home Module VLAN</th>
<th>Curr Module IP</th>
<th>Roam</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:5E:25:39:1C</td>
<td>10.4.1.70</td>
<td>10.4.1.20</td>
<td>10.4.2.30</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>00:13:5E:25:39:1C</td>
<td>10.4.1.150</td>
<td>10.4.1.30</td>
<td>10.4.1.30</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>00:13:5E:25:39:1C</td>
<td>10.4.1.189</td>
<td>10.4.1.30</td>
<td>10.4.1.30</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>00:13:5E:25:39:1C</td>
<td>10.4.2.201</td>
<td>10.4.2.30</td>
<td>10.4.2.30</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

---

9-27
In Figure 9-13, the 10.4.1.30 Wireless Edge Services zl Module is the HM for three stations associated with the wireless network, and the 10.4.2.30 module is the HM for one station. However, one of the 10.4.1.30 module's stations has roamed to an RP supported by the 10.4.2.30 module. Because these two modules are on different VLANs, the roam occurred at Layer 3. As you can see in the top row in Figure 9-13, the station has 10.4.1.30 as its HM, but 10.4.2.30 as its CM; the Roam column has a green check mark.
Redundancy Groups

Contents

High Availability for Wireless Services .................................. 10-2
Redundant Wireless Services z1 Module ................................. 10-2
Redundancy Group ................................................................. 10-3
Active or Standby Mode ......................................................... 10-4
Adopting RPs ................................................................. 10-5
Adopting RPs in Active Mode ........................................... 10-5
Adopting RPs in Standby Mode ........................................... 10-6
RP Licensing for Redundancy Groups .................................... 10-6
Establishing a Redundancy Group ......................................... 10-7
Creating Matching Configurations for the Redundancy Group .... 10-9
Redundancy Group Configuration Mode Context ..................... 10-9
Redundancy Group Behavior When a Member Fails ............... 10-10
Configuring a Redundancy Group .......................................... 10-11
Configuring Redundancy Group Settings ............................... 10-12
Adding Members to the Redundancy Group ......................... 10-14
Enabling Redundancy ......................................................... 10-16
Viewing Information about the Redundancy Group ............... 10-18
History ................................................................. 10-21
Viewing Information about the Other Members of the Redundancy Group ......................................................... 10-22
Setting up Adoption Preference IDs to Control RP Adoption .... 10-24
Configure an Adoption Preference for the Module ............... 10-28
Configure an Adoption Preference for Targeted Radios .......... 10-28
Configure an Adoption Preference for Newly Adopted Radios .. 10-30
Reverting RPs Adopted by a Standby Member to the Active Member ......................................................... 10-33
High Availability for Wireless Services

For many companies, wireless access has become as critical to their business as traditional wired access. Recognizing the importance of wireless access, ProCurve Networking has designed its wireless services with high availability in mind.

To protect the availability of your company's wireless services, purchase multiple Wireless Edge Services zl Modules and place them in a redundancy group. ProCurve Networking provides two types of modules, both of which can be members of a redundancy group:

- Wireless Edge Services zl Module (J9001A)
- Redundant Wireless Services zl Module (J9003A)

In this chapter, a Wireless Edge Services zl Module is called a primary module, and a Redundant Wireless Services zl Module is called a redundant module.

The section below describes the particular features of a Redundant Wireless Services zl Module. The next section, “Redundancy Group” on page 10-3, explains how both types of modules work together in a redundancy group.

Redundant Wireless Services zl Module

To provide failover capabilities for the ProCurve Wireless Edge Services zl Module (J9001A), you can purchase a Redundant Wireless Services zl Module (J9003A).

The Redundant Wireless Services zl Module provides the same functionality as the Wireless Edge Services zl Module, with one exception: the redundant module does not have any radio port (RP) licenses. On its own, the redundant module cannot adopt any RPs.

When combined with one or more Wireless Edge Services zl Modules in a redundancy group, however, the Redundant Wireless Services zl Module can adopt RPs under certain circumstances. Primarily, the redundant module is designed to adopt RPs if one of the primary Wireless Edge Services zl Modules becomes unavailable for any reason. However, you can also configure the Redundant Wireless Services zl to use a primary module's licenses to adopt RPs at any time. (For more information about RP adoption in a redundancy group, see “Adopting RPs” on page 10-5.)
The redundant module has its own software image and configuration file. Before a redundant module can deliver wireless services for your network, you must configure it to provide those services—just as you would configure a primary module.

Redundancy Group

A redundancy group can contain up to twelve modules:

- at least one Wireless Edge Services zl Module
- up to 11 other Wireless Edge Services zl Modules or Redundant Wireless Services zl Modules, in any combination

For example, the group can include one Wireless Edge Services zl Modules (primary module) and two Redundant Wireless Services zl Module (redundant modules). Or it can include eight primary modules and four redundant modules. However, the typical configuration includes one primary module and one or more redundant modules. This is because adding modules to the group does not add licenses, as explained in “RP Licensing for Redundancy Groups” on page 10-6.

You can install up to two modules in a wireless services-enabled switch. For higher availability, you should install modules in separate switch chassis. Then if one wireless services-enabled switch becomes unavailable—due to a cable failure, for example—the other wireless services-enabled switch can still provide the wireless services that your company needs. (See Figure 10-1.)
Active or Standby Mode

When you configure a module to be part of a redundancy group, you must select a mode, which determines the module’s role in the group.

For each of the 12 members of a redundancy group, you can select:

- **Active mode**—In active mode, the module is responsible for adopting RPs and providing the wireless services that you have configured on the module.
Redundancy Groups
High Availability for Wireless Services

- **Standby mode**—In standby mode, the module is primarily responsible for providing failover capabilities if a module in active mode becomes unavailable. (A module in standby mode can adopt RPs in the circumstances described in “Adopting RPs” on page 10-5.)

Both Wireless Edge Services zl Modules and Redundant Wireless Services zl Modules support both modes. This difference between primary and redundant modules lies in the redundant module’s lack of RP licenses, not in the modes in which the modules function. For example, in a group that includes one primary module and two redundant modules, you can configure the primary module in active mode and the redundant modules in standby mode. But you can also choose to configure all three modules in active mode. In fact, this is often a good idea because the active modules load balance RPs between them, adding capacity to the network.

**Note**

Selecting active mode for more than one module in a redundancy group still provides high availability. If one module fails, another active module will adopt the failed module’s radio ports.

**Adopting RPs**

How a Wireless Edge Services zl Module or Redundant Wireless Services zl Module adopts RPs depends on the module’s mode.

**Adopting RPs in Active Mode**

All active members of a redundancy group can adopt RPs. By default, the modules load balance the available RPs based on each module’s load value. When an RP is detected, the active module with the lowest load value adopts that RP. If more than one module has the same load value, the module with the lowest media access control (MAC) address adopts the RP. The load value is based on the number of RPs adopted by the module, not on the amount of traffic the RPs support.

Basing adoption on the load value is not always the best way to manage RPs, however. Sometimes, you may want manual control over which RPs are adopted by which module. See “Setting up Adoption Preference IDs to Control RP Adoption” on page 10-24 to learn how to use adoption preference IDs to determine which RPs each module adopts.
Adopting RPs in Standby Mode

In standby mode, a redundancy group member adopts RPs only in certain circumstances:

- The standby member does not receive a heartbeat from an active member for the length of time specified in the hold period option.

  In a group with multiple active members, the standby member takes action should even one member fail.

- All active members fail to adopt an RP, although the group has enough RP licenses to adopt the RP.

Table 10-1 describes some of these situations.

Table 10-1. Situations in Which a Standby Member Adopts RPs

<table>
<thead>
<tr>
<th>Situation</th>
<th>Possible Causes</th>
</tr>
</thead>
</table>
| A standby member misses heartbeats from an active member. | • The active member has failed.  
• The wireless services-enabled switch in which the active member is installed has failed.  
• A failed network connection has isolated the wireless services-enabled switch from the network. |
| Active modules fail to adopt an RP.          | • Active members’ internal downlink ports have not been tagged for the RP VLAN.  
• Active members’ are explicitly prohibited from adopting the RP. |

If the active member becomes unavailable and a standby member adopts its RPs, the standby member continues to support these RPs even after the active member becomes available again, which maintains continuity of service. You can, however, manually revert the standby member to force it to return the RPs to the active member.

RP Licensing for Redundancy Groups

The sections above described the circumstances in which a member of a redundancy group can adopt an RP. A final condition for adopting an RP is that the group have sufficient licenses. (See “Radio Port Licenses” on page 2-122 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)
The number of licenses for the redundancy group equals the number of licenses installed on the group member with the most licenses. For example, a group includes these members:

- one Wireless Edge Services zl Module with the default license (for 12 RPs) and one additive license (for 12 RPs)
- one Wireless Edge Services zl Module with the default license (for 12 RPs)
- one Redundant Wireless Services zl Module

The redundancy group has two licenses and can adopt 24 RPs.

All members of the redundancy group share the group’s licenses. Any active member can use the groups’ licenses to adopt an RP at any time. Any standby member can use the groups’ licenses to adopt an RP in the circumstances listed in “Adopting RPs in Standby Mode” on page 10-6.

Establishing a Redundancy Group

To ensure that each module recognizes that it is part of a redundancy group and knows the IP address of the other modules in the group, you must complete the steps to configure a redundancy group on each module. In addition, you must ensure that the modules can communicate with one another. For example, if the modules are installed in different wireless services-enabled switches, the switches must be connected either directly or indirectly (through one or more infrastructure switches).

When you configure and enable a redundancy group on a module, that module begins the process of establishing a group. To successfully complete this process, the module must receive communications from the other modules in the redundancy group.

The process for establishing a redundancy group is the same for both primary and redundant modules. If all modules all configured correctly as a redundancy group, each will go through the following stages in establishing a group:

- **Startup state**—The redundancy service starts on the module.
- **Discovery state**—The module begins to send heartbeat messages to advertise that it is available. It listens for the other modules to send heartbeat messages to verify that its peers are also available.

In addition, the module sends an update message, listing the current values for its redundancy group settings, such as heartbeat time, discovery time, hold time, redundancy ID, and redundancy protocol version. The other modules send an update message as well. The modules
Redundancy Groups
High Availability for Wireless Services

compare their redundancy group settings to ensure that they are the same. If the modules are not using the same settings, they cannot establish a functioning redundancy group.

- **Online state**—If the modules can reach each other and they are using the same redundancy group settings, they change their status to online. In this state, a standby module can take over for an active module if the active module becomes unavailable. However, you must configure the standby modules to provide wireless services, as explained in “Creating Matching Configurations for the Redundancy Group” on page 10-9.

If redundancy is not enabled for a module, it is in the disabled state.

Figure 10-2 illustrates the process of establishing a redundancy group between two modules.
Creating Matching Configurations for the Redundancy Group

To establish a redundancy group, modules must support the same redundancy group settings. Typically, you also want all modules in the redundancy group to provide the same wireless services.

You can use one module’s configuration file as a starting point for configuring other modules. You can transfer the first module’s configuration file to a TFTP or an FTP server and then upload the configuration file to the other modules in the group. You can then edit module-specific settings (such as IP addresses for virtual LANs [VLANs] and redundancy group settings) and save the configuration to the each module’s startup-config. If you later change the configuration of one module, you must remember to make the same change to other modules.

Redundancy Group Configuration Mode Context

Alternatively, you can use the redundancy group configuration mode in the CLI to configure settings that are pushed to all members of the group.

The redundancy group configuration mode is a special configuration mode available from the enable mode context of the Wireless Edge Services zl Module CLI. You can only access the redundancy group configuration mode, however, in these circumstances:

- The module is a member of a redundancy group.
- All members of the group are in the Online state.

The redundancy group configuration mode is shared among all members, so that must the local module must be able to communicate with them.

To enter the redundancy group configuration mode context, enter this command from the module enable mode context:

```
ProCurve(wireless-services-C)# redundancy-group-cli-config enable
ProCurve(wireless-services-C)#redundancy-cli*#
```

After accessing the redundancy group configuration mode context, you can enter almost any command that you can enter from the configuration mode contexts of an individual module. For example, you can configure a WLAN. However, when you enter commands, not only the local module, but all modules in the group, receive the commands. In this way, all members of the redundancy group enforce consistent settings.
Redundancy Groups
High Availability for Wireless Services

You cannot enter some commands from the redundancy group configuration mode context. For example, you cannot configure IP settings and redundancy group settings. These you must set on members on an individual basis.

If you paste a configuration file into the redundancy group configuration mode context, the invalid commands simply do not take effect. For example, you could configure one Wireless Edge Services zl Module with all the settings for your network. Then you could set up the redundancy group, access the redundancy group configuration mode context, move to the global configuration mode context, and paste the startup-config of the base module into the CLI. The other modules in the redundancy group would receive WLAN, radio, DHCP, and RADIUS settings (as well as others), but each module would keep its own IP address.

**Note**

At most four managers can access a group's redundancy group configuration mode context at once.

For more information on CLI commands, see Appendix A: “ProCurve Wireless Edge Services zl Module Command Line Reference.”

**Redundancy Group Behavior When a Member Fails**

Members of a redundancy group listen for heartbeats from every other member. If, over the duration of the hold period, modules miss heartbeats from one member, standby members load balance the failed member’s RPs among themselves. If you desire, you can configure adoption preference IDs to control which of several standby modules adopt particular RPs.

Active members take no action when another member of the group fails unless, for whatever reason, the standby members fail to adopt the orphaned RPs. For example, a failed network connection might isolate a standby member from the RPs, or manual adoption might be inadvertently enabled on the standby member. If a redundancy group consists of only active members, active members can also adopt a failed members’ RPs, load balancing the RPs among themselves.

When the active member becomes functional again, the standby modules continue to support the RPs. You can manually force the standby modules to revert the RPs to the recovered member. You cannot, however, force an active member to return any RPs that it may have adopted. (See “Reverting RPs Adopted by a Standby Member to the Active Member” on page 10-33.)
Configuring a Redundancy Group

When you configure a redundancy group, you must define the following on each module that is a member of the group:

- the interface IP address for the module that you are configuring
- the member IP addresses (which are the IP addresses for the other modules in the redundancy group)

These two settings enable each module to send messages to and receive messages from other modules. The interface IP address that you enter on the one module should be the member IP address that you enter on each of the other modules. Table 10-2 provides an example.

Table 10-2. Configuring IP Addresses for a Redundancy Group

<table>
<thead>
<tr>
<th>Setting</th>
<th>Configuring a Redundancy Group on Primary Module A</th>
<th>Configuring a Redundancy Group on Redundant Module B</th>
<th>Configuring a Redundancy Group on Redundant Module C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP</td>
<td>192.168.1.10 (IP address of the default management interface on the primary module)</td>
<td>192.168.1.59 (IP address of the default management interface on redundant module A)</td>
<td>192.168.1.69 (IP address of the default management interface on redundant module B)</td>
</tr>
<tr>
<td>IP addresses for members</td>
<td>192.168.1.59</td>
<td>192.168.1.10</td>
<td>192.168.1.10</td>
</tr>
<tr>
<td></td>
<td>192.168.1.69</td>
<td>192.168.1.69</td>
<td>192.168.1.59</td>
</tr>
</tbody>
</table>

For each module, you must also select either active mode or standby mode.

In addition to defining these settings, you must configure other settings for the redundancy group, such as the length of the discovery period, the interval between heartbeats, and the redundancy group ID. These settings must be the same on all members of the group. If these settings do not match, the modules cannot establish a functioning redundancy group.

After you define the redundancy group settings, you must enable redundancy. You must perform this step last; if you try to enable the redundancy group before you add at least one member, an error message is displayed, telling you that you must first add a member. If you enable redundancy before configuring other redundancy settings, the fields for these settings are dimmed, and you cannot configure them (unless you disable redundancy once again).
Configuring Redundancy Group Settings

Redundancy group settings must match on all members of the group. (However, each member has its own IP address.) To configure the redundancy group settings a module, complete these steps:

1. Select **Network Setup > Redundancy Group** and click the **Configuration** tab.

2. In the **Interface IP** field, enter the IP address of the module that you are configuring. The redundancy feature uses this IP address to send heartbeat and update messages to the other modules in the redundancy group. (When you configure the redundancy group on the other modules, you enter this IP address when you add a member.)
Redundancy Groups
Configuring a Redundancy Group

Note

If you have assigned an IP address to more than one VLAN on the module, you should use the IP address assigned to the default management interface (which, by default, is VLAN 1).

If you decide to enter the IP address for a different VLAN, however, you must ensure that the redundancy traffic (such as the heartbeat and update messages) can be transmitted to the other module in the group. If the other module is installed in another wireless services-enabled switch on the network, both wireless services-enabled switches and all the switches in between must be able to transmit traffic on that VLAN.

3. In the Redundancy Group ID field, enter a number for the group. Each redundancy group on your network must have a unique group ID, and you must use the same group ID for each member of the group. You can enter any number from 1 through 65535.

4. Choose the Mode:
   • Select Active to allow the module to adopt RPs in all circumstances (as long as the group has sufficient licenses).
   • Select Standby to allow the module to adopt RPs only when active members fail to do so.

   More than one member of the group can act in active mode, and more than one can act in standby. You can choose either mode for either model (the Wireless Edge Services zl Module or the Redundant Wireless Services zl Module). See “Active or Standby Mode” on page 10-4 and “Adopting RPs” on page 10-5 for more information on the effects of the mode.

5. In the Discovery Period field, accept the default setting of 30 seconds, or enter a number from 10 through 60 seconds. (The discovery period is the amount of time that the module spends locating the other modules and ensuring that they are using the same redundancy group configuration.)

6. In the Heartbeat Period field, accept the default setting of 5 seconds, or enter a number from 1 through 255 seconds. Each module in the redundancy group periodically sends a heartbeat to determine if the other modules are still “alive,” or available. This setting determines the number of seconds between each heartbeat.
7. In the **Hold Period** field, accept the default setting of 15 seconds, or enter a number from 1 through 255 seconds. This setting determines the number of seconds that the module waits when it does not receive a heartbeat from another module in the redundancy group. If no heartbeats are received for the number of seconds specified in the hold period, the module determines that the other module in the group is unavailable. If the active member is unavailable, a standby member takes over its responsibilities and begins to adopt RPs.

As a general rule, you should configure the hold period to be three times as long as the heartbeat period. In practice, this means that if a module does not receive three consecutive heartbeats, it decides that the other module is unreachable.

8. Check the **Handle STP convergence** box if you want the module to factor in Spanning Tree Protocol (STP) convergence time before trying to establish the redundancy group.

STP’s relatively slow convergence can cause a problem when one member of a group is in a subnetwork that uses STP while another member is in a subnetwork that does not use STP or that uses rapid STP (RSTP). The second member does not hear any heartbeats from the first member, which is waiting for the spanning tree to be established before transmitting messages. The second member assumes that the first member is down and may attempt to adopt RPs when it should not.

When you select the **Handle STP convergence** box, the module waits 50 seconds, which is the standard time period allowed for STP convergence, before attempting to establish the redundancy group.

9. Click the **Apply** button to apply changes to the running-config.

**Adding Members to the Redundancy Group**

You must manually specify the IP address of every other module in the redundancy group. Follow these steps to define each member:

1. Select **Network Setup > Redundancy Group** and select the **Member** tab.
2. Click the **Add** button. The **Add Members** screen is displayed.

![Figure 10-4. Network Setup > Redundancy Group > Member Screen](image)

![Figure 10-5. Add Members Screen](image)
3. Enter the IP address of one of the other modules in the redundancy group. This address should match the address that you configure for the Interface IP in the other module's redundancy group settings.

4. Click the OK button. The module is now listed on the Network Setup > Redundancy Group > Member screen.

5. Repeat this step for each additional module in the redundancy group.

Enabling Redundancy

After you enable redundancy, the Wireless Edge Services zl Module begins communicating with other modules and establishing the redundancy group. Completely configure the redundancy group before enabling redundancy. After you enable redundancy, you can no longer alter settings or add new members.

Follow these steps:

1. Click the Configuration tab to return to the Network Setup > Redundancy Group > Configuration screen.

2. Check the Enable Redundancy box. The redundancy group configuration options are now dimmed. You also cannot change the member configuration (on the Member tab) while redundancy is enabled.
3. Click the **Apply** button to save the configuration to the running-config.

4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

5. Access the Web browser interfaces for each of the other modules in the redundancy group and configure those modules in the same way.
Viewing Information about the Redundancy Group

To view information about the redundancy group, select Network Setup > Redundancy Group and select the State tab.

<table>
<thead>
<tr>
<th>Network Setup &gt; Redundancy Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td><strong>State</strong></td>
</tr>
<tr>
<td>Redundancy state is</td>
</tr>
<tr>
<td>Group Authorization Level</td>
</tr>
<tr>
<td>Radio Ports adopted by Group</td>
</tr>
<tr>
<td>Adoption capacity in group</td>
</tr>
<tr>
<td>Unapproved Radio Ports in group</td>
</tr>
<tr>
<td>Radios in group</td>
</tr>
<tr>
<td>Self-healing Radios in group</td>
</tr>
<tr>
<td>Wireless Stations in group</td>
</tr>
</tbody>
</table>

Figure 10-7. Network Setup > Redundancy Group > State Screen

After the primary module and the redundant modules establish a redundancy group, each module tracks the following information about the group:

- **Redundancy state is**—This field lists the current state of the module. Both primary and redundant modules go through the same redundancy states:
  - Disabled
  - Startup
  - Discovery
  - Online

If this module is running redundancy, its state is Online.
Redundancy Groups
Configuring a Redundancy Group

■ **Module Authorization Level**—This field displays the number of RPs this module’s licenses allow it to adopt when it functions on its own. The authorization level for a redundant module, however, is taken from the level of the primary module with the most licenses.

■ **Protocol Version**—When the modules attempt to establish a redundancy group, each module includes its protocol version in the update messages sent during the discovery stage. If the modules are not all using the same protocol version, they cannot establish a group. You should ensure that the modules are running the same major release version of the software image. (In the software image, WS.XX.YY, XX indicates the major release version.)

■ **Group Authorization Level**—This field displays the maximum number of RPs that the group as a whole can adopt. This number matches the number for the module with the highest module authorization level. The group authorization level is *not* the sum of member’s individual authorization level. In other words, a redundancy group that includes two primary modules, one with licenses to adopt 36 RPs and one with licenses to adopt 12, has a group authorization level of 36.

■ **Group Connectivity Status**—This field displays one of the following:
  • All members connected—This is the normal state for a functioning redundancy group.
  • Not all members present—The modules in the group are not all communicating. A module may be unavailable, or the communication links between the modules may be disrupted.
  • n/a—Redundancy is not enabled.

■ **Radio Ports adopted by Group**—This field displays the total number of RPs adopted by the redundancy group. This number should equal the total number of RPs in your network (or that are part of the group). If the number indicates that RP has not been adopted, investigate the problem.

■ **Radio Ports adopted by this module**—This field displays the number of RPs that this module has adopted. If you are viewing the Network Setup > Redundancy Group > Configuration screen for a module that is running in standby mode, this field will typically display 0. If the standby module has adopted an RP, determine which active module has failed.

■ **Adoption capacity in group**—The group’s adoption capacity is the total number of RPs that the group is capable of adopting. This number is a sum of the adoption capacity of every online member of the group. Remember that the group authorization level sets the maximum for RPs that the group can *actually* adopt: a group might be capable of adopting many more RPs than its licenses allow.

■ **Adoption capacity on this module**—The number of RPs that this module is capable of adopting.
Other fields in the **Network Setup > Redundancy Group > State** screen allow you to monitor activity both on this particular module and throughout the group. For example, you can compare the **Unapproved Radio Ports on this module** value to the **Unapproved Radio Ports in the group** value to see whether this module’s RPs seem to detect more rogue APs—a sign of a possible security issue in a particular location of your network.

You can also check these fields:

- **Radios in group** or **Radios on this module**—the number of radios adopted by the group or by the individual module.
  
  Because some RPs include two radios, these numbers may be greater than those for the corresponding **Radio Ports adopted by** fields.

- **Self-healing Radios in group** or **Self-healing Radios** on this module—the number of radios adopted by the group or by the individual module that are enabled for self-healing.
  
  This field counts any radio that is enabled for self healing; the radio does need to be currently taking self healing action.

- **Wireless Stations in group** and **Wireless Stations on this module**—the number of wireless stations associated to all RPs adopted by the entire group or by this individual module.
History

At the bottom of the Network Setup > Redundancy Group > Configuration screen, you can also view the history of redundancy events that have occurred on this module.

The module records an event each time its redundancy state changes. For example, when you enable redundancy on the module, its state changes to startup, and the module records this event in the history. (The most recent events are listed first.) Each event listed includes:

- **State**—disabled, startup, discovery, or online
- **Time**—the day of the week, the date, the time, and the year
- **Trigger**—the event that initiated the change in the module’s state
- **Description**—a brief description of the event that initiated the change

---

**Figure 10-8. Redundancy Group History**

The module records an event each time its redundancy state changes. For example, when you enable redundancy on the module, its state changes to startup, and the module records this event in the history. (The most recent events are listed first.) Each event listed includes:

- **State**—disabled, startup, discovery, or online
- **Time**—the day of the week, the date, the time, and the year
- **Trigger**—the event that initiated the change in the module’s state
- **Description**—a brief description of the event that initiated the change
Viewing Information about the Other Members of the Redundancy Group

In addition to viewing information about the redundancy group, you can view information about the other members of the group. Select **Network Setup > Redundancy Group** and click the **Member** tab.

![Network Setup > Redundancy Group > Member Screen](image)

**Figure 10-9. Network Setup > Redundancy Group > Member Screen**

You can select a member and review the following information about the selected member:

- **IP Address**
- **State**—what the module knows about this member
  - Configured—The member is configured on the current module but no additional information is known about the member.
  - Seen—The module has exchanged heartbeats with this member.
  - Invalid—The redundancy group settings on the member (including heartbeat time, discovery time, hold time, redundancy ID, and redundancy protocol version) do not match the configuration on this module.
Redundancy Groups
Configuring a Redundancy Group

- Not Seen—The module can no longer exchange heartbeats with the member.
- Established—The module and this member have successfully established a redundancy group.

- **Last Seen**—the day of the week, the date, the time, and the year that the module last received a heartbeat from this member
- **Adoption Count**—the number of RPs adopted by the member
- **Authorization Level**—the maximum number of RP licenses on this member
- **Mode**—standby or active

If you want to view additional information about the selected member in the redundancy group, click the **Details** button. The **Details** screen is displayed.

![Figure 10-10.Member Details Screen](image)

In addition to the fields listed on the preceding screen, the **Details** screen lists:

- **Image Version**—the software image used by this member.
- **First Seen**—the day of the week, the date, the time, and the year that the module first received a heartbeat from this member
- **HB Sent**—the number of heartbeats that the module has sent to this member
- **HB Received**—the number of heartbeats that the module has received from this member
- **Updates Sent**—the number of updates that the module has sent to this member
Redundancy Groups
Configuring a Redundancy Group

- **Updates Received**—the number of updates that the module has received from this member
- **Radio Portals**—the number of radios adopted by this member (some RPs have two radios)
- **Associated Stations**—the number of stations associated to RPs adopted by this member
- **Rogue AP**—the number of unapproved APs detected by RPs adopted by this member
- **Self Healing Radios**—the number of radios adopted by this member that are configured for self healing

When you have finished reviewing this information, click the **Close** button.

**Setting up Adoption Preference IDs to Control RP Adoption**

Your redundancy group might include more than one active module. In this case, you can use adoption preference IDs to control which Wireless Edge Services zl Module (or Redundant Wireless Services zl Module) adopts particular RPs.

You set an adoption preference ID for both the module and the RPs. If you want a module to adopt an RP, the module’s adoption preference ID should match the RP’s adoption preference ID (which can be set in the radio adoption default configuration or the configuration for a particular RP).

Before configuring adoption preference IDs, consider your goals. Which RPs do you want a particular module to support and why? Sometimes you might want to group RPs in the same general location on the same module in order to simplify roaming. On the other hand, having different modules adopt RPs in the same general location can help build redundancy into your network. In this case, though, remember to set up roaming correctly as described in Chapter 9: “Fast Layer 2 Roaming and Layer 3 Mobility.”

Once you have planned your deployment, begin to configure adoption preference IDs. The following procedure for setting preference IDs gives you the greatest control over RP adoption: you set adoption preference IDs for each RP on each module before you install the RPs.

**Note**

These instructions also apply to Wireless Edge Services zl Modules that are not in a redundancy group but are in the same network.
1. Assign a different adoption preference ID to each active module in the redundancy group. Record the IDs in a table such as Table 10-3 on page 10-27.

2. Assign RPs to the modules that should adopt them. Record the Ethernet MAC addresses for the RPs in a table such as Table 10-3 on page 10-27.

3. On every module in the redundancy group, configure the redundancy settings and enable redundancy. Verify that all members are connected.

4. On every active module in the redundancy group, set the adoption preference ID that you assigned that module in step 1. (See “Configure an Adoption Preference for the Module” on page 10-28.)

5. Have one module adopt all the RPs.
   For example, you could wait to set the country code on the other modules until after the specified module has adopted all RPs. Or you could shutdown the other modules until after the RPs have become adopted.
   You can also push all RPs toward a single module by setting that module’s ID as the ID in the radio adoption default configurations on all modules. Every time that a new RP is added to the network, that RP is adopted by the same module so you know where to look for it.

6. Access the **Network Setup > Radio** screen on the module that has adopted the RPs. Set the correct adoption preference ID for each RP, as explained in “Configure an Adoption Preference for Targeted Radios” on page 10-28.
   For each RP, match the ID for the module that should adopt that RP. You can set the ID for multiple radios at the same time: press the Ctrl key, select the radios, and click the **Edit** button.
   For example, your Wireless LAN System includes these components:
   - one Wireless Edge Services zl Module with adoption preference ID 10, acting in active mode
   - one Redundant Wireless Services zl Module with adoption preference ID 20, acting in active mode
   - ten RP 230s that should be adopted by the primary module
   - five RP 220 that should be adopted by the redundant module
   You have the primary module adopt the 15 RPs. You select the 20 RP 230 radios (two for each RP) and assign them adoption preference ID 10. Then you select the 10 RP 220 radios at assign them adoption preference ID 20.
Redundancy Groups
Configuring a Redundancy Group

7. Copy the targeted radio configurations to every active module in the network.
   You can use the redundancy group configuration mode context to speed this process. For example, you could view the running-config of the module that adopted the RPs and copy the radio configurations. Then paste these commands in the global configuration mode context of the redundancy group configuration mode.

8. After you have created a configuration for every RP in your network on every active module, reset the RPs. The correct module should now adopt each RP.

---

Note

If your redundancy group includes multiple standby members, you might want to control which standby members adopt particular RPs if an active member fails. Assign every standby member an adoption preference ID. Then set the IDs just as you would for a group of active members. On every standby module, make sure that every RP has been assigned one of the IDs used by standby modules.

As always, if the preferred standby member cannot adopt the RP, another standby member will. However, the failover time might be slight greater while the other members of the group wait for the preferred member to adopt the RP.

The following sections explain how to set the adoption preference ID so that you can complete the procedure described above. You can set the ID for:

- a module
- an individual RP
- all newly adopted RPs
### Table 10-3. Assigning Adoption Preference IDs

<table>
<thead>
<tr>
<th>Module (Hostname or IP Address)</th>
<th>Adoption Preference ID</th>
<th>Assigned RPs (MAC Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure an Adoption Preference for the Module

To set an adoption preference for the module itself, complete these steps:

1. Select **Network Setup > Radio** and click the **Configuration** tab.
2. Click the **Global Settings** button. The **Global** screen is displayed. (See Figure 10-11.)

![Network Setup > Radio > Global](image)

**Figure 10-11.Global Settings Screen**

3. In the **Module Adoption Preference ID** field, enter a number, and then click the **OK** button.
4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Configure an Adoption Preference for Targeted Radios

To configure an adoption preference ID for a single radio, follow these steps:

1. Select **Network Setup > Radio > Configuration**.
Redundancy Groups
Configuring a Redundancy Group

Figure 10-12. Network Setup > Radio > Configuration Screen

2. Select the radio or radios to which you want to assign the adoption preference ID.

   Hold down \texttt{Ctrl} while selecting the radios to select multiple radios and assign them the same ID.

3. Click the \texttt{Edit} button. The radios’ \texttt{Edit} screen is displayed.

   If you have selected multiple radios, the screen has limited configurable options. (See Figure 10-13.) However, you can change the adoption preference ID.

4. In the Adoption Preference ID field, enter the ID that you have assigned to the Wireless Edge Services zl Module that should adopt the radio or radios.
Redundancy Groups
Configuring a Redundancy Group

5. Click the **OK** button.

6. Click the **Save** link to copy the radio configurations to the startup-config.

Configure an Adoption Preference for Newly Adopted Radios

To configure an adoption preference ID for all adopted RPs, edit the radio adoption default configuration. Complete these steps:

1. Select **Network Setup > Radio Adoption Defaults** and click the **Configuration** tab.
2. Select a radio type and click the **Edit** button. The **Configuration** screen is displayed. (See Figure 10-15.)
3. Under **Advanced Properties**, in the **Adoption Preference ID** field, enter a preference ID, and then click the **OK** button.

4. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

To force another module to adopt a particular RP, change its radio preference ID to match the ID on that second module, as explained in “Configuring Advanced Properties for a Particular Radio” on page 3-33 in *Chapter 3: “Radio Port Configuration.”*
Reverting RPs Adopted by a Standby Member to the Active Member

When an active member of a redundancy group fails, a standby member of the group adopts the RPs. For continuity of service, the standby member continues to support the RPs even when the active member comes back online. However, eventually you may want to return the RPs to the original module.

You can manually revert a standby module, which means that you force it to unadopt all of its RPs. Only revert a module when you can afford a disruption to network service for the minute or two during which RPs become adopted by the active module.

You are allowed to revert a module when all of these conditions are met:
- The module is a standby member of the group.
- The module has adopted a failed member’s RPs.
- The module has detected that the failed member has returned online.

If the module has adopted RPs from more than one failed member, all must be recovered.

**Note**

Your redundancy group configuration might define multiple modules as active members. In some circumstances, another active member can adopt a failed member’s RPs. (See “Redundancy Group Behavior When a Member Fails” on page 10-10.) However, you cannot revert an active member.

Follow these steps to have a standby member relinquish its RPs:
1. Select **Network Setup > Redundancy Group > Configuration**.
2. Click the **Revert Now** button.

   The button is active only if the three conditions described above are met.
Redundancy Groups
Configuring a Redundancy Group

Figure 10-16. Revert Now Button in the Network Setup > Redundancy Group > Configuration Screen

The module immediately unadopts all RPs when you click the button. The RPs are adopted by any active member that can accept them, not necessarily the recovered module. However, either load balancing or adoption preference IDs, will probably guide most of the RPs toward the recovered module.
RADIUS Server

Contents

Overview .......................................................... 11-2
RADIUS Authentication ........................................... 11-3
  Configuring the Internal RADIUS Server ................. 11-4
    Choosing the Authentication Type for 802.1X/EAP .... 11-5
    Specifying the RADIUS Server’s Digital Certificate ... 11-8
    Choosing the Source for User Credentials .............. 11-9
  Configuring the Local RADIUS Database ................. 11-12
  Using LDAP for the Data Source ......................... 11-19
  Specifying a Domain Proxy RADIUS Server ............... 11-27
  Specifying Global RADIUS Settings ..................... 11-30
  Adding RADIUS Clients .................................. 11-31
  Starting and Stopping the RADIUS Server ............... 11-32
  Enabling Authentication to the Internal Server on a WLAN ...... 11-33
RADIUS Accounting .............................................. 11-37
  Enabling Accounting to the Internal RADIUS Server on a WLAN ......................... 11-39
  Viewing the Internal RADIUS Server’s Accounting Logs .... 11-43
Overview

A Remote Access Dial In User Service (RADIUS) server provides centralized authentication (and sometimes accounting) for a network. The RADIUS protocol regulates communications between network access servers (NASs) and RADIUS servers.

The NASs are devices such as switches and Wireless Edge Services zl Modules, which provide network access to stations. First, however, they can force the stations to authenticate themselves.

Although the NAS enforces authentication, it does not decide whether a particular station is authenticated. Instead it submits an authentication request for the station to the RADIUS server. The RADIUS server decides whether a station can connect to the network according to the user’s credentials and the policies configured on the server.

The Wireless Edge Services zl Module acts as a NAS when it enforces 802.1X, Web authentication (Web-Auth), or MAC authentication. In addition to forwarding authentication requests to an external RADIUS server, the module can make decisions with its internal server. In this second case, the module acts as the NAS and as the RADIUS server.

You learned about configuring settings for an external RADIUS server in Chapter 4: “Wireless Local Area Networks (WLANs).” In this chapter, you will learn how to configure the module’s internal RADIUS server.

The Wireless Edge Services zl Module's internal RADIUS server can provide the following services:

- authenticating users who attempt to connect to a wireless LAN (WLAN) that requires authentication to a RADIUS server
- responding to authentication requests from network access servers (NASs) in the wired network
- creating accounting logs of user activity on a WLAN
RADIUS Authentication

The Wireless Edge Services zl Module’s RADIUS authentication server fulfills these roles:

- decides whether a user can connect to a WLAN that enforces one of these types of security:
  - 802.1X
  - Web authentication (Web-Auth)
  - MAC authentication
- makes the decision based on credentials stored in one of these locations:
  - user accounts configured on the module itself
  - user accounts on a Lightweight Directory Access Protocol (LDAP) server, such as Novell eDirectory
- specifies policies (such as a dynamic virtual LAN (VLAN) assignment) for authenticated users

For 802.1X authentication, the module’s internal RADIUS server supports these Extensible Authentication Protocol (EAP) methods:

- EAP-Transport Layer Security (TLS)
- EAP-Tunneled TLS (TTLS) with Message Digest 5 (MD5)
- EAP-TTLS with Password Authentication Protocol (PAP)
- Protected EAP (PEAP) with Generic Token Card (GTC)
- PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2)

All of these methods are suitable for a wireless network. That is, they not only enable a wireless user to authenticate securely, they also help the Wireless Edge Services zl Module and the station to generate a unique encryption key for the association. This key can be either for Wired Equivalent Privacy (WEP) or the more secure Wi-Fi Protected Access (WPA).

Table 11-1 summarizes the characteristics of these different EAP types.
### Configuring the Internal RADIUS Server

You must complete the following steps to configure the internal RADIUS server to authenticate users that connect to a WLAN:

1. Select the authentication type.
2. Specify the internal RADIUS server’s digital certificate.
3. Select the source for policies and credentials:
   - If you select the local database, create groups and user accounts.
   - If you select a LDAP-compliant server, configure the LDAP settings and create a group.
4. Restart the RADIUS server.
5. Specify the internal server (loopback address) as the RADIUS server for one or more WLANs.

### Table 11-1. EAP Methods

<table>
<thead>
<tr>
<th>EAP Type</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>The wireless station and the module’s RADIUS server exchange digital certificates in a three-step TLS handshake.</td>
</tr>
</tbody>
</table>
| EAP-TTLS with MD5 | • The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.  
                     • Inside the secure tunnel, the wireless station submits a username and a hashed (MD5) password. |
| EAP-TTLS with PAP | • The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.  
                     • Inside the secure tunnel, the wireless station sends a PAP request. |
| PEAP with GTC     | • The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.  
                     • Inside the secure tunnel, the wireless station submits a GTC packet with its username and a password. |
| PEAP with MS-CHAP v2 | • The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.  
                           • Inside the secure tunnel, the wireless station submits a username and a password using the MS-CHAP v2 protocol. |
Depending on your environment, you might also need to complete these tasks:

- **Specify proxy RADIUS servers to which the local RADIUS server forwards queries**—This step allows the Wireless Edge Services zl Module to relay authentication requests in certain domains to external servers.

- **Specify RADIUS clients, which query the local RADIUS server**—This step allows the module to authenticate users who connect to different NASs—in both the wired and wireless network.

Whenever you make a change to the RADIUS settings, the Web browser interface will ask you to restart the RADIUS server. (See Figure 11-1).

![Figure 11-1. Restarting the RADIUS Server](image)

Click the **Yes** button.

**Choosing the Authentication Type for 802.1X/EAP**

For 802.1X authentication, you must select the EAP method with which the RADIUS server authenticates users. Users' wireless client utilities must be configured for the same EAP method. Table 11-2 lists the available options, including the requirements for each. Refer to this table when you add the user's account.
Table 11-2. Internal RADIUS Server EAP Methods

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Server Credentials</th>
<th>Station Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>Digital certificate</td>
<td>Digital certificate</td>
</tr>
<tr>
<td>EAP-TTLS with MD5</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-TTLS with PAP</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-PEAP with GTC</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-PEAP with MSCHAPv2</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
</tbody>
</table>

**Note**

You do not have to select any particular protocol to use the module’s internal RADIUS server for Web-Auth or MAC authentication.

To select the method, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
2. From the **802.1X EAP/Auth Type** drop-down menu, select a method. Select all to allow users to authenticate with any of the supported methods.

3. Next, choose your server’s digital certificates (explained in the section below). Or click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.
Specifying the RADIUS Server’s Digital Certificate

As an authentication server, the Wireless Edge Services zl Module requires various certificates:

- a server certificate
  
  No matter which EAP type you select, the internal RADIUS server must authenticate itself using a digital certificate.

  By default, the module identifies itself to users with the server certificate in the default-trustpoint. This certificate is installed on the module when it ships and is self-signed with the name Hewlett-Packard.

  Alternatively, the module can authenticate itself with one of these certificates:
  
  • a self-signed certificate that you create on the module
  • a digital certificate signed by a trusted certificate authority (CA) and installed on the module

- a CA certificate
  
  The Wireless Edge Services zl Module uses the public key in the CA certificate to verify certificates signed by that CA.

  For example, for EAP-TLS, the RADIUS server checks users’ digital certificates. So the server needs the CA certificate for the CA that signed the users’ digital certificates.

On the Wireless Edge Services zl Module, you create trustpoints and load certificates into those trustpoints. Install the correct certificates before completing the following tasks for the RADIUS server:

- selecting which of the module’s own digital certificates it should use to authenticate to users (mandatory)
- selecting which of the module’s CA certificates it should use to authenticate users (for EAP-TLS)

See “Digital Certificates” on page 2-166 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module” for instructions on creating trustpoints.
Then follow these steps:

1. Select **Network Setup > Radius Server** and click the **Authentication** tab.

2. In the **Cert Trustpoint** drop-down menu, select the trustpoint in which you have loaded the server certificate for RADIUS authentication.

   Selecting **<Create a New Certificate>** opens the Certificates Wizard and guides you through the creation or installation of certificates.

3. If you have selected EAP-TLS, choose a trustpoint from the **CA Cert Trustpoint** drop-down menu.

   Select the trustpoint in which you loaded the CA certificate for the CA that signs users’ digital certificates. This trustpoint should typically match the one you selected for the **Cert Trustpoint**.

   Again, you can select **<Create a New Certificate>** to open the Certificates Wizard.

4. Next choose the source for authentication data (explained in the section below). Or click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.

Choosing the Source for User Credentials

The RADIUS server can draw on one of two potential databases for authenticating users:

- **its local database**
  
  In addition to checking a user’s credentials against user accounts its local database, the RADIUS server verifies that the user is connecting at an allowed time (specified in the user’s assigned group).

  After authenticating a user, the Wireless Edge Services zl Module can place that user in a dynamic VLAN (also specified in the user’s assigned group).

- **an LDAP-compliant directory server**
  
  The module’s RADIUS server binds to the directory server and looks up users’ credentials.

To select the database, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
Figure 11-3. Choosing the Source for Credentials

2. In the **Auth Data Source** field, use the drop-down menu to select the source for policies and credentials, either **local** or **ldap**.

3. Click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.

4. Click the **Save** link to copy the configuration to the startup-config.
Depending on your choice, you must complete one of the following tasks:

- configure the local database (see “Configuring the Local RADIUS Database” on page 11-12)
- configure LDAP server settings and at least one group in the local database (see “Using LDAP for the Data Source” on page 11-19)

Table 11-3 explains the requirements for configuring credentials for each EAP method, depending on whether the Wireless Edge Services zl Module uses its local database or an LDAP server for the data store.

**Table 11-3. Requirements for Credentials Depending on EAP Method**

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Requirement for Credentials in Local Database</th>
<th>Requirement for Credentials on LDAP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Host certificates (issued by the same CA) loaded on the wireless stations&lt;br&gt;• CA certificate loaded on both the module and stations&lt;br&gt;• Usernames submitted with host certificates added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Host certificates (issued by the same CA) loaded on the wireless stations&lt;br&gt;• CA certificate loaded on both the module and stations&lt;br&gt;• Host certificate loaded in the user account on the LDAP server</td>
</tr>
<tr>
<td>EAP-TTLS with MD5</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>EAP-TTLS with PAP</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>PEAP with GTC</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>PEAP with MS-CHAP v2</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
</tbody>
</table>
Configuring the Local RADIUS Database

You must complete the following tasks to configure the local database:

1. Create groups, which define policies for users.
2. Add user accounts to the group.

Creating a Group. A group defines policies on the Wireless Edge Services Module’s internal RADIUS database, including:

- the dynamic VLAN for authenticated users in this group
- when users in this group are allowed to connect to the network

You can create two types of groups:

- a normal group
- a guest group, which only allows temporary guest accounts

To configure a group, complete these steps:

1. Select Network Setup > Radius Server and click the Groups tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Guest Group</th>
<th>VLAN ID</th>
<th>Time of Access Start</th>
<th>Time of Access End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>✓</td>
<td>0000</td>
<td>0000</td>
<td>1659</td>
</tr>
<tr>
<td>Faculty</td>
<td>✗</td>
<td></td>
<td>0000</td>
<td>2359</td>
</tr>
<tr>
<td>Students</td>
<td>✗</td>
<td>120000</td>
<td>120000</td>
<td>2359</td>
</tr>
</tbody>
</table>

Figure 11-4. Configuring RADIUS Server Groups
2. Click the **Add** button. The **ADD** screen is displayed.

![Network Setup > Local RADIUS Server > ADD](image)

3. In the **Name** field, enter a meaningful name—for example, “Faculty.”

4. In the **VLAN ID** field, enter the dynamic VLAN for users in this group.

   If you enter 0, the Wireless Edge Services zl Module assigns the user to the VLAN configured for the user’s WLAN.

   You should not use dynamic VLANs with Web-Auth. The user’s station receives an IP address in the static VLAN before the user can log in and receive the dynamic VLAN assignment.

**Note**

You must enable dynamic VLANs in the WLAN to which users connect for this setting to take effect. See “Enabling Authentication to the Internal Server on a WLAN” on page 11-33.
5. Specify the times of day when users in this group can connect to the wireless network.
   a. In the **Time of Access Start** field, enter the earliest time that users can connect.
   b. In the **Time Access End** field, enter the latest time users can connect. Always enter times in four digits, the first two digits being the hour in the 24-hour clock and the second two digits being the minutes. As shown in Figure 11-5, by default, users can connect at any time of the day or night.

6. In the **Time of access in days** section, check the boxes to specify the days of the week when users in this group can connect to the wireless network. By default, network access is available every day.

7. Check the **Guest Group** box if you want this group to be for guests. Guests have temporary accounts. (See “Creating User Accounts” on page 11-15.)

8. Click the **OK** button.

The group is displayed in the top section of the **Network Setup > Local RADIUS Server > Groups** screen. Information and policies for the group are listed in these columns:

- **Name**—the name of the group
- **Guest Group**—displays a red X for normal groups and a green check for guest groups
- **VLAN ID**—the dynamic VLAN for users in this group (if dynamic VLANs are enabled for the WLAN to which the user associates)
- **Time of Access Start**—the time at which users in this group can begin connecting to the network
- **Time of Access End**—the time at which users in this group can no longer connect to the network (even if they enter the correct password)

The **Time of access in days** section of the **Network Setup > Local RADIUS Server > Groups** screen includes a box for each day of the week. When you select a group, the boxes are checked for days on which users in that group can connect to the network.

You can modify these settings for a group:

- VLAN ID
- time of access start and end
- days access is allowed
To modify a group, select it and click the **Edit** button. In the **EDIT** screen that is displayed, configure the settings just as you would for a new group. (However, you cannot change the group’s name nor whether it is a normal or guest group.) When you are finished, click the **OK** button.

To delete a group, select it in the **Network Setup > Local RADIUS Server > Groups** screen and click the **Delete** button. The Web browser interface asks you to restart the RADIUS server for the change to take effect.

**Creating User Accounts.** You must configure a user account for every user allowed to connect to your network. This requirement holds true whether the internal RADIUS server authenticates users with passwords or with digital certificates.

Just as the Wireless Edge Services zl Module’s RADIUS server defines two types of groups, it defines two types of user accounts:

- a normal account
- a guest account

Normal users can only join normal groups, and guest users can only join guest groups.

You configure the following parameters for user accounts:

- username
- if you are using TTLS or PEAP, a password
- if the account is a guest account, an expiration time

To configure an account, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Users** tab.
2. Click the **Add** button. The **ADD** screen is displayed.
3. In the **User ID** field, enter the username.

   The username can be up to 64 characters and can include alphanumeric and special characters.

4. Check the **Guest User** box if this is a temporary account for a guest.

5. In the **Password** and **Confirm Password** fields, specify the user’s password.

   The password can be up to 21 characters and can include alphanumeric and special characters.
By default, this password is displayed in plaintext in the Wireless Edge Services zl Module's configuration. To learn how to encrypt the password, see “Password Encryption” on page 2-105 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”

6. For a guest user, you must specify the period during which the account is active.

As soon as you check the Guest User box, the OS creates a default period, which begins at the current time (shown in the Current Switch Date field) and ends 24 hours after the current time. See Figure 11-7.

Figure 11-7. Creating a Guest User in the Local RADIUS Database
The guest account is active only for the period between the two times. To alter the times, follow these steps:

a. In the **Start Date & Time** field, enter the date and time at which this account is enabled.

   Enter the date in this format, in which **MM** is the number of the month, **DD** is the date, and **YYYY** is the year:

   **MM/DD/YYYY**

   After the date, enter a hyphen (-) and the time in this format, in which **HH** is the hour in the 24-hour clock and **MM** is the minutes:

   **HH:MM**

   For example, enter:

   02/17/2007-08:00

   By default, the account’s start date and time is the current time.

b. In the **Expiry Date & Time** field, enter the date and time at which this account is disabled.

   Use the same format as for the **Start Date and Time** field. Of course, the expiry time must be later than the start time.

   After the account expires, it may remain listed in the **Network Setup > Local RADIUS Server > Users** screen. The Wireless Edge Services zl Module automatically clears out expired accounts every 24 hours. In the meantime, however, no one can use the expired account to connect.

7. In the **Available Groups** section, which lists all groups configured for this type of user, select a group and click the **Add** button. The group enters the **Configured Groups** section.

   For example, in Figure 11-6, the user is a normal user (the **Guest User** box is not checked), so the normal groups are displayed.

8. You can repeat step 6 and assign the user to multiple groups. However, it is recommended that you assign the user to one group only.

   Only assign a user to more than one group when the groups allow access at mutually exclusive times. The policy configured for the group that currently allows access takes effect.

   For example, you could create a Weekdays group and a Weekend group and assign the groups to different VLANs. A user that is a member of both groups would be placed in the Weekdays VLAN on Friday, but in the Weekend VLAN when she logs in on Saturday.
You must never assign a user to groups with overlapping access days or times: such a configuration prevents you from determining which policy applies to the user during the overlapping times. For example, if one group allows access at all times and another group allows access only during normal work hours, you cannot assign a user to both groups. During the day, the policies would conflict.

9. Click the **OK** button.

The user account is displayed in the **Network Setup > Local RADIUS Server > Users** screen. Information about the account is listed in these columns:

- **User ID**—the username
- **Guest User**—displays a red X for normal accounts and a green check for guest accounts
- **Start Date**—the date and time at which a guest account becomes active (not applicable to normal accounts, which are immediately active)
- **Expiry Date**—the date and time at which the guest account becomes no longer active (not applicable to normal accounts, which are permanent)

When you select an account, the group or groups for the user are displayed in the **Assigned Groups** section.

To modify an account, select it and click the **Edit** button. The **EDIT** screen, which is similar to the **Add** screen, is displayed.

In the **EDIT** screen, you can change the user’s password and group assignments. However, you cannot alter the username or the definition of the account as a normal or guest account. When you have finished your modifications, click the **OK** button.

To delete an account, select it in the **Network Setup > Local RADIUS Server > Users** screen and click the **Delete** button. When prompted, click **OK** to restart the RADIUS server and apply the change.

Every 24 hours, the Wireless Edge Services zl Module checks the local RADIUS server database and removes any expired guest accounts.

**Using LDAP for the Data Source**

The Wireless Edge Services zl Module’s internal RADIUS server can authenticate users against an LDAP data source. To authenticate successfully, a user must meet these conditions:

- has an account stored on the directory server
enters a password that matches the password in this account (or, for TLS, has a valid digital certificate)

is listed in the directory as member of a group currently allowed access

The internal RADIUS server verifies that these conditions are met. To do so, it must bind to the LDAP server and perform searches, looking up the user’s account and group memberships and verifying the user’s password. See “Configuring the Internal RADIUS Server to Bind to an LDAP Server” on page 11-20.

To determine whether the user’s group is currently allowed access, the server checks the policy stored for that group on its internal database. See “Configuring Groups for Use with an LDAP Server” on page 11-24.

**Configuring the Internal RADIUS Server to Bind to an LDAP Server.**

If you select LDAP as the source for policies and user accounts, you must enable the Wireless Edge Services z1 Module to communicate with your company’s LDAP server.

The internal RADIUS server performs these functions:

- It binds to the LDAP server.
  
  To complete the binding, the server submits a distinguished name and password to the LDAP server. You must specify the name and password of an account with administrative rights. In addition, you must specify the base directory in which the administrator account is stored.

- It searches the LDAP server’s directory to check the user’s credentials and group memberships.

  You must configure filter strings, which the internal RADIUS server uses to retrieve information from the directory:

  - With the user login filter, the internal RADIUS server verifies that the supplicant has an account and that his or her password matches the password in that account.

  - With the group login filter, the internal RADIUS server checks that the supplicant is a member of a group that is allowed access.

  You must also specify the names of attributes that the RADIUS server retrieves during these searches, including the password and group memberships.

To configure LDAP settings, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
2. From the **Auth Data Source** drop-down menu, select **ldap**.

3. In the **LDAP Server Details** section, click the **Primary** tab.

4. In the **IP Address** and **Port #** fields, specify your LDAP server's IP address and port.

   The port number can be from 1 through 65535. The default port for LDAP is 389.
5. Configure the information that the internal RADIUS server submits to bind to the LDAP server:
   a. In the **Bind DN** field, enter the distinguished name for an administrator account on the LDAP server.
      For example, enter:
      
      \texttt{cn=Administrator,dc=mydomain,dc=com}
      
      The administrator account must be in the domain that you specify in step 5.
   b. In the **Bind Password** field, enter the password for the name that you specified above.

6. In the **Base DN** field, enter the name of the domain in which the module begins searching for user accounts.
   For example, enter:
   
   \texttt{cn=Users,dc=mydomain,dc=com}

7. In the **User Login Filter** field, enter a filter string that searches for a user’s account based on the username submitted during EAP.
   An example of a user login filter is:
   
   \texttt{(sAMAccountName=%{Stripped-User-Name})}

   Another example is:
   
   \texttt{(uid=%{Stripped-User-Name}:{User-Name})}

   The purpose of this filter is to verify that the LDAP server has a particular user account—an account that matches the username that the user enters.

   The syntax follows that for standard LDAP searches.

   First, you enter the name of the attribute that your LDAP server uses to store a username. This attribute might be “uid,” “sAMAccountName,” or “cd.”

   Next, set the attribute equal to the username submitted through EAP. This username is specified by one or both of the following:
   
   - %{Stripped-User-Name}
   - %{User-Name}

   These strings configure the internal RADIUS server to submit the username *without* appending a domain name. Make sure that the attribute you chose lists the username in this form.
8. In the **Password Attribute** field, specify the attribute that stores a user’s password.

When looking up a user’s account, the internal RADIUS server also requests a check on the user’s password (or, depending on the EAP type, a hash of that password). The string that you enter in the **Password Attribute** field determines the attribute name that the server requests.

Match the attribute name used by your LDAP server—commonly “user-Password” or “User-Password.”

9. In the **Group Filter** field, enter a filter string that searches for the groups to which the user belongs.

This purpose of the group filter is to verify that the user is a member of the group on the local RADIUS server that currently allows access.

An example of a group filter is:

\[
&(objectClass=Group)(member=%{Ldap-UserDn}))
\]

The first part of this filter tells the internal RADIUS server to search only for group type objects. “Group” is one example of the name for this object class. Other examples include:

- **GroupOfUniqueNames**
- **GroupOfNames**

The second part of the filter configures the internal RADIUS server to search only for groups in which this user is a member. First enter the name of the attribute that your LDAP server uses to list the members of a group. In this example, that attribute is “member.” Another example is “unique-member.” Next, set this attribute equal to this variable:

\%

This variable configures the module to submit the username as an LDAP distinguished name. To create this name, the module adds the username to the base distinguished name. For example:

\[cn=user,cn=Users,dn=mydomain,dn=com\]

Make sure that the name produced is the user’s correct distinguished name.

The internal RADIUS server automatically adds this string to the filter:

\(<\text{group attribute}>=<\text{local group name}>\)
The RADIUS server replaces `<group attribute>` with the string that you enter in the Group Attribute field. (See step 11). The server replaces `<local group name>` with the name of the group configured in the local RADIUS database.

10. In the Group Membership Attribute field, specify the attribute that stores a user's group memberships.

The internal RADIUS server requests this attribute in the search for the user accounts. The attribute is commonly named “memberOf” or “radius-GroupName.”

11. In the Group Attribute field, specify the attribute that your LDAP server uses to store the name of a group object.

The internal RADIUS server uses this attribute as part of the search with the group filter. See step 9 for more information about this search.

12. In the Net Timeout field, enter a time from 1 through 10 seconds.

If the Wireless Edge Services zl Module does not receive a response within this time, it considers the LDAP server unreachable. If you have configured a secondary LDAP server, the module contacts it. Otherwise, authentication fails.

13. Optionally, click the Secondary tab in the LDAP Server Details section.

Repeat steps 4 through 12 to configure the secondary LDAP server.

14. Click the Apply button.

15. Click the Save link to save your configuration to the startup-config.

You can edit LDAP setting by changing the appropriate fields and clicking the Apply button. Whenever you change a setting, you must re-enter the bind password.

You can also remove all settings for a particular LDAP server at once:

1. Click the server's tab (Primary or Secondary).

2. Check the Delete Primary Ldap server or Delete Secondary Ldap server box.

3. Click the Apply button and save your configuration to the startup-config.

**Configuring Groups for Use with an LDAP Server.** To authenticate users, the Wireless Edge Services zl Module's internal RADIUS server requires at least one group policy. If you are using an LDAP server as the data source, the group name must match the name of wireless users' group as stored on the LDAP server.
Follow these steps to configure the group and set policies for it:

1. Select **Network Setup > Radius Server** and click the **Groups** tab.

![Figure 11-9. Configuring RADIUS Server Groups](image-url)
2. Click the Add button, The ADD screen is displayed.

![Figure 11-10. Adding a RADIUS Server Group](image)

3. In the Name field, enter a name that matches the name of a group on your directory server. This is the group that is allowed wireless access; make sure that all potential wireless users are members. (Or create multiple groups.)

   The name you assign the group must match exactly the group name as stored on your LDAP server. The LDAP server might use several attributes to name the group. The Group Attribute field, in the LDAP bind settings, specifies the attribute that the group name matches. (See step 9 on page 11-23.)

   For example, you specify “cn” for the group attribute. The cn of the group for wireless users is listed as “Wireless Users” on the directory server. So you enter “Wireless Users” in the Name field.

4. In the VLAN ID field, enter the dynamic VLAN for users in this group.

   If you leave the ID at 0, the Wireless Edge Services zl Module assigns the user to the static VLAN associated with the user’s WLAN.
You should be careful when using dynamic VLANs with Web-Auth. The user’s station receives an IP address in the static VLAN before the user can login and receive the dynamic VLAN assignment. So you must set the lease for the DHCP address in the static VLAN very low. Then the station will automatically renew its address soon after it receives the dynamic assignment.

**Note**

You must enable dynamic VLANs in the WLAN to which users connect for this setting to take effect. See “Enabling Authentication to the Internal Server on a WLAN” on page 11-33.

5. Specify the times of day when users in this group can connect to the wireless network.
   a. In the **Time of Access Start** field, enter the earliest time that users can connect.
   b. In the **Time Access End** field, enter the latest time users can connect.

   Always enter times in four digits, the first two digits being the hour in the 24-hour clock and the second two digits being the minutes.

   If a user is already logged in, and the end access time passes, the user remains logged in. However, the next time the user’s station re-authenticates, the re-authentication fails. You can require period re-authentication in the WLAN’s RADIUS settings. See “Enabling Authentication to the Internal Server on a WLAN” on page 11-33.

   As shown in Figure 11-5, by default, users can connect at any time of the day or night.

6. In the **Time of access in days** section, check the boxes to specify the days of the week when users in this group can connect to the wireless network. By default, network access is available every day.

7. Click the **OK** button.

For more information about managing groups, see “Creating a Group” on page 11-12.

**Specifying a Domain Proxy RADIUS Server**

The Wireless Edge Services zl Module’s internal RADIUS server can query external RADIUS servers to authenticate users in a different domain.
To specify the proxy RADIUS server, complete these steps:

1. Select **Network Setup > Local RADIUS Server > Configuration**.

   ![Figure 11-11. Network Setup > Radius Server > Configuration Screen](image)

2. In the lower section of the screen, click the **Domain Proxy Servers** tab.

3. Click the **Add** button. The **ADD** screen is displayed.
4. In the **Realm Name** field, enter the domain name for users who authenticate to the domain proxy server.

When a user submits his or her username, the Wireless Edge Services zl Module’s internal server checks the domain name. If this name matches the name in the **Realm Name** field, the internal RADIUS server queries the proxy server specified below.

For example, you enter “procurve.com” in the **Realm Name** field. If a user enters “Joe” as his username, the internal RADIUS server uses its local database to authenticate him. If the user enters “Joe@procurve.com,” the internal server uses the proxy server to authenticate Joe.

The internal RADIUS sends the username to the proxy server with the full domain extension.

The domain name can be up to 50 alphanumeric and special characters.

5. In the **IP Address** and **Port Number** fields, specify the external RADIUS server’s IP address and port. The default port for RADIUS is 1812.

6. In the **Shared Secret** field, enter a string, which can include up to 31 alphanumeric and special characters.

The Wireless Edge Services zl Module must be configured as a RADIUS client on the external RADIUS server, and the client configuration must include this exact shared secret.

7. Click the **OK** button.

The external RADIUS server is now displayed in the **Domain Proxy Servers** section.
Specifying Global RADIUS Settings

Global RADIUS settings regulate the Wireless Edge Services zl Module’s RADIUS server’s communications with proxy RADIUS servers.

To configure these settings, follow these steps:

1. Select Network Setup > Local RADIUS Server > Configuration.

2. In the Timeout field, specify how long, in seconds, the module should wait for a response to a request to a domain proxy server.

   The default timeout is 5 seconds, and the valid range is from 5 to 10 seconds. You might select a longer time for a busy network.

8. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.
3. In the **Retries** field, specify the number of times the module should re-send a proxy request that times out.

   The default number of retries is 3 (which means that the module will send up to four requests). Valid values are from 3 to 6.

4. Click the **OK** button to apply the settings, remembering to save your configuration by clicking the **Save** link.

### Adding RADIUS Clients

The Wireless Edge Services zl Module’s internal RADIUS server typically authenticates wireless users connecting to its own WLANs. But it can also authenticate users throughout your network—on both the wireless and the wired side. Simply add the NASs for those users as RADIUS clients. For example, you can add a ProCurve Intelligent Edge Switch, or you can add another Wireless Edge Services zl Module.

To specify a RADIUS client, complete these steps:

1. Select **Network Setup > Local RADIUS Server > Configuration**.
2. In the lower section of the screen, click the **Clients** tab.
3. Click the **Add** button. The **ADD** screen is displayed.

4. In the **IP Address/Mask** fields, enter the client device’s IP address, including the CIDR prefix length for its subnetwork.

   If you specify a subnetwork address and prefix length, any device in that subnetwork can act as a RADIUS client (as long as it sends the correct password, specified in step 5). For example, you specify 10.4.10.0/24. NASs with IP addresses 10.4.10.10 and 10.4.10.120 can both contact the Wireless Edge Services zl Module’s RADIUS server.

---

**Figure 11-14.Adding a RADIUS Client**
If the client has more than one IP address, make sure to specify the address that it includes in RADIUS requests.

5. In the **Shared Secret** field, enter the client’s password.
   Of course, you must specify this same password when you configure the client device to query this module.

6. Click the **OK** button. The client is displayed in the **Network Setup > Radius Server > Configuration** screen under the **Clients** tab.

7. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

### Starting and Stopping the RADIUS Server

You must restart the RADIUS server for configuration changes to take effect. The Web browser interface automatically asks you to restart the server whenever you make a configuration. You can also manually stop and start the server from the **Network Setup > Radius Server > Configuration** screen.

The **Global Settings** section indicates whether the server is running:
- **“Start the RADIUS server”—The server is currently disabled.**
- **“Stop the RADIUS server”—The server is currently enabled.**

To change the RADIUS server’s status, click link portion of the indication. To disable the server, click the **Stop** link. To re-enable a stopped server, click the **Start** link.

In either case, a screen is displayed, informing you of the change in status.

![Status](image)

**Figure 11-15.Restarting the RADIUS Server**

Click the **OK** button to close the screen, remembering to save your configuration by clicking the **Save** link.
Enabling Authentication to the Internal Server on a WLAN

WLANs that use the following authentication methods require authentication to a RADIUS server:

- 802.1X
- Web-Auth
- MAC Authentication

In Chapter 4: “Wireless Local Area Networks (WLANs),” you learned how to configure a WLAN to require authentication to an external RADIUS server.

This section explains how to configure the Wireless Edge Services zl Module’s internal RADIUS server to take over authentication.

You must enter 127.0.0.1 for the RADIUS server’s IP address. The shared secret field does not matter.

To configure 802.1X authentication to the internal RADIUS server, complete these steps:

1. Select Network Setup > WLAN Setup > Configuration.
2. Select the WLAN from the list and click the Edit button. The Edit screen for the WLAN is displayed.
3. If you have configured the RADIUS server to place users in dynamic VLANs, check the Dynamic Assignment box.

4. Configure other WLAN settings as described in Chapter 4: “Wireless Local Area Networks (WLANs).”

5. In the Authentication section, select 802.1X EAP, Web-Auth, or MAC Authentication.

6. Click the RADIUS Config… button at the bottom of the screen. The Radius Configuration screen is displayed.
7. Specify 127.0.0.1 in the primary RADIUS server’s RADIUS Server Address field.
8. Do not enter anything in the **RADIUS Shared Secret** field.

   By default, the module can communicate with the internal server. If you enter a string in this field, the module’s internal server will no longer work on this WLAN. If you do change the secret, you can fix the problem in one of two ways:

   - Clear the **RADIUS Shared Secret** field and click **OK**. The secret returns to the default.
   - Configure the loopback interface (127.0.0.1) as a client for the internal RADIUS server. Specify the new secret for the client. See “Adding RADIUS Clients” on page 11-31.

9. If you want the module’s RADIUS server to periodically re-authenticate stations, check the **Re-authentication** box. Then specify how often (in seconds) stations re-authenticate in the **Re-authentication Period** field.

   The valid range for the re-authentication period is 30 to 65535 seconds (about 18 hours). The default setting is 3600 seconds (1 hour).

10. Choose **CHAP** or **PAP** for the **Authentication Protocol**.

    This setting determines how the Wireless Edge Services zl Module forwards MAC authentication or Web-Auth credentials to an external server. The module’s internal RADIUS server supports both protocols. However, if you choose PAP, users’ passwords display in plaintext in logs. Generally, you should choose CHAP for higher security.

11. Click the **OK** button.

12. On the **Edit** screen, click the **OK** button.

13. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.
RADIUS Accounting

RADIUS accounting tracks users’ activity and consumption of network resources. NASs, such as the Wireless Edge Services zl Module, send reports that summarize users’ activity to a centralized RADIUS accounting server. A company might analyze the reports for security auditing and traffic management. Or the company might submit the reports to a billing server in order to charge users for wireless access.

The Wireless Edge Services zl Module can implement RADIUS accounting in one of two ways:

■ It can report to an external RADIUS server.
■ It can report to its internal RADIUS server.

The module can send the following messages:

■ **Stop messages**—when a station disconnects from a wireless LAN (WLAN)
■ **Start messages**—when a station connects to a WLAN
■ **Interim messages**—at set intervals throughout the station’s session

You choose which messages the module sends.

A message includes information such as the identity of the user, the duration of the session, and the bandwidth consumed. Table 11-4 shows a complete list of fields in the report. Some fields are present in all messages; others are specific to certain types of messages.
### Table 11-4. Information in a RADIUS Accounting Log

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>user’s username</td>
</tr>
<tr>
<td>Acct-Status-Type</td>
<td>state of connection and type of message—start, stop, or interim</td>
</tr>
<tr>
<td>Acct-Session-ID</td>
<td>unique ID for each session</td>
</tr>
<tr>
<td>Calling-Station-ID</td>
<td>station’s MAC address</td>
</tr>
<tr>
<td>Called-Station-ID</td>
<td>MAC address of the port to which the station connects—for a wireless connection, the radio’s MAC address</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>ID of the NAS’s port—for example, the port number on a switch</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>the type of connection—for example Wireless 802.11</td>
</tr>
<tr>
<td>NAS-IP-Identifier</td>
<td>NAS’s IP address—when the module is the NAS, 127.0.0.1</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>NAS’s hostname</td>
</tr>
<tr>
<td>Event-Timestamp</td>
<td>date and time (including timezone) at which the event that triggered the message occurred</td>
</tr>
<tr>
<td>Acct-Delay-Time</td>
<td>specifies how long the RADIUS client has attempted to transmit the message</td>
</tr>
<tr>
<td>Acct-Authentic</td>
<td>the method by which the station authenticated</td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>IP address of the RADIUS client (typically the NAS, but sometimes another RADIUS server) that forwarded this message</td>
</tr>
<tr>
<td>Acct-Unique-Session-Id</td>
<td>a value that identifies the station’s session; all messages for a particular session have the same ID</td>
</tr>
<tr>
<td>Timestamp</td>
<td>message’s timestamp</td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td>• number of packets received by the station over the entire duration of the session (stop message)</td>
</tr>
<tr>
<td></td>
<td>• number of packets received by the station since the beginning of the session (interim message)</td>
</tr>
<tr>
<td>Acct-Output-Packets</td>
<td>• number of packets sent by the station over the entire duration of the session (stop message)</td>
</tr>
<tr>
<td></td>
<td>• number of packets sent by the station since the beginning of the session (interim message)</td>
</tr>
</tbody>
</table>
Enabling Accounting to the Internal RADIUS Server on a WLAN

To activate accounting to the internal RADIUS server, follow these steps:

1. Select Network Setup > WLAN Setup > Configuration.

2. Select the WLAN from the list and click the Edit button. The Edit screen for the WLAN is displayed.

### Field Meanings

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct-Input-Octets</td>
<td>• number of bytes received by the station over the entire duration of the session (stop message)</td>
</tr>
<tr>
<td></td>
<td>• number of bytes received by the station since the beginning of the session (interim message)</td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td>• number of bytes sent by the station over the entire duration of the session (stop message)</td>
</tr>
<tr>
<td></td>
<td>• number of bytes sent by the station since the beginning of the session (interim message)</td>
</tr>
<tr>
<td>Acct-Terminate-Cause</td>
<td>the reason that the station's session ended (stop messages only)—for example, the user might log off (User-Request) or the session might time out due to inactivity</td>
</tr>
</tbody>
</table>
3. In the **Advanced** section, in the **Accounting Mode** field, use the drop-down menu to select *Radius*.

4. Click the **Radius Config** button. The **Radius Configuration** screen is displayed.
To enforce RADIUS accounting, the WLAN must use 802.1X authentication, Web-Auth, or MAC authentication for the Authentication mode.
5. Configure settings for the primary accounting server in the Primary
   column of the Accounting section.
   a. Specify the server’s IP address in the Accounting Server Address field.
      To use the Wireless Edge Services zl Module’s internal server for
      accounting, enter 127.0.0.1. You can use the internal RADIUS server
      for accounting both when the internal RADIUS server is the authen-
      tication server and when an external server is the authentication
      server.
   b. Leave the default port: 1813.
   c. You should not specify a key when you use the module’s internal
      server. If you have already specified a key, erase the Accounting Shared
      Secret field.

6. Optionally, configure settings for a secondary server by completing the
   fields in the Secondary column of the Accounting section.

7. From the Accounting Mode drop-down menu, choose when the Wireless
   Edge Services zl Module forwards a message to its internal server:
   • Start-Stop—when a station connects to this WLAN and when it dis-
     connects
   • Stop-Only—only when a station disconnects
   • Start-Interim-Stop—when a station connects to this WLAN, periodi-
     cally for as long as the connection persists, and when the station
     closes the connection

8. If you have selected Start-Interim-Stop for the Accounting Mode, enter a
   value in the Interval field.
   This setting determines how often, in seconds, the module sends periodic
   reports on user activities. (It applies only when you select Start-Interim-
   Stop.) The default value is 60 seconds, and the valid range is from 60 to
   3600 seconds (1 hour).

9. Click the OK button.

10. In the WLAN’s Edit screen, click the OK button.

11. Click the Save link at the top of the Web browser interface to save the
    changes to the startup-config.
Viewing the Internal RADIUS Server’s Accounting Logs

When you set up RADIUS accounting to the Wireless Edge Services zl Module’s internal server, the module stores messages about user activity as accounting logs. The directory for the logs is flash:/log/radius.

To view the log file in the Web browser interface, select **Network Setup > Local RADIUS Server** and click the **Accounting Logs** tab.

The panel at the left of the screen shows the directories in the main RADIUS accounting directory (flash:/log/radius). By default, RADIUS reports are logged to the radacct directory, which you can see in Figure 11-20. Double-click the directory name to view log files within the directory.
RADIUS Server
RADIUS Accounting

![Network Setup > Local RADIUS Server](image)

**Figure 11-21.Viewing RADIUS Accounting Log Files Within a Directory**

The screen displays the following information for each log file:
- **Filename**—accounting.log, for the default file
- **Type**—Log, for logged reports
- **Size**—the size of the file in bytes

A log file might include multiple RADIUS accounting messages. As the Wireless Edge Services zl Module’s internal RADIUS server receives the messages, it adds them to the log file.

The **Network Setup > Local RADIUS Server > Accounting Logs** screen shows log file names; it does not show information contained within a file. To actually view the logged messages, you must export the log file: select the file and click the **Transfer Files** button. You can transfer the file to an FTP or TFTP server and from that server to a billing or auditing server. You can also open the file in a text editor or word processor and view the logged messages.
The module only creates accounting logs for its own activities as RADIUS server if you specifically enable RADIUS accounting to the internal server on a WLAN. See “Enabling Accounting to the Internal RADIUS Server on a WLAN” on page 11-39.
Wireless Network Management

Contents

Overview .................................................. 12-3
Monitoring the Wireless Network .................. 12-4
   Wireless Stations .................................. 12-4
      Viewing Wireless Stations .................. 12-4
      Disconnecting a Wireless Station .......... 12-6
      Viewing Details about a Wireless Station 12-7
      Viewing All Stations in a Layer 3 Mobility Domain 12-10
Wireless Statistics for Stations ................. 12-12
   Viewing Detailed Wireless Statistics ........ 12-13
   Viewing a Graph of Wireless Station Statistics 12-15
Radio Statistics ..................................... 12-19
   Viewing Detailed Radio Statistics .......... 12-20
   Viewing a Graph of Radio Statistics ........ 12-21
WLAN Statistics .................................... 12-26
   Viewing Traffic Statistics for the WLAN ... 12-27
   Viewing Detailed WLAN Statistics .......... 12-28
   Viewing a Graph of WLAN Statistics ....... 12-30
Module Statistics .................................... 12-34
   Radio Port Adoption Statistics ............ 12-36
AP Detection .......................................... 12-39
   Configuring AP Detection .................... 12-40
   Creating Lists of Detected APs ............ 12-46
      Creating Rules That Define Allowed APs 12-47
   Monitoring Detected APs ................... 12-51
      Managing the Unapproved APs List ....... 12-51
      Managing the Approved APs List ......... 12-54
      Configuring the Module to Report Unapproved APs 12-55
Configuring Station Intrusion Detection ........................................ 12-58
Configuring Thresholds for Station Intrusion Detection ............... 12-59
Configuring the Module to Report Station Intrusion ................... 12-60
Viewing Blocked Stations ...................................................... 12-62
Logging and Alarms .............................................................. 12-63
Configuring Logging ............................................................. 12-64
   Enabling Logging .......................................................... 12-64
   Forwarding Logs to an External Server ................................ 12-65
   Viewing Events in the Local Log File ................................... 12-66
   Deleting and Transferring the Local Log File ......................... 12-69
Managing the Alarm Log ....................................................... 12-71
   Details .............................................................................. 12-73
   Delete .............................................................................. 12-73
   Acknowledge ................................................................. 12-74
   Export ............................................................................ 12-74
MAC Filters (Local MAC Authentication) ...................................... 12-75
   Configuring MAC Standard ACLs (Filters) ............................. 12-76
   Configuring WLAN Memberships ....................................... 12-78
   Exporting and Importing MAC Standard ACLs (Filters) .......... 12-82
      Exporting MAC Standard ACLs ........................................ 12-82
      Importing MAC Standard ACLs ...................................... 12-84
Network Self Healing ............................................................... 12-89
   Neighbor Recovery ......................................................... 12-89
      Enabling Neighbor Recovery ....................................... 12-90
      Specifying Neighbors Manually .................................... 12-92
      Configuring Radios to Automatically Detect Neighbors ...... 12-94
      Selecting the Self-Healing Action ................................. 12-95
      Configuring a Self Healing Offset ................................. 12-98
Interference Avoidance .......................................................... 12-100
In this chapter you will learn how to monitor and manage your wireless network. You will learn about monitoring:

- wireless stations that are associated to a Wireless Edge Services zl Module’s radio ports (RPs)
- access points (APs) detected by a module’s RPs
- logged events
- alarm logs

When viewing such information in the Web browser interface, you can take several common actions, such as:

- clicking a Details button to view more in-depth information
- clicking an Export button to save the information to your workstation

You will also learn how to configure the Wireless Edge Services zl Module to collect information when necessary. For example, RPs do not automatically detect other APs. You must enable this feature and configure the module to manage the information that it receives.

Finally, you will learn how to implement self healing in your wireless network, which maximizes network performance by allowing RP radios to respond to changing conditions.
Monitoring the Wireless Network

This section explains how you can access information about wireless stations and wireless network activity. It then provides some tips for interpreting this information.

You can monitor:
- wireless stations’ associations
- wireless statistics:
  - individual statistics for traffic to and from each wireless station
  - average statistics for all traffic to and from an RP radio
  - average statistics for all traffic in a wireless LAN (WLAN)
  - average statistics for all traffic to and from all RPs adopted by a module
- RPs

When troubleshooting, you can compare the various wireless statistics to determine, for example, whether congestion seems to be problem throughout a WLAN or is centered on a particular RP or group of RPs.

Wireless Stations

The Wireless Edge Services zl Module stores information about the associations that adopted RPs have established with wireless stations. You should view this information to monitor network activity and to detect intruders. You can also use this information to help a wireless user who is having difficulty with his or her connection.

Viewing Wireless Stations

To view the wireless stations, select Device Information > Wireless Stations, as shown in Figure 12-1.
Wireless Network Management
Monitoring the Wireless Network

Figure 12-1. Viewing Wireless Station Associations

The screen displays this information for each station associated with one of the WLANs on this module:

- **Station Index**—Stations are listed in the order in which they associated.
- **MAC Address**—Each station’s Media Access Control (MAC) address is listed.
- **IP Address**—A station must receive an IP address to receive complete network connectivity.
- **Ready**—A green check mark indicates that the station has completely authenticated and associated to a WLAN. A red X reveals that the station cannot yet send data, usually because it failed to authenticate.
- **Power Save**—A station that uses power save turns off the wireless connection except when actively sending or receiving data. The Wireless Edge Services zl Module tracks these stations and ensures that packets are correctly buffered for them. A green checkmark indicates that the station is currently in power save mode.
Although power save extends a station's battery life, it might result in jittery performance for real-time applications. If a user complains of low quality of service (QoS) and you see that the user's station implements power save, you could suggest that the user disable this feature.

- **WLAN**—The index number of the WLAN to which the station has connected is listed. (This column does not show the service set identifier [SSID]). The WLAN defines the broadcast group for the station and determines settings such as encryption and QoS.

- **VLAN**—The virtual LAN (VLAN), or subnetwork, in which the module will forward traffic from this station is listed. This important setting determines the type of network access that the station receives. If the module implements user-based VLANs for a WLAN, you should verify that the station has received the correct VLAN assignment.

- **Radio Index**—The radio to which the station connects is listed. If you see an unauthorized station, this information will point you toward the intruder's physical location.

- **Radio Type**—This setting indicates the 802.11 mode in which the station and the RP radio to which it connects operate.

You should be able to interpret the information on the **Device Information > Wireless Stations** screen to monitor and troubleshoot your wireless network.

For example, if the user of a wireless station listed in Figure 12-1 reports that he or she cannot connect to the network, the network administrator can quickly access the **Network Setup > Wireless Stations** screen while talking to the user. The administrator can immediately see that the user's station is not ready to send and receive traffic and has not received an IP address. The administrator can then begin to troubleshoot the problem, working with the user to ensure that login credentials were entered correctly and that the station's VLAN assignment is correct. The administrator can also troubleshoot the network's Dynamic Host Configuration Protocol (DHCP) setup.

You can also save information about one or more wireless stations to a comma-separated file on your workstation. Select the stations, and then click the **Export** button. (Use the **Ctrl** or **Shift** keys to select more than one station.)

**Disconnecting a Wireless Station**

If you access the **Device Information > Wireless Stations** screen and see a wireless station that should not connect to your network, you can immediately disassociate the station. Select the station and click the **Disconnect** button.

Because the station can immediately reassociate unless you take steps to prevent this, the prompt shown in Figure 12-2 is displayed.
Wireless Network Management
Monitoring the Wireless Network

Figure 12-2. Preventing a Station from Reconnecting to the Wireless Network

If you click the Yes button, the Filter dialog box is displayed. (See Figure 12-3.)

As the figure shows, the station’s MAC address is already listed in the Starting MAC and Ending MAC fields, allowing you to quickly create a MAC filter to prevent the station from reaccessing the wireless network.

You should also take steps to prevent the user from using another station (with a different MAC address) to access the wireless network. For example, you may need to change a preshared key that has been compromised or reset a user’s password.

Viewing Details about a Wireless Station

If you want to view more information about a particular station’s capabilities and connection, select that station on the Device Information > Wireless Stations screen, and then click the Details button. The Details screen is displayed. (See Figure 12-4.)
Figure 12-4. Viewing Detailed Information about a Station
In addition to the information that is listed on the **Device Information > Wireless Stations** screen (such as MAC address, IP address, Power Save, WLAN, and VLAN), you can view:

- **Authentication**—This field displays the authentication method used—802.1X Extensible Authentication Protocol (EAP), Web authentication (Web-Auth), MAC authentication, or none. None is displayed for Wi-Fi Protected Access (WPA)/WPA2-preshared keys (PSK) and Wired Equivalency Protocol (WEP).

- **Last Active**—You can view how many seconds it has been since the station last sent a frame. If the station is idle for longer than the WLAN’s inactivity timeout, the Wireless Edge Services zl Module will force the station to reassociate.

- **QoS Information**—Two fields are reported for QoS:
  - **UAPSD enabled for**—This field reports whether the Unscheduled Automatic Power Save Delivery (UAPSD) feature has been enabled. Designed for Voice over IP (VoIP) and Wi-Fi Multimedia (WMM), UAPSD preserves the mobile device’s battery life while allowing the device to control when it “sleeps” and “awakens.” At regular intervals (configured on and controlled by the mobile device), the mobile device queries the AP to determine whether the AP has any buffered frames. (With normal power save mode, the AP contacts the station—at intervals defined on and controlled by the AP—when the AP has buffered frames for the station.)
  - **Service Period**—When QoS is enabled for a WLAN, the AP grants a station a transmission opportunity, allowing the station to transmit a frame. If an AP grants a station two or more contiguous transmission opportunities, this is called the service period.

- **BSS Address**—This address is the basic SSID (BSSID) on the radio to which the station connects. Each RP radio has four BSSIDs, which carry traffic for different WLANs.

- **Voice**—This setting indicates whether this station sends voice frames. You can configure the Wireless Edge Services zl Module to grant higher QoS for voice traffic.

- **WMM**—This setting indicates whether the station supports Wi-Fi Multimedia (WMM). If it does, then the Web browser interface indicates the Access Category (AC) that the station is currently using to transmit traffic. The higher the AC, the better the QoS for the traffic. You can view the WMM settings associated with that AC on the station’s WLAN by selecting **Network Setup > WLAN Setup** and clicking the **WMM** tab.

- **Encryption**—This field displays the encryption method—WEP, WPA/WPA2 with Temporal Key Identity Protocol (TKIP), WPA2 with Advanced Encryption Standard (AES), or WPA/WPA2 with both TKIP and AES.
Wireless Network Management
Monitoring the Wireless Network

- **Roam Count (No de-authentication)**—The module tracks the number of times that the station has de-authenticated, which indicates the number of times that the station has roamed away from the module (not between RPs on the same module).

- **IDM Attributes**—If you are using ProCurve Identity Driven Manager (IDM), this section lists IDM settings received for the user accessing the network through this station. Possible settings include a dynamic VLAN (which is also called the user-based VLAN), access control lists (ACLs), priority (which is the 802.1p value assigned to the user’s traffic), and ingress bandwidth (which is displayed if rate limiting has been configured for the user).

Viewing All Stations in a Layer 3 Mobility Domain

When your Wireless Edge Services zl Module is in a Layer 3 mobility domain, it tracks all stations associated with any module in the domain. This information prepares the module for implementing Layer 3 roaming should one of these stations roam to it. In addition, the module must maintain information about stations that have roamed away from it, but for which it still acts as home module.

To view information about every station associated with any Wireless Edge Services zl Module in the Layer 3 mobility domain, follow these steps:

1. Select **Device Information > Wireless Stations**.
2. Click the **Layer 3 Mobility-Station Status** tab.
The screen displays the following information for all Layer 3 mobility domain stations:

- **Station MAC**—station MAC address
- **Station IP**—station IP address
- **Home Module IP**—the IP address of the module responsible for forwarding the station’s traffic into the wired network
- **Home Module VLAN**—the static VLAN ID for the WLAN on the home module (HM)
- **Curr Module IP**—the IP address of the module to which the station is currently associated
- **Roam**—This column tracks Layer 3 roams. The station is considered to be in a roaming state (green check mark) if its current module (CM) differs from its HM.
Wireless Statistics for Stations

Like the Device Information > Wireless Stations screen, the Device Information > Wireless Statistics screen lists every station associated with RPs adopted by the Wireless Edge Services zl Module. However, this screen focuses on activity on the connection.

![Device Information > Wireless Statistics](image)

The first two columns, Radio Index and MAC Address, identify the station according to the RP radio to which the station connects and the station’s MAC address. The WLAN column indicates the station’s WLAN.

The next columns display traffic statistics for the connection:

- **Throughput Mbps**—the total throughput for data in Mbps
- **Bit Speed (Avg.) Mbps**—the average bit speed in Mbps when the station actually transmits or receives traffic
- **% Non Unicast**—the percentage of multicast and broadcast packets (as compared to total packets)
- **Retries**—the number of times that a station must retransmit a packet, whether due to a collision or another error

Select Last 30s or Last Hr to view the average statistics over either the last 30 seconds or the last hour.
A high number of retries can indicate interference or excessive congestion.

Wireless phones, which send traffic to a multicast address, may have a high percentage of nonunicast traffic. For traditional stations, a high percentage of nonunicast traffic can be normal for brief periods—for example, when the station first associates and requests a DHCP address. You may be able to decrease the number of frames that stations broadcast by enabling proxy ARP. (See Chapter 4: “Wireless Local Area Networks (WLANs).”)

Viewing Detailed Wireless Statistics

For more detailed information about the connection to a particular station, select that station and click the Details button. The Details screen is displayed. (See Figure 12-7.)

![Figure 12-7. Viewing Detailed Statistics about a Wireless Station](image)
The **Station Properties** section displays the same information that is listed on the **Device Information > Wireless Stations** screen, including the station’s MAC and IP address. However, you can also see whether the station supports QoS capabilities such as Voice and WMM.

You can use the **Traffic** section to monitor the quality and performance of the connection. The Web browser interface reports speed in terms of packets per second, total throughput in Mbps, and average speed in Mbps. The Web browser interface further breaks down statistics into received and transmitted traffic.

Note that these statistics do not include retry overhead, which means that in a network with significant congestion or interference, a user might perceive the connection to be slower than these statistics would seem to indicate. The sections below can help you monitor that aspect of the wireless connection.

The **RF Status** section displays the status of the radio medium:
- **Avg Station Signal (dBm)**—average signal level detected for this station
- **Avg Station Noise (dBm)**—average background noise for this station
- **Avg Station SNR (dBm)**—average SNR for this station

In the **Errors** section, the Web browser interface reports the total number of error packets:
- **Avg Number of Retries**—average number of retries necessary to successfully transmit a packet to this station
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.
- **% Gave Up Pkts**—number of packets that the Wireless Edge Services zl Module never successfully transmitted to this station
- **% of Undecipherable Pkts**—percentage of packets received from this station that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The statistics in black apply to the last 30 seconds, giving you a snapshot of current performance. The statistics in blue show the station’s average performance over the last hour.
Viewing a Graph of Wireless Station Statistics

The Wireless Edge Services zl Module can create a graph of statistics for a wireless station. This graph displays how the statistics change over time.

To view this graph, follow these steps:
1. Select **Device Information > Wireless Statistics**.
2. Select the station (identified by MAC address) from the list.

3. Click the **Graph** button. The **Station Statistics** screen is displayed.
The **Station Statistics** screen displays the station’s MAC address and IP address in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per sec.) You can choose any of the statistics displayed in the **Details** screen (refer to “Viewing Details about a Wireless Station” on page 12-7 for more information on a statistic):

- **Pkts per sec**—total packets transmitted and received by this station per second
  - **TX Pkts per sec**—packets transmitted by this station per second
  - **RX Pkts per sec**—packets received by this station per second

---

**Figure 12-9. Station Statistics Graph**

![Station Statistics Graph](image)
Throughput (Mbps)—the actual throughput for data transmitted and received by this station
  • TX Tput (Mbps)—actual throughput for data transmitted by this station
  • RX Tput (Mbps)—actual throughput for data received by this station
Avg Bits per sec—average bit speed for all traffic sent and received by this station
NUcast Pkts—percentage of multicast and broadcast packets (as compared to total packets)
Avg Retries—average number of times the station must retransmit a packet, whether due to a collision or another error
Avg Signal (dBm)—average signal level detected from this station
Avg Noise (dBm)—average background noise in the wireless cell
Avg SNR (dBm)—average SNR for the connection to the station
Dropped Pkts—number of packets that the Wireless Edge Services zl Module never successfully transmitted to this station (also called gave up packets)
Undecr Pkts—number of packets from this station encrypted with the wrong key

Check the appropriate box for the statistic you want to view.
The x-axis of the graph displays the time—in Figure 12-10 the time is labelled in 10 second intervals. The y-axis adds a label that matches the box that you chose. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time. For example, the graph in Figure 12-10 shows this station’s total throughput, which experienced a spike just before 15:00.

You can select more than one box and compare statistics against each other. For example, Figure 12-10 compares total throughput to the average bit speed. As you can see, the station’s bit speed averages about 50 Mbps—near the 54 Mbps theoretical data rate. However, the station’s throughput is actually much lower. The lines are distinguished by color, as indicated in the legend below the x-axis.

You can select a maximum of four boxes at once.
When you have finished viewing the graph, click the Close button.

Radio Statistics

The Wireless Edge Services zl Module stores information about the wireless network activity on each RP radio. To view these statistics, select Network Setup > Radio and click the Statistics tab.

![Figure 12-11. Network Setup > Radio > Statistics Screen](image)

Every radio adopted by the module is listed, identified by:

- **Index**
- **Description**
- **Type** (802.11a or 802.11bg)

In addition to providing this information, the Network Setup > Radio > Statistics screens lists the number of stations that are connected to each RP. The following columns display average traffic statistics for connections to these stations, including:

- **Throughput Mbps**
- **Average Mbps**
- **RF Util**
Wireless Network Management
Monitoring the Wireless Network

■ % Non-UNI
■ Retries

These statistics are similar to those described for individual stations in "Wireless Statistics for Stations" on page 12-12. The RFUtil percentage compares the radio's actual utilization to its potential utilization by dividing the throughput by the average Mbps.

Again, you can select either Last 30s or Last Hr to view either the most current statistics or statistics over a more extended period.

Viewing Detailed Radio Statistics

To view more detailed statistics for a specific radio, select that radio and click the Details button. The Details screen is displayed. (See Figure 12-12.)

![Network Setup > Radio > Details](image)

Figure 12-12. Radio Statistics Details
The **Information** section describes this radio and shows the number of stations currently associated to it. You should check the **Current Channel** listing; if the radio is configured with a manual channel but currently uses a different channel, the channel number is listed in red.

On the **Details** screen, statistics for wireless traffic are broken down into received and transmitted traffic.

You can view the average status of the wireless medium or all stations connected to this radio under **RF Status**:

- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the radio
- **Avg Station Noise (dBm)**—average background noise in the wireless cell
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the radio

View the **Errors** section to monitor for congestion. Statistics include:

- **Avg Number of Retries**—average number of retries the radio must make to successfully transmit a packet
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.
- **% Gave Up Pkts**—number of packets that the Wireless Edge Services zl Module never successfully transmitted to a station associated to this radio
- **% of Undecipherable Pkts**—percentage of packets received by this radio that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The **Details** screen also allows you to simultaneously compare statistics for the last 30 seconds and the last hour.

**Viewing a Graph of Radio Statistics**

The Wireless Edge Services zl Module can create a graph of statistics for a radio, which displays how the statistics change over time.

To view this graph, follow these steps:

1. Select **Network Setup > Radio**.
2. Select the **Statistics** tab.
3. Select the radio.
4. Click the **Graph** button.

The **RP Statistics** screen is displayed.
The **RP Statistics** screen displays the radio’s name and MAC address in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per second.) You can choose any of the statistics displayed in the **Details** screen for radio statistics. The statistics apply to all stations associated to the radio. Refer to “Viewing Detailed Radio Statistics” on page 12-20 for more information on a statistic.

You can choose:
- **Pkts per sec**—total packets transmitted and received by this radio per second
  - **TX Pkts per sec**—packets transmitted by this radio per second
  - **RX Pkts per sec**—packets received by this radio per second
Wireless Network Management
Monitoring the Wireless Network

- **Throughput (Mbps)**—total throughput for data transmitted and received by this radio
  - **TX Tput (Mbps)**—throughput for data transmitted by this radio
  - **RX Tput (Mbps)**—throughput for data received by this radio
- **Avg Bits per sec**—average bit speed for traffic when the radio actually transmits or receives it
- **NUcast Pkts**—percentage of multicast and broadcast packets sent and received by the radio (as compared to total packets)
- **Avg Retries**—average number of times that all stations must retransmit a packet, whether due to a collision or another error
- **Avg Signal (dBm)**—average signal level detected for all stations associated to the radio
- **Avg Noise (dBm)**—average background noise in the wireless cell
- **Avg SNR (dBm)**—average SNR for all stations associated to the radio
- **Dropped Pkts**—number of packets that the Wireless Edge Services zl Module never successfully transmitted to a station associated to this radio (also called gave up packets)
- **Undecr Pkts**—number of packets from this station encrypted with the wrong key
- **MUs associated**—number of stations associated to this radio

Check the appropriate box for the statistic you want to view.
Wireless Network Management
Monitoring the Wireless Network

Figure 12-15. Comparing RP Statistics

The x-axis of the graph displays the time—in Figure 12-15, marked at 5 second intervals. The y-axis adds a label that matches your choice. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time. You can select more than one box and compare statistics against each other. For example, Figure 12-10 compares average retries and average SNR. The lines are distinguished by color, as indicated in the legend below the x-axis.

You can select a maximum of four boxes at once.

When you have finished viewing the graph, click the Close button.
Wireless Network Management
Monitoring the Wireless Network

WLAN Statistics

To monitor wireless activity on a WLAN-wide scale, select **Network Setup > WLAN Setup** and click the **Statistics** tab.

![Network Setup > WLAN Setup > Statistics Screen](image)

This screen lists every WLAN that is enabled on the module. WLANs are identified by:
- **Index** (the WLAN's number)
- **SSID**
- **Description**
- **VLAN**

The **Stations** column shows the number of stations currently connected to that WLAN.
Monitoring the Wireless Network

The remaining columns display statistics similar to those described in “Wireless Statistics for Stations” on page 12-12; however, these statistics are averages for all stations in the WLAN:

- **Throughput Mbps**—the total throughput for all data transmitted in the WLAN in Mbps
- **Bit Speed (Avg.) Mbps**—the average bit speed for all data transmitted in the WLAN in Mbps
- **% Non Unicast**—the percentage of multicast and broadcast packets (as compared to total packets)
- **Retries**—the number of times that all stations in the WLAN must retransmit a packet, whether due to a collision or another error

Viewing Traffic Statistics for the WLAN

The **Network Setup > WLAN Setup > Statistics** screen includes a **Module Statistics** button.

<table>
<thead>
<tr>
<th>Network Setup &gt; WLAN Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
</tr>
<tr>
<td><strong>Index</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

**Figure 12-17. Module Statistics Button in the Network Setup > WLAN Setup > Statistics Screen**
Select a WLAN and click this button to view:

- the percentage of packets in this WLAN transmitted at each data rate
- the percentage of packets in this WLAN that required a certain number of retries (for 0 to 15)

![Module Statistics Screen](image)

**Figure 12-18. Module Statistics Screen**

Click the **Refresh** button to update the statistics. When you have finished viewing the screen, click the **Close** button.

**Viewing Detailed WLAN Statistics**

To view more detailed statistics for a specific WLAN, select the WLAN and then click the **Details** button in the **Network Setup > WLAN Setup > Statistics** screen.
The *Information* section shows settings for this WLAN including:

- **SSID**
- **VLAN**
- **security settings**
  - authentication type
  - encryption type

The *Information* section also displays the number of stations associated to the WLAN and of radios mapped to the WLAN. (If the Wireless Edge Services zl Module is using normal mode configuration, all adopted radios are mapped to the WLAN.)

The *Traffic* section displays the same information that is listed on the *Network Setup > WLAN Setup > Statistics* screen. You can use the *Traffic* section to monitor the quality and performance of the WLAN. The Web browser interface
Wireless Network Management
Monitoring the Wireless Network

reports speed in terms of packets per second, total throughput in Mbps, and average speed in Mbps. The Web browser interface further breaks down statistics into received and transmitted traffic.

The RF Status section displays statistics dealing with the status of the radio medium. The statistics apply to all radios mapped to the WLAN:

- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the WLAN
- **Avg Station Noise (dBm)**—average background noise for all stations associated to the WLAN
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the WLAN

In the Errors section, the Web browser interface reports the total number of error packets in the entire WLAN:

- **Avg Number of Retries**—average number of attempts radios must make to successfully transmit a packet to stations in this WLAN
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.

- **% Gave Up Pkts**—number of packets that the Wireless Edge Services zl Module never successfully transmitted to a station associated to this WLAN

- **% of Undecipherable Pkts**—percentage of packets in this WLAN that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The statistics in black apply to the last 30 seconds, giving you a snapshot of current performance. The statistics in blue show activity in the WLAN over the last hour.

Viewing a Graph of WLAN Statistics

The Wireless Edge Services zl Module can create a graph of statistics for a WLAN, which displays how the statistics change over time.

To view this graph, follow these steps:

1. Select **Network Setup > WLAN**.
2. Select the **Statistics** tab.
3. Select the WLAN.
4. Click the **Graph** button.

The **WLAN Statistics** screen is displayed.
The **WLAN Statistics** screen displays the WLAN’s SSID and static VLAN ID in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per second.) You can choose any of the statistics displayed in the **Details** screen for WLAN statistics. (Refer to “Viewing Detailed WLAN Statistics” on page 12-28 for more information on a statistic.) The statistics apply to all radios and stations associated to the WLAN.

You can choose:

- **Pkts per sec**—total packets transmitted and received in this WLAN per second
- **TX Pkts per sec**—packets transmitted in the WLAN per second
- **RX Pkts per sec**—packets received in this WLAN per second

---

**Figure 12-21.WLAN Statistics Graph**

The **WLAN Statistics** screen displays the WLAN’s SSID and static VLAN ID in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per second.) You can choose any of the statistics displayed in the **Details** screen for WLAN statistics. (Refer to “Viewing Detailed WLAN Statistics” on page 12-28 for more information on a statistic.) The statistics apply to all radios and stations associated to the WLAN.

You can choose:

- **Pkts per sec**—total packets transmitted and received in this WLAN per second
- **TX Pkts per sec**—packets transmitted in the WLAN per second
- **RX Pkts per sec**—packets received in this WLAN per second
Wireless Network Management
Monitoring the Wireless Network

- **Throughput (Mbps)**—total throughput for data transmitted and received in this WLAN
  - **TX Tput (Mbps)**—throughput for data transmitted in this WLAN
  - **RX Tput (Mbps)**—throughput for data received in this WLAN
- **Avg Bits per sec**—average bit speed for all traffic transmitted and received in the WLAN
- **NUcast Pkts**—percentage of multicast and broadcast packets sent and received in the WLAN (as compared to total packets)
- **Avg Retries**—average number of times that all stations and radios in the WLAN must retransmit a packet, whether due to a collision or another error
- **Avg Signal (dBm)**—average signal level detected for all stations in the WLAN
- **Avg Noise (dBm)**—average background noise in all wireless cells in the WLAN
- **Avg SNR (dBm)**—average SNR for all stations in the WLAN
- **Dropped Pkts**—number of packets from this station dropped by the Wireless Edge Services zl Module
- **Undecr Pkts**—number of packets from this station encrypted with the wrong key
- **# Radios**—number of radios mapped to this WLAN

Check the appropriate box for the statistic you want to view.
Wireless Network Management
Monitoring the Wireless Network

Figure 12-22.Comparing WLAN Statistics

The x-axis of the graph displays the time—in Figure 12-22, marked at 5 second intervals. The y-axis adds a label that matches your choice. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time.

You can select up to four boxes at once and compare statistics against each other. When you have finished viewing the graph, click the Close button.

Module Statistics

You can also monitor all wireless traffic to and from stations associated with this Wireless Edge Services zl Module. Select Network Setup and click the Module Statistics tab.
Monitoring the Wireless Network

The top of the screen displays:
- the number of stations currently associated with RPs on this module
- the number of RPs adopted by this module
- the number of RP radios adopted by this module

The Traffic section contains statistics similar to those discussed in “Wireless Statistics for Stations” on page 12-12:
- Pkts per second
- Throughput in Mbps
- Avg. Bit Speed in Mbps
- % Non-unicast pkts

These statistics apply to all wireless traffic associated with this module and are divided into statistics for the last 30 seconds (in black) and the last hour (in blue). The Traffic section also divides statistics into traffic received and traffic transmitted.
You can use the **RF Status** section to monitor the quality of radio media on a network-wide level, and you can use the **Errors** section to look for problems with congestion or interference. You can then examine these statistics for radios or for WLANs to pinpoint the source of a problem.

The **RF Status** includes these statistics:

- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the Wireless Edge Services zl Module
- **Avg Station Noise (dBm)**—average background noise for all stations associated to the module
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the module

In the **Errors** section, the Web browser interface reports the total number of error packets for this Wireless Edge Services zl Module:

- **Avg Number of Retries**—average number of attempts to transmit a packet to a station
- **% Gave Up Pkts**—number of packets that the Wireless Edge Services zl Module never successfully transmitted to a station
- **% of Undecipherable Pkts**—percentage of packets received that could not be deciphered

A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

**Radio Port Adoption Statistics**

To view information about all RPs detected by this Wireless Edge Services zl Module, select **Device Information > Radio Adoption Statistics**.
Select the **Adopted RP** tab to view the RPs that the module has actually adopted, and the **Unadopted RP** tab to view other detected RPs.

The number of RPs adopted by this module is listed at the bottom of the **Device Information > Radio Adoption Statistics > Adopted RP** screen.

For each adopted RP, the screen lists:

- **Base Radio MAC**—This is the MAC address on the RP's Ethernet interface.
- **Model**—The Wireless Edge Services zl Module adopts only ProCurve Radio Ports 210, 220, or 230.
- **Serial**—The serial number is unique to this device.
- **HW Version**—This column indicates the hardware used by the RP.
- **IP Address**—This column displays an IP address if you have configured Layer 3 adoption for RPs. For more information about Layer 3 adoption, see Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”
- **Bootloader**—This column indicates the software from which the RP boots.
- **Protocol Version**—RPs and the Wireless Edge Services zl Module communicate with a particular protocol. If an RP experiences problems, you should verify that the two devices’ protocol versions match. Also check the hardware version and the bootloader version.
Wireless Network Management
Monitoring the Wireless Network

- **SW Version**—You should verify that the software version with which the RP loads is up-to-date.
- **Radio Indices**—The RP includes one or two radios. These radios are listed on the Network Setup > Radio > Configuration screen according to the indices displayed in this column. You can configure settings for these radios on that screen. (See Chapter 3: “Radio Port Configuration.”)

If you have configured manual radio adoption, the module may detect RPs that it is not authorized to adopt. These RPs are listed on the Device Information > Radio Port Adoption Statistics > Unadopted RP screen. (See Figure 12-25.)

![Device Information > Radio Adoption Statistics > Unadopted RP Screen](image)

You should review this screen to determine whether you need to manually add an unadopted RP (see Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module”) or find and remove an unauthorized RP. The screen lists this information:

- **Index**—RPs are listed in the order in which they are detected.
- **MAC Address**—This is the MAC address on the RP’s Ethernet interface.
- **Last Seen (In Seconds)**—View this setting to determine how recent the information about this RP is.
AP Detection

People may introduce unauthorized APs into your network for several reasons.

Sometimes attackers set up rogue APs in your environment, hoping to lure wireless users to authenticate to them instead of to your network’s RPs. In this way, attackers can collect sensitive information, including passwords with which they can then access your private network and view, steal, or damage data.

More commonly, users introduce APs for their own convenience, not meaning any particular harm. However, because users often take inadequate measures to secure these APs, the unauthorized APs open vulnerabilities for hackers to exploit.

The ProCurve RPs 210, 220, and 230 can listen for such unauthorized APs, collecting information about them to be sent to the Wireless Edge Services zl Module.

The module helps you to manage this information. You can even configure the module to automatically send an alarm when an unauthorized AP is detected.

**Note**

AP detection tracks devices that are not connected, either directly or indirectly, to the Wireless Edge Services zl Module. It does not prevent unauthorized RPs from being adopted. To control RPs that connect to your network, you must configure the module’s adoption settings as described in Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”

You can enable and manage AP detection from the **Special Features > Access Point Detection** screen, which is shown in Figure 12-26.
Configuring AP Detection

By default, AP detection is disabled. To configure AP detection, you must complete two main steps: you must enable AP detection, and you must configure at least one radio to scan for APs.

When you configure a radio to scan for APs, you can select one of these options:

- **Single-channel scan for Unapproved APs**—If you select this option, the radio listens for beacons from other APs operating on its own channel. When a radio hears such a beacon, it forwards information in the beacon to the Wireless Edge Services Module. The radio can send and receive traffic from associated wireless stations at the same time it listens for beacons from APs.

- **Dedicate this Radio as a Detector**—If you select this option, the radio constantly scans for neighboring APs. Such a radio is called a detector, and it cannot connect to wireless stations. A detector uses auto channel select (ACS) to change to and scan all channels that are:
  - in its frequency (either 802.11a’s 5 GHz or 802.11bg’s 2.4 GHz)
  - allowed by its country’s regulations

Table 12-1 and Figure 12-27 compare single-channel detectors and dedicated detectors.
Table 12-1. Comparing Single-Channel Detectors and Dedicated Detectors

<table>
<thead>
<tr>
<th>Single-Channel Detector</th>
<th>Dedicated Detector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio passively listens for beacons</td>
<td>Radio actively sends probe requests</td>
</tr>
<tr>
<td>Radio listens on its own channel only</td>
<td>Radio sends probes on all channels in its frequency that are allowed by its country’s regulations</td>
</tr>
<tr>
<td>Radio supports wireless stations</td>
<td>Radio does not support wireless stations</td>
</tr>
</tbody>
</table>

Figure 12-27. AP Detection on Single-Channel Detectors and Dedicated Detectors
You can configure a radio as a single-channel detector or a dedicated detector in one of two ways:

- as part of an override configuration for a particular radio

  For example, your organization might install an RP that is entirely dedicated to searching out rogue APs.

  Another reason to dedicate a radio as a detector is so it can monitor all nearby RPs in your wireless network and take action if an RP experiences problems. See “Network Self Healing” on page 12-89 for more information on how detectors participate in neighbor recovery.

- as part of the radio adoption default configuration for all radios of a certain type

  If your network does not include any stations that use, for example, 802.11a mode, then you could dedicate all 802.11a radios to scanning for rogue APs. (Note, however, that these radios will only detect APs operating on an 802.11a channel.)

---

**Note**

You can enable the detector option in both radio adoption default configurations as a security measure. In this case, all RP radios are adopted as detectors. Thus, a radio cannot forward wireless traffic into your network until you determine that it is authorized to do so and explicitly disable the detector option on it.

---

To configure AP detection, complete the following steps:

1. Enable AP detection.
   a. Select **Special Features > Access Point Detection > Configuration**.
Figure 12-28. Enabling AP Detection and Configuring Settings

b. Check the Enable box.

c. Customize the timeout setting for approved and unapproved APs. (For more information about approved and unapproved APs, see “Creating Lists of Detected APs” on page 12-46.)
   – Approved AP timeout—specifies how long the module retains information about APs that you have defined as allowed.
   – Unapproved AP timeout—specifies how long the module retains information about APs that are not allowed.

   Enter a time from 1 through 65,535 seconds (approximately 18 hours), or accept the default setting of 300 seconds (five minutes).

d. Click the Apply button.

2. Configure a particular radio or radios to scan for APs.
   a. Select Network Setup > Radio > Configuration.
   b. Select the radio or radios.
   c. Click the Edit button. The Configuration screen for the radio is displayed. (See Figure 12-29.)
d. On the radio’s **Configuration** screen, check the option that you want for AP detection:
   - **Dedicate this Radio as a Detector**
   - **Single-channel scan for Unapproved APs**

e. Click the **OK** button.
The radio state should now be listed as **Detector** on the **Network Setup > Radio > Configuration** screen, as shown in Figure 12-30.

**Note**

The Wireless Edge Services zl Module stores the configuration for a particular radio with its MAC address so that this configuration persists even if the radio powers down.

For more information on radio configurations, see Chapter 3: “Radio Port Configuration.”

3. Configure all radios of a particular type to scan for APs.
   a. Select **Network Setup > Radio Adoption Defaults > Configuration**.
Wireless Network Management
AP Detection

b. Select the radio type (802.11a, 802.11b, or 802.11bg).

c. Click the Edit button.

d. On the radio type’s Configuration screen, check the option that you want for AP detection:
   - Dedicate this Radio as a Detector
   - Single-channel scan for Unapproved APs

e. Click the OK button.

4. Click the Save link at the top of the screen to save your changes to the startup-config.

Creating Lists of Detected APs

AP detection simply enables adopted RPs to report the APs that they detect. The Wireless Edge Services zl Module then sorts the detected APs into approved and unapproved lists.

By default, the module considers all APs to be unallowed, which means that they are displayed on the unapproved list.
You should configure the module to allow APs that meet certain criteria—for example, that are part of your wireless network. The module then moves these APs to an approved APs list so that they do not clutter the unapproved list and make it difficult for you to identify actual threats to network security.

You can use two criteria to define allowed APs:
- MAC address
- SSID

For example, you can list the MAC address of every AP and RP in your network (not connected to this module) and allow those addresses. Or, you can simply allow all APs and RPs that are members of one of your network's WLANs (as defined by the SSID). These solutions are appropriate only in a relatively secure environment.

For tighter security, you can force the module to match APs to both a MAC address and an SSID. For example, a rogue AP might mimic your network's SSID; if you allow all APs using that SSID, then you will overlook this security hazard.

You specify these criteria in a series of up to 200 rules, each identified by an index number. Each rule can specify one of the following:
- one MAC address
- one SSID
- one MAC address and one SSID

For example, if you want to use hardware-based rules to allow APs and your network includes 14 RPs adopted by a different module and two APs, then you must create 16 rules.

Creating Rules That Define Allowed APs

To create a rule, complete these steps:

1. Select Special Features > Access Point Detection > Configuration. The screen displays, in the Allowed APs section, the APs that are currently allowed, listed in order of index number.

   This section shows the rules for allowed APs. Your RPs may or may not detect the APs in question at the moment.
2. Click the Add button.

3. In the Index field, enter a value from 1 through 200. Each rule must have a unique index.

   By default, the field displays the next available index number.

4. Create one of the three types of rules:
   a. Allow an AP with a particular MAC address no matter what WLAN it supports, as shown in Figure 12-33:
      i. Select the second field under Radio MAC Address and then enter the address.
      ii. Under SSID, keep the selection at Any SSID.
b. Allow any AP that is a member of a particular WLAN, as shown in Figure 12-34:
   i. Select the second field under **SSID** and then enter the WLAN’s **SSID**.
   ii. Leave the **Radio MAC Address** selection at **Any MAC Address**.
c. Allow a particular AP only if it is a member of the correct WLAN, as shown in Figure 12-35:
   i. Select the **Radio MAC Address** field and then enter the address.
   ii. Select the **SSID** field and then enter the WLAN's SSID.
5. Click the **OK** button.

The AP is now listed in the **Allowed APs** section of the **Special Features > Access Point Detection > Configuration** screen.

### Monitoring Detected APs

You should periodically check the unapproved APs list for rogue APs. You may also want to configure the Wireless Edge Services zl Module to automatically generate and send an alarm whenever a radio detects an unapproved AP.

### Managing the Unapproved APs List

Select **Special Features > Access Point Detection** and click the **Unapproved APs** tab to view a list of detected APs not expected in your environment. (In other words, this list displays any APs that the rules do not allow.)
Wireless Network Management
AP Detection

Special Features > Access Point Detection

Figure 12-36.Viewing the Unapproved APs List

You can also view this list by selecting Device Information > Access Point Detection and clicking the Unapproved APs tab. However, you can only view information about APs on the other screen; you cannot allow the APs as described below.

As shown in Figure 12-36, the list includes the following information for each AP:

- **BSS MAC Address**—This address is the AP's BSSID. RPs report each BSSID that is a source of a beacon as a detected AP. Because an AP might send beacons using several different BSSIDs, RPs might report the same physical AP several times.
- **Reporting Radio**—This is the index for the adopted radio that detected this AP. This information can help you pinpoint a rogue AP's location.
- **Channel**—This is the channel on which the detected AP operates.
- **Signal Strength (In dBm)**—This field lists the detected AP's signal strength, expressed in dBm. This information can help you determine how close the AP is to the reporting radio.

<table>
<thead>
<tr>
<th>BSSID MAC Address</th>
<th>Reporting Radio</th>
<th>Channel</th>
<th>Signal Strength (In dBm)</th>
<th>Last Seen (In Seconds)</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:12:83:02:65:40</td>
<td>2</td>
<td>1</td>
<td>-79</td>
<td></td>
<td>05/05-00</td>
</tr>
<tr>
<td>00:12:83:02:65:41</td>
<td>4</td>
<td>1</td>
<td>-10</td>
<td></td>
<td>05/05-00</td>
</tr>
<tr>
<td>00:12:83:02:65:42</td>
<td>4</td>
<td>1</td>
<td>-5</td>
<td></td>
<td>05/05-00</td>
</tr>
<tr>
<td>00:12:83:02:65:43</td>
<td>4</td>
<td>1</td>
<td>-19</td>
<td></td>
<td>05/05-00</td>
</tr>
<tr>
<td>00:12:83:02:65:44</td>
<td>2</td>
<td>1</td>
<td>-90</td>
<td></td>
<td>ONE TEAM</td>
</tr>
<tr>
<td>00:12:83:02:65:45</td>
<td>2</td>
<td>1</td>
<td>-90</td>
<td></td>
<td>ONE TEAM</td>
</tr>
<tr>
<td>00:12:83:02:65:46</td>
<td>4</td>
<td>1</td>
<td>-16</td>
<td></td>
<td>ONE TEAM</td>
</tr>
</tbody>
</table>

Number of Unapproved APs: 35
■ **Last Seen (In Seconds)**—This column indicates how recent the information is.

■ **SSID**—If a radio has an unapproved MAC address but one of your WLAN’s SSIDs, this may signal a hacker phishing for passwords and other sensitive data.

If this list becomes too long and unmanageable, you should take one or more of these steps:

■ Lower the timeout value for unapproved APs. (See “Configuring AP Detection” on page 12-40.)

■ Move legitimate APs to the approved APs list.

**Allowing an Unapproved AP.** Not all APs in the unapproved list are necessarily rogue APs. Some may be APs adopted by another module or APs that belong to your organization; others may belong to legitimate neighboring organizations.

To move an AP to the approved list, complete these steps:

1. Select the AP and click the **Allow** button.

   As shown in Figure 12-37, the Web browser interface automatically fills in the AP’s MAC address and SSID. It also fills in the next available index number.

![Figure 12-37. Add Allowed AP Screen](image-url)
2. If you so desire, you can change these settings. (For example, you could allow the MAC address, but any SSID.)

3. Click the **OK** button.

In a way, allowing an AP is like acknowledging an alarm. You are letting other administrators know that you have checked the potential threat. This feature is particularly useful for allowing APs that do not belong to your network—so you cannot create a rule to allow them in advance—but that you have verified as legitimate APs in a nearby organization.

**Managing the Approved APs List**

You should also periodically check the approved APs list to make sure that no rogue APs have been added.

You can view this list in two ways:

- Select **Special Features > Access Point Detection** and click the **Approved APs** tab.
- Select **Device Information > Access Point Detection > Approved APs**.

The approved APs list includes all detected APs that match the criteria for one of the rules on the **Allowed APs** screen. For each AP, the list displays information similar to that in the unapproved list, as shown in Figure 12-38.

---

**Special Features > Access Point Detection**

<table>
<thead>
<tr>
<th>AP ID</th>
<th>Reporting Radio</th>
<th>Channel</th>
<th>Last Seen (in Seconds)</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2C-10-08-AP-86</td>
<td>2</td>
<td>1</td>
<td>196</td>
<td></td>
</tr>
<tr>
<td>2C-10-08-AP-86</td>
<td>4</td>
<td>1</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 12-38.** Managing the Approved APs List
If a rogue AP is on this list, you should reconfigure the rule that allowed it. For example, to screen APs you may need to use MAC addresses instead of, or in addition to, SSIDs.

Configuring the Module to Report Unapproved APs

You can configure the Wireless Edge Services zl Module to trigger a Simple Network Management Protocol (SNMP) trap whenever a radio detects an unapproved AP.

Complete these steps:
1. Select Management > SNMP Trap Configuration > Configuration.

2. Expand the Wireless heading and then the RP Detection heading.
3. Click the Enable all sub-items button.
4. Make sure that the Allow Traps to be generated box is checked.
5. Click the **Apply** button.

If an RP detects an external AP, a log is displayed on the **Device Information > Alarm Log** screen, as shown in Figure 12-41.
The module will log the alarm, as well as forward it to a trap receiver (if one has been specified). (For instructions on configuring the trap receiver, see “SNMP Traps” on page 2-112 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)
Configuring Station Intrusion Detection

AP detection protects your network against unauthorized APs. The Wireless Edge Services zl Module can also guard against hackers who use stations to launch attacks. Using station intrusion detection, the module monitors stations for suspicious behavior that might indicate an attack such as the following:

- **Reconnaissance attack**—An attacker sends probes to discover APs and the stations that are associating with those APs. Using the information discovered, the attacker can launch additional attacks.

- **Association flood attack**—An attacker spoofs multiple clients, sending so many association requests that the AP cannot handle them all. The AP begins to deny additional associations.

- **Disassociation flood attack**—After launching a reconnaissance attack, the attacker identifies the stations attached to a particular AP. The attacker then masquerades as the AP and sends disassociation frames to the stations. Although the stations quickly re-associate with the AP, the attacker continues to send disassociation frames to end the stations’ sessions.

- **Authentication failure attack**—The attacker uses a tool to masquerade as an AP. When a station submits its login credentials, the attacker sends an authentication failed message to the station. The station then removes itself from the WLAN. An attacker may also launch this attack by spoofing a station, sending invalid login credentials. The AP then denies the station access to the WLAN.

- **802.11 replay attack**—The attacker captures and resends legitimate frames. This attack can be used to overwhelm the network, spoof a legitimate user, or learn additional information about the network.

- **Decryption attack**—If an attacker is trying to crack the encryption used on your WLAN, your AP will receive a high number of encryption failures.

- **EAP start frame attack**—An attacker floods the AP with EAP start frames, causing the AP to allocate resources for each session. Eventually, the attack consumes all of the AP’s resources, creating a DoS.

- **TKIP attack**—An attacker tries to alter a frame and bypass the Michael integrity check. TKIP is designed to take countermeasures against such attacks, such as closing the session or refreshing the master key.

When a station exhibits a potentially harmful behavior, the Wireless Edge Services zl Module filters all traffic from the station for a certain period.
Configuring Thresholds for Station Intrusion Detection

To configure station intrusion detection, complete these steps:

1. Select **Special Features > Station Intrusion Detection > Configuration**.

2. In the **Detection Window** field, enter a value from 5 through 300 seconds. This setting determines the length of time to which each threshold applies. For example, if the threshold for **Excessive Probes** is 60 and the **Detection Window** is 10 seconds, the Wireless Module will count how many probes it detects in each 10-second time period.

3. Set the **Station** threshold for each field. Enter a number from 0 through 65,535. The Wireless Edge Services zl Module will apply this threshold to each station.
4. Set a Radio threshold and a Wireless Module threshold for:
   - Excessive Probes
   - Excessive Association
   - Excessive Disassociation
   - Excessive Authentication failure
   - Excessive Crypto replays
   - Excessive 802.11 replays
   - Excessive Decryption failures
   - Excessive Unassociated Frames
   - Excessive EAP Start Frames
   Again, enter a number from 0 through 65,535.

5. In the Time to Filter field, enter a time from 0 through 86,400 seconds to control how long the module will filter, or block, traffic from a station that exceeds a threshold. The default time is 60 seconds.

6. Click the Apply button.

Configuring the Module to Report Station Intrusion

You can also configure the module to send an alarm when it detects station intrusion. To configure this SNMP trap, complete these steps:

1. Select Management > SNMP Trap Configuration > Configuration.
2. Expand the Wireless heading and then the Intrusion Detection heading.
3. Select **Intrusion Detection** and click the **Enable all sub-items** button. (Alternatively, select one of the sub-items and click the **Enable** button.)

4. Make sure that the **Allow Traps to be generated** box is checked.

5. Click the **Apply** button.

The module will log the alarm, as well as forward it to a trap receiver (if one has been specified). (For instructions on configuring the trap receiver, see “SNMP Traps” on page 2-112 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)
Viewing Blocked Stations

If a station exceeds the thresholds that you set, the Wireless Edge Services zl Module blocks the station. You can view any stations that have been blocked by selecting Special Features > Station Intrusion Detection and clicking the Filtered Stations tab.

![Special Features > Station Intrusion Detection > Filtered Stations Screen](image)

Figure 12-44.Special Features > Station Intrusion Detection > Filtered Stations Screen
Logging and Alarms

The Wireless Edge Services zl Module generates logs for various events that occur on a system; these logs report on messages that the module receives and actions that the module takes. The module can log events to:

- its buffer
- the console
- an external server

Events are ranked according to severity, as shown in Table 12-2. The lower the number, the greater the risk to network functionality.

Table 12-2. Event Severity

<table>
<thead>
<tr>
<th>Level</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
</tr>
<tr>
<td>6</td>
<td>Info</td>
</tr>
<tr>
<td>7</td>
<td>Debugs</td>
</tr>
</tbody>
</table>

The Wireless Edge Services zl Module can also log alarms, which it receives when an SNMP trap is triggered. These alarms are stored in the module's local alarm log; the module can also forward alarms to an external server.
Configuring Logging

To configure logging, select Management > System Logging > Log Options.

Enabling Logging

As shown in Figure 12-45, logging is enabled by default, and the Wireless Edge Services zl Module logs events to:

- **Its buffer**—The module saves events that have collected in the buffer to its local log as they occur. Viewing this log is described in “Viewing Events in the Local Log File” on page 12-66. You can disable this feature by unchecking the **Enable logging to Buffer** box.

  By default, the module logs all events of severity level 3 or lower (more severe)—that is, all events from severity level 0 through level 3. You can raise or lower this level according to the needs of your network by selecting a level in the **Enable logging to Buffer** drop-down menu. Keep in mind that the higher the level, the more events through which you will have to search.

- **The console**—If you are managing your module through the console port, events will appear on the command line as they occur. You can disable this feature by unchecking the **Enable logging to Console** box. By default, events of severity level 3 or lower (more severe) are listed; you can raise or lower this setting.

---

**Table 12-3. Logged Events and Alarms**

<table>
<thead>
<tr>
<th>Logged Events</th>
<th>Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered when an event occurs on the module:</td>
<td></td>
</tr>
<tr>
<td>• the module receives a message</td>
<td></td>
</tr>
<tr>
<td>• the module takes an action</td>
<td></td>
</tr>
<tr>
<td>Can be sent to:</td>
<td></td>
</tr>
<tr>
<td>• the module’s local buffer (log file)</td>
<td></td>
</tr>
<tr>
<td>• the CLI console</td>
<td></td>
</tr>
<tr>
<td>• an external syslog server</td>
<td></td>
</tr>
<tr>
<td>Events are logged or not depending upon severity</td>
<td>Triggered when an SNMP trap is generated</td>
</tr>
<tr>
<td>Can be sent to:</td>
<td></td>
</tr>
<tr>
<td>• the module’s local alarm log</td>
<td></td>
</tr>
<tr>
<td>• an external SNMP server</td>
<td></td>
</tr>
</tbody>
</table>

Logged Events

Alarms

Triggered when an SNMP trap is generated

Can be sent to:

- the module’s local alarm log
- an external SNMP server

Events are logged or not depending upon whether the corresponding trap type is enabled
You can configure the module to store events for up to 60 seconds before logging them, by entering a value in the **Logging aggregation time** field. (If the value is 0, then events are logged immediately.)

**Forwarding Logs to an External Server**

You can also configure the Wireless Edge Services zl Module to forward logs to up to three external syslog servers. Complete these steps:

1. Select **Management > System Logging > Log Options**.
2. Check the Enable logging to Syslog Server box.

3. From the corresponding drop-down menu, select the lowest severity for logs that the module will forward. The default level is level 6, Info.

4. In the Server Facility field, use the drop-down menu to select the facility that your syslog server uses to receive such logs. Local7 is typically reserved for network devices.

5. In one of the Server fields, enter the server’s IP address. You can specify up to three syslog servers.

6. Click the Apply button.

Viewing Events in the Local Log File

To view the events that the Wireless Edge Services zl Module has stored in its own log file, select Management > System Logging and click the File Mgmt tab.
The top section of the screen displays files of logs that the module has stored. Each file is identified by its name, its size in bytes, the time at which it was created, and the time at which it was last modified (that is, when a new event was added to it).

The local log file stores the events that the Wireless Edge Services zl Module logs to its buffer.

You can view the types of events in a file by selecting the file. The preview id displayed in the bottom section of the screen, as illustrated in Figure 12-47.

To view the actual log file with all saved events, select the file and click the View button. A screen similar to the one shown in Figure 12-48 is displayed.
Figure 12-48. Viewing Logged Events

The most recent events are listed at the top of the screen. The color code helps you to quickly identify the most important events (that is, those with the lowest level, or greatest severity).

For each event, the log reports:

- **Time stamp**—Remember to look at the time stamp to make sure that you are not examining obsolete logs. (Quickly checking the time stamp when you preview the log file can also save you time.)

- **Module**—The module indicates which part of the system has reported this event. (Different modules report different types of activity.)

- **Severity**—It is often important to focus quickly on the most severe events, which, as mentioned above, the color code helps you to do.
Wireless Network Management
Logging and Alarms

- **Mnemonic**—This field includes an abbreviated identification of the type of event.

- **Description**—The description gives you the most information about the event.

You can click on any column heading to organize events according to the information in that column. The bottom of the screen shows you which line in the log file that you are currently examining.

You can also enter a value in the field at the bottom of the screen to quickly move to another page in the log.

Note that the Wireless Edge Services zl Module will continue to save events to this log. You can view newly saved events without leaving this screen by clicking the **Refresh** button.

Click the Close button to close the log and return to the Management > System Logging > File Mgmt screen.

Deleting and Transferring the Local Log File

If you are certain that neither you nor other administrators need to review the events in the log, you can select the log file on the Management > System Logging > File Mgmt screen and click the **Clear Buffer** button. The module erases the contents of the file, allowing you to focus on the most important events.

If the buffer should become full, the next event will write over the oldest (least recent) event.

It is often a good idea to store a copy of the log remotely before you clear it. Your organization might also have a policy of periodically collecting device information and storing it on a central server.
To transfer the local log file, complete these steps:

1. Click the **Transfer Files** button. The **Transfer** screen is displayed.

![Figure 12-49.Transferring Log Files to a Server or Workstation]

2. In the **From** field in the **Source** section, use the drop-down menu to select **Wireless Services Module**. In the **File** field, use the drop-down menu to select the log file that you want to transfer.

3. Select the destination for the file. You can save the log to your workstation or to a remote server:
   a. To save the log to your workstation, in the **To** field, use the drop-down menu to select **Local Disk**.
      
      You can then enter the filename in the **File** field and click the **Browse** button to select the destination for the file.
   b. To save the log to a remote server, in the **To** field, use the drop-down menu to select **Server**. Then enter this information in the fields below:
      - **File**—Name the file on the remote server. (This name can be different from that of the source file.)
      - **Using**—Use the drop-down menu to select the type of server. You can use a TFTP or an FTP server.
      - **IP Address**—Specify the server’s IP address.
      - **User ID** and **Password**—FTP servers may require you to enter the correct username and password.
Wireless Network Management
Logging and Alarms

Path—Enter the path for the directory in which the destination file should be saved. Depending on your server, you may or may not need to enter / before the directory name. Leave this field empty (or simply enter /) to save the file to the server's default directory.

4. Click the Transfer button.

Managing the Alarm Log

In order for the Wireless Edge Services zl Module to log an alarm, you must activate the corresponding trap. See “SNMP Traps” on page 2-112 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module” for information on setting these traps. When an enabled trap is triggered, the module generates an entry in its alarm log. If you have configured an SNMP server, the module will also send the alarm to it.

View the alarm log by selecting Device Information > Alarm Log.

A list of alarms that the module has logged is displayed, as shown in Figure 12-50.

<table>
<thead>
<tr>
<th>Index</th>
<th>Status</th>
<th>Time Stamp</th>
<th>Severity</th>
<th>Module Name</th>
<th>Associated</th>
<th>Type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:42 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>27</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:42 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>28</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>29</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>30</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>31</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>32</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>33</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>34</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>35</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>36</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>37</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>38</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
<tr>
<td>39</td>
<td>Unacknowledged</td>
<td>Wed Apr 18 10:24:48 2007 G.</td>
<td>Normal</td>
<td>wireless ...</td>
<td>dissociated</td>
<td>Station ...</td>
<td>00-0E-35-94-2C-88, radio 1</td>
</tr>
</tbody>
</table>

Figure 12-50.Viewing the Alarm Log
For each alarm, the screen displays this information:

- **Index**—Alarms are numbered in the order in which they were received.
- **Status**—If the alarm has been acknowledged, then an administrator has seen it and presumably dealt with it.
- **Time Stamp**—Among other purposes, you can view the time stamp to:
  - check whether a problem is ongoing
  - look for the cause of a behavior that you know occurred at a particular time
  - track patterns of activity
  - determine the duration of a problem
- **Severity**—Severity signals the relative threat to network functions and security.
- **Module Name**—You can use the name of the module that reported the alarm to point you toward the cause.
- **Type**—You should quickly focus on this information, as it is, in many ways, the alarm. It indicates the type of problem or behavior.
- **Message**—The message, which varies according to the alarm’s type, includes specific information about the particular event. For example, the message for the “radiusAuthFailed” alarm is the MAC address of the station that failed to authenticate and the radio to which the station attempted to connect. You could use this information to track down the station.

By default, the alarm log lists alarms according to index number. However, you can sort the alarms according to any of the information described above, by simply clicking on the heading for the column.

For example, you might want to focus on only the most serious events. Click **Severity** and scroll to the top of the list to view the most crucial alarms.

Or, if you are troubleshooting a particular problem, you might want to group alarms by **Module Name**—to see, for example, all the logs associated with wireless stations when you are troubleshooting a station having difficulty with its connection.

You can take action on alarms using the four buttons at the bottom of the screen:

- **Details**
- **Delete**
- **Acknowledge**
- **Export**
Details

When you do not know what an alarm means, or when you need direction in solving the problem indicated, you should view alarm details.

Select the alarm from the list, and then click the Details button. The screen that is displayed points you toward the cause of the alarm and possible solutions for an associated problem. (See Figure 12-51.)

![Figure 12-51.Viewing Alarm Details](image)

General information that applies to all alarms of this type is listed in the Alarm Details section. The interface explains what the alarm means and suggests possible solutions or causes. For example, details for a “radiusAuthFailed” alarm suggest that you verify that your Wireless Edge Services zl Module can connect to its RADIUS server.

The Alarm Message shows information specific to this alarm—in Figure 12-51, identifying the station that failed to authenticate. Other information specific to the log is listed throughout the screen, with the time stamp at the top and the status at the bottom.

Delete

You should periodically delete from the log alarms that are unimportant or no longer relevant, so that you can easily focus on the most current alarms. For example, you could group alarms by time stamp, use the Shift key to select all events before a particular date, and then click the Delete button.
Acknowledge

Sometimes you will want to store an alarm in the log even after you have viewed it, either because you want another administrator to see it or because you want to track a particular pattern of activity. In this case, instead of deleting the alarm, you should click the **Acknowledge** button to change its status.

You should only acknowledge an alarm, of course, if you have addressed any associated problems; otherwise, other administrators may also neglect to do so.

Export

The Wireless Edge Services zl Module allows you to save logged information to your workstation. This useful feature lets you:

- save information that might be important later, while keeping the log clear for future events
- send a file of alarms to support staff for troubleshooting help
Wireless Network Management
MAC Filters (Local MAC Authentication)

- pool information from multiple devices in a central location
- track patterns of network activity

To export the information in one or more alarms, select those alarms and click the **Export** button. On the screen that is displayed, select a filename and a location for the logs, which are saved as a comma-separated file.

---

**MAC Filters (Local MAC Authentication)**

The Wireless Edge Services zl Module can control which wireless stations connect to a WLAN according to their MAC, or hardware-based, addresses. You configure standard MAC ACLs, or filters, and the module blocks stations denied by those ACLs before they can authenticate and associate with the WLAN.

MAC authentication can act by itself or in conjunction with another form of authentication. For example, you could configure ACLs for MAC authentication and apply them to a WLAN; you could also enable Web authentication on that WLAN. When a station attempts to connect to the WLAN, the module first checks the station’s MAC address. If the ACLs allow the station, the module lets the station proceed to associate to the WLAN and complete the Web authentication.

MAC authentication is particularly important with Web authentication because without it, stations can actually connect to the WLAN before they authenticate.

The module supports up to 1,000 ACLs, each of which can specify a range of MAC addresses.

To configure MAC authentication, complete these steps:

1. Configure one or more filters, or ACLs.
2. Configure WLAN memberships for each ACL.
Configuring MAC Standard ACLs (Filters)

When configuring ACLs on the module, keep these rules in mind:

- ACLs are ordered by index number.
- The module processes ACLs that are applied to a WLAN starting with the ACL that has the lowest index number. The module stops processing the ACLs as soon as it finds a match for the station’s MAC address.
- The module supports two types of ACLs:
  - **Allow ACLs**—If the module matches a station to this ACL, it permits traffic from the station.
  - **Deny ACLs**—If the module matches a station to this ACL, it blocks all traffic from the station, and the station cannot associate to the WLAN.
- By default, the module allows all stations. Unless you explicitly deny a station in an ACL, it can connect.

You will generally follow one of two strategies for MAC authentication:

- **Deny all stations except a select group of authorized stations.**
  
  In this case, you should create one or more allow ACLs that specify the group of authorized stations. Then you should create a deny ACL that specifies all stations (00-00-00-00-00-00 through FF-FF-FF-FF-FF-FF). The index numbers for the allow ACLs must be lower than that for the deny ACL.

- **Allow all stations except a select group of unauthorized stations.**
  
  In this case, you should create one or more deny ACLs that specify the MAC addresses of unauthorized stations. You do not need to create an allow ACL, because allowing all stations is the module’s default behavior.

You can, of course, also combine the strategies—for example, deny a station with a range of allowed stations.

To configure an ACL, complete these steps:

1. Select **Security > MAC Filters.**
2. Click the Add button. The Add ACL screen is displayed.
3. Enter a value from 1 through 1,000 in the **Station-ACL Index** field. Each ACL must have a unique index number. Pay close attention to this number because, when a station matches more than one entry, only the entry with the lowest number affects the station.

4. Enter a range of MAC addresses, placing the first address in the **Starting MAC** field and the last address in the **Ending MAC** field. Every MAC address between the two is included in the list. You cannot add noncontiguous MAC addresses to the ACL; instead, you must create a new ACL.

5. Using the **Allow/Deny** drop-down menu, select whether the module will permit traffic from these stations (**Allow**) or block it (**Deny**).

6. Click the **OK** button.

The ACL is listed on the **Security > MAC Filters** screen.

**Configuring WLAN Memberships**

The ACL will not affect traffic until you associate the ACL with one or more WLANs. To do so, you make the ACL a member of those WLANs.

Complete these steps:

1. On the **Security > MAC Filters** screen, select the ACL.

   You can select multiple ACLs by holding down **Ctrl** as you select them.

2. Click the **Memberships** button. The **Edit Memberships** screen is displayed. (See Figure 12-55.)
3. Check the boxes for the WLANs to which you want to apply the ACL.

   WLANs are displayed by index (not SSID). The module will use the ACL to filter traffic on the selected WLANs.

   If you have selected multiple ACLs, they are listed in separate columns by index number. (See Figure 12-56.)
Figure 12-56. Assigning ACLs to WLANs

4. Click the OK button.

When you select this ACL on the Security > Wireless Filters screen, the selected WLANs appear in the Associated WLANs section. (See Figure 12-57.) In this screen, you can view the WLAN’s SSID, as well as other security options for that WLAN.
Wireless Network Management
MAC Filters (Local MAC Authentication)

Figure 12-57. Associating ACLs with WLANs

Note that it is possible to prevent a station from associating to one WLAN but to allow the station to associate to another.

Just as you can make an ACL a member of more than one WLAN, you can associate more than one ACL to a WLAN. The module filters traffic first against the ACL with the lowest index number, then against the ACL with the next lowest number, and so on. Parsing stops with the first successful match to an ACL.

In Figure 12-57, network administrators have created four ACLs. The first ACL denies a single station, the second and third ACLs allow stations, and the fourth ACL denies all stations. The network administrators made all these ACLs members of the WLAN called MyWLAN.
With this configuration, only the stations allowed by ACLs 2 and 3 can connect to MyWLAN. Notice that the network administrators have numbered the ACL that denies all stations as 100. They can add ACLs to allow other stations, and as long as these ACLs have an index number lower than 100, the Wireless Edge Services zl Module will process them before it processes the ACL that denies all stations.

Exporting and Importing MAC Standard ACLs (Filters)

You can export the MAC standard ACLs (filters) configured on the Wireless Edge Services zl Module to the local disk of the management station. Exporting the ACLs enables you to archive them and also to upload them to another device that needs to enforce the same policies.

The filters save as a .cvs file, which you can open with a spreadsheet application. This file includes four columns for information in the ACL:

- Station ACL Index
- Starting MAC
- Ending MAC
- Allow/Deny

The first line in the file lists these four names. Each subsequent line specifies the values associated with one of the exported ACLs.

You can also import a .cvs file to the Wireless Edge Services zl Module. In this way, you can quickly configure all of your modules with the same MAC standard ACLs. See “Importing MAC Standard ACLs” on page 12-84 for information on information that the .cvs file must include.

Exporting MAC Standard ACLs

To export the MAC standard ACLs configured on your module, follow these steps:

1. Select Security > MAC Filters.
2. Select the ACL that you want to export.

If you want to export all of the ACLs in the same file, select an ACL and then press Ctrl+A.
3. Click the **Export** button.

4. A dialog screen is displayed for saving the file to the local disk of your management station. Name the file and choose the directory in which to save it. Then confirm the save.

5. A screen reports that the export was successful. Click the **OK** button.
Importing MAC Standard ACLs

Instead of (or in addition to) manually configuring MAC standard ACLs (filters) on your Wireless Edge Services zl Module, you can import a .cvs file that includes these ACLs to your module. The file should be saved on the local disk of your management station.

You can create the ACLs file using a spreadsheet application. Include four columns for each ACL. Table 12-4 displays the information specified in that column and valid values for that column. The column number matters; in other words, the first column for each row must include a number from 1 to 1000, and this number specifies the ACLs index number.

Table 12-4. Required Information in a File To Be Imported to the Wireless Edge Services zl Module’s List of MAC Filters

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Specifies</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Station-ACL Index—the order in which the module processes this ACL (as compared to other MAC standard ACLs)</td>
<td>1 to 1000</td>
</tr>
<tr>
<td>2</td>
<td>Starting MAC—first MAC address in the range of addresses selected by this ACL</td>
<td>any MAC address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>3</td>
<td>Ending MAC—final MAC address in the range of addresses selected by this ACL (often the same as the starting address)</td>
<td>any MAC address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>4</td>
<td>Allow/Deny—the action the module performs on selected stations (does or does not allow them to connect to the WLAN)</td>
<td>• Allow  • Deny</td>
</tr>
</tbody>
</table>

Alternatively, you can configure ACLs on another module, export the ACLs to a .cvs file, and then import that file to your module.

When you import the file, the Wireless Edge Services zl Module saves each row in the imported file as an ACL in its list of MAC standard ACLs (filters). Your module can already have filters configured on it; the ACLs in the imported file are simply added to the list.

The new ACLs should have different index numbers than the current ACLs. If you want the imported ACLs to override the currently configured ACLs, you should delete those ACLs first.
To import MAC standard ACLs to your Wireless Edge Services zl Module, follow these steps:

1. Select **Security > MAC Filters**.
2. Click the **Import** button.

3. A dialog screen is displayed for choosing the file from the local disk of your management station. Find your file and confirm the import.

4. A screen reports the results of the import. If the import is completely successful, the message shown in Figure 12-61 is displayed.

   If you see any errors, refer to “Resolving Import Errors” on page 12-86.
5. Click the **OK** button.

6. For the imported ACLs to take effect, you must assign them WLAN memberships:
   a. Select the new ACLs. You can select multiple ACLs by holding down **Ctrl** as you select them.
   b. Click the **Memberships** button.
   c. Check boxes to assign the ACLs to WLANs.
   d. Click the **OK** button.

   See “Configuring WLAN Memberships” on page 12-78 for more information.

**Resolving Import Errors.** When you attempt to import ACLs, the **ACL Import Result** screen may display one or more errors.

The errors are listed by the line in the .cvs file at which the error occurs.
Errors include:

- messages informing you that a field contains an invalid value:
  - “ACL index must be an integer”
  - “Invalid starting MAC.”
  - “Invalid ending MAC.”
  - “ACL mode must be either Allow or Deny”

As explained earlier, each line in the file must include four fields with valid values for index number, MAC addresses, and ACL mode (allow or deny).

The screen in Figure 12-62 displays four such errors—all in line 1. In this case, the imported file is a file exported from another module. Exported files use the first line to list the names of columns rather than to specify an ACL. You can ignore the errors. Click OK, and the ACLs are imported to the module.

If the line indicated should specify an actual ACL, click the Cancel button. Open the file, find the line with the error, and make the correction. See Table 12-4 on page 12-84 for help in specifying correct values.

Then re-import the file, as described in “Importing MAC Standard ACLs” on page 12-84.
“ACL index already exists - please choose another”

The ACL in the line indicated conflicts with an ACL already configured on the Wireless Edge Services zl Module. That is, they have the same index number.

Make one of two choices:

- Click the **OK** button, and import the file despite the conflict. The module retains all of its already-configured ACLs. However, any non-conflicting ACLs are imported normally.
- Click the **Cancel** button, and cancel the import. The module retains all of its already-configured ACLs, and no new ACLs are saved to the module. You can fix the problem in one of two ways:
  - If you want your Wireless Edge Services zl Module to keep its current ACLs, but also to receive all of the imported ACLs, edit the .cvs file. Change the index numbers so that they no longer conflict with those on the module. Then re-import the file, as described in “Importing MAC Standard ACLs” on page 12-84.
  - If you want the ACLs in the imported file to override already-configured ACLs, you must delete these ACLs from your Wireless Edge Services zl Module.

In **Security > MAC Filters** screen, select the ACLs that conflict with imported ACLs. Click the **Delete** button.

Then re-import the file, as described in “Importing MAC Standard ACLs” on page 12-84.
Network Self Healing

Self healing keeps your wireless network functioning optimally in response to changing conditions. A radio in a self-healing network can automatically change the properties of its RF network, which include:

- channel
- transmit power
- supported rates

By managing this ability, the Wireless Edge Services zl Module provides two basic services:

- **Neighbor recovery**—When radios detect that a neighbor has failed, they automatically adjust settings so that they can support as many of the stations associated with the failed radio as possible.
- **Interference avoidance**—Radios adjust their channel setting to avoid interfering with neighboring radios.

Neighbor Recovery

When enabled on the Wireless Edge Services zl Module, neighbor recovery can automatically configure radios to change their settings to compensate for another radio's failure.

Both the Wireless Edge Services zl Module and RP radios monitor for failed radios. The RPs monitor neighbors by listening for beacons from RPs that they have learned that they can hear on their channel.

**Note**

Both single-channel detectors and dedicated detectors can monitor neighbors. However, dedicated detectors monitor all channels instead of just one. For this reason, it can be a good idea to configure one RP in a self-healing network as a dedicated detector (depending, of course, on the total number of RPs).

A radio “fails” in any of these circumstances:

- The module no longer recognizes the RP as adopted.

  In other words, the module and the RP cannot communicate, whether due to a physical or a logical problem.
Wireless Network Management
Network Self Healing

- Neighbors no longer receive beacons from the radio.
  
  An RP checks the beacons that it has received every 30 seconds. If the RP has not received beacons from a neighbor in the last two seconds, it reports that neighbor as down. In other words, an RP considers a neighbor failed when it loses contact with that neighbor for more than two seconds; however, the RP only checks whether it has lost contact with a neighbor every 30 seconds.

- Neighbors fail to detect Wireless Internet Service Provider (WISP) heartbeats from the radio.

Enabling Neighbor Recovery

To enable neighbor recovery, complete these steps:

1. Select **Special Features > Self Healing > Configuration**.

   ![Figure 12-63. Enabling Neighbor Recovery](image)

   - Enable Neighbor Recovery
   - Interference Avoidance
     - Enable Interference Avoidance
     - Average Retries: 14 (0.0 - 15.0)
     - Hold Time: 3080 (0 - 65535 seconds)

2. Check the **Enable Neighbor Recovery** box.

3. Click the **Apply** button.
An RP radio only responds to the loss of a radio if that radio is defined as one of its neighbors. To further configure neighbor recovery, you must:

- specify neighbors
- specify the action that a radio takes if one of its neighbors fails

Select **Special Features > Self Healing** and click the **Neighbor Details** tab.

![Table of Neighbor Relationships](12-64.png)

**Figure 12-64. Neighbor Relationships**

The screen lists all RP radios adopted by this module, displaying this information for each:

- **Radio Index**—index number
- **Description**—name
- **Type**—802.11bg or 802.11a
- **RP Ethernet MAC**—Ethernet MAC address for the RP that includes this radio
- **Action**—self-healing action when a neighbor fails
- **Neighbor Radio Indices**—neighbors’ index numbers

When you first enable the self-healing feature, all radios display **None** in the **Neighbor Radio Indices** column.
You can configure the neighbors in one of two ways: manually or with automatic neighbor detection.

**Specifying Neighbors Manually**

Keep these concepts in mind as you configure neighbors:

- The neighbor relationship is reciprocal: if you configure a neighbor list on radio 1 that includes radio 3, radio 3’s neighbor list automatically adds radio 1. (See Figure 12-64.)
- However, the relationship is not communicative: if radio 1’s neighbor list includes both radio 3 and radio 4, radio 3’s list will include radio 1, but radio 3’s list will not include radio 4 unless you explicitly configure radio 4 and radio 1 as neighbors.
- You configure neighbors on a per-radio basis. That is, instead of configuring a group of neighbors with certain members, you assign each radio a list of neighbors.

To assign neighbors to a radio, complete these steps:

1. Select **Special Features > Self Healing** and click the **Neighbor Details** tab. In the upper-right corner of the screen, verify that neighbor recovery is enabled.

![Figure 12-65.Configuring Neighbors](image)
All RP radios adopted by this module are listed.

2. Select a radio and click the **Edit** button. The **Edit Neighbor** screen is displayed. (See Figure 12-66.)

![Figure 12-66. Editing Neighbors](image)

The available RP radios—those adopted by this module—are listed on the left under **Available Radios**: these are potential neighbors.

3. To add a neighbor, select a radio from the field on the left and then click the **Add** button. The radio moves to the right; it is now the neighbor of the radio that you are editing.

You can add up to 16 neighbors, including radios that use a different 802.11 mode than the radio for which you are selecting neighbors. Keep in mind, however, that if the second radio's wireless stations do not support the other mode, then this radio cannot help them.

4. To remove a radio from the neighbor list, select that radio from the list on the right and click the **Remove** button.

5. In the **Self Healing Action** field, use the drop-down menu to select the action that this radio takes when a neighbor fails. Because you must also complete this step when you use automatic neighbor detection, configuring this setting is described in “Selecting the Self-Healing Action” on page 12-95.
6. Click the OK button.

You return to the Special Features > Self Healing > Neighbor Details screen, on which you can confirm the neighbors in the Neighbor Radio Indices column for the radio that you were editing. Note that the neighbors also display the edited radio in their Neighbor Radio Indices column.

Configuring Radios to Automatically Detect Neighbors

Instead of manually configuring neighbors, you can have RP radios detect each other and choose their own neighbors. In this case, each radio will select the three other radios from which it receives the strongest signal.

To use this option, complete these steps:

1. Select Special Features > Self Healing and click the Neighbor Details tab.
2. Click the Detect Neighbors button. The Automatic Neighbor Detection screen is displayed. (See Figure 12-67.)

![Automatic Neighbor Detection Screen](image)

**Figure 12-67. Automatic Neighbor Detection Screen**

**Note**

As soon as you enable this feature, every RP disassociates its wireless stations and begins scanning for neighboring RPs. For this reason, it is particularly important that you configure self healing when the wireless network is inactive.

Remember also that any manually defined neighbors for radios are erased when you click the Detect Neighbors button.

3. To confirm that you want RPs to begin detecting neighbors, click the Yes button.

After RPs have selected their neighbors, you must define the action that they will take when a neighbor fails, as described in the next section.
Selecting the Self-Healing Action

The Wireless Edge Services zl Module can configure RPs to take one of several actions in response to a failed neighbor. A radio can:

■ open its data rates so that it supports both 802.11g and 802.11b stations

   For example, one radio in your network might operate in G-only mode (that is, it supports higher data rates only) while a nearby radio also supports the lower data rates of 802.11b. You might configure the first radio to add the lower data rates so that it can support both types of stations if the second fails.

■ raise its transmit power to the maximum allowable power in your regulatory domain

   You might have lowered the transmit power because you have placed RPs close together for denser coverage. Raising the transmit power when one RP fails increases the chance that stations can receive a good signal from remaining radios.

   In some cases, you may need to configure a self healing offset to prevent the RP radio from raising its power too high. See “Configuring a Self Healing Offset” on page 12-98.
both raise its transmit power and open its data rates (see Figure 12-68)

Sometimes you lower radios’ transmit power so that closely grouped RPs can support higher data rates within their relatively small coverage areas. When an RP radio raises its transmit power to take over a failed neighbor’s coverage area, it can no longer support high data rates for all stations (some are too far away). In this case, you should remember to configure the radio to open its data rates as well as raise its power. (This is the default action.)
Wireless Network Management
Network Self Healing

- take no action

Remember that radios are always neighbors to each other. However, you might want one radio to respond to the failure of a second radio, but you might not want the second radio to respond to the failure of the first radio. For example, the second radio might be in a more important location. When editing the second radio, configure it to take no action.

**Note**

If you configure a dedicated detector to take action when a neighbor fails, that radio automatically changes to single-channel detector mode when it takes the action so that it can support wireless stations.

Keep these considerations in mind as you configure the action:

- You configure an action for a radio, not for a neighbor. The radio must take the same action no matter which of its neighbors fails.
- You can configure one action for one radio and another for one of its neighbors. For example, you might configure one radio to open its data rates, but you might configure the neighbor to take no action.

To configure the self-healing action, complete these steps:

1. Select **Special Features > Self Healing** and click the **Neighbor Details** tab. In the upper-right corner of the screen, verify that neighbor recovery is enabled.

2. Select the radio for which you want to define the action, and then click the **Edit** button. The **Edit Neighbors** screen is displayed. (See Figure 12-69.)
Wireless Network Management
Network Self Healing

3. In the **Self Healing Action** field, use the drop-down menu to select the action:
   - **Open Rates**—to configure the radio to support all data rates
   - **Raise Power**—to configure the radio to raise its power to the legal maximum. See “Configuring a Self Healing Offset” on page 12-98 to determine whether you will need to configure a self healing offset.
   - **Both**—to configure the radio to take both of these actions. This is the default setting.
   - **None**—to configure the radio to take neither of these actions.

4. Click the **OK** button.

Configuring a Self Healing Offset

When you configure a radio to raise its transmit power as part of neighbor recovery, you must configure a self healing offset for that radio if it meets either of these criteria:
- It uses an external antenna.
- It is located close to another RP radio.
The Wireless Edge Services zl Module subtracts the offset from the maximum power allowed in your regulatory domain to define the maximum power for that radio. To configure this parameter, complete these steps:

1. Select **Network Setup > Radio > Configuration**.
2. Select the radio and click the **Edit** button. The **Configuration** screen for the selected radio is displayed. (See Figure 12-70.)

![Figure 12-70.Configuring the Self Healing Offset Option](image)

3. In the **Advanced Properties** section, enter a value in the **Self Healing Offset** field.
   
   Base the offset on the radio’s antenna gain and the rules of your regulatory domain as explained in [http://www.hp.com/rnd/support/manuals/rports.htm](http://www.hp.com/rnd/support/manuals/rports.htm).

4. Click the **OK** button.
Interference Avoidance

Also called dynamic channel selection, interference avoidance helps your RP radios choose the best channel in your environment at the moment. If the Wireless Edge Services zl Module detects interference on a radio’s current channel, it has the radio use Auto-Channel Selection (ACS) to choose a new channel.

The module implements this procedure for interference avoidance:

1. Every time a wireless station’s packet fails to reach its destination, presumably because of a collision, the station resends the packet. For each RP radio, the module tracks the average number of times in the last 30 seconds that stations reattempted to send a packet.

2. If a radio’s average retries exceeds a specified threshold, the module assumes that the excessive collisions are caused by another device operating on the same channel. (This could be an RP in another WLAN, a rogue RP, or even wireless headsets.)

3. The module has the RP radio use ACS to select a new channel based on the best SNR.

To enable interference avoidance, complete these steps:

1. Select Special Features > Self Healing > Configuration.
2. Select the **Enable Interference Avoidance** box.

3. Typically, you should leave the settings for this feature at their defaults. However, you can customize them:
   a. In the **Average Retries** field, enter a value from 1 through 15 to set the threshold for the number of times stations must resend frames during a 30-second interval. The default value is 14, which means that, if in a 30-second interval the average station must resend a packet 15 times, the radio will select a new channel.

   Resending packets 14 times implies a relatively high latency, and you can lower the threshold. Be aware, however, that changing channels is a relatively drastic action that radios should not take too often.
b. In the **Hold Time** field, enter a time from 0 through 65,535 seconds. This setting determines how long a radio must wait in between selecting a new channel and again running ACS. If you set this value too low, then radios might begin to run ACS continuously, preventing stations from associating to them.

   By default, the **Hold Time** is set at 3,600 seconds (one hour).

4. Click the **Apply** button.
sFlow Agent

Contents

Overview ................................................................. 13-2
  Flow Sampling by the sFlow Agent ......................... 13-2
  Counter Polling by the sFlow Agent ....................... 13-3
  sFlow Receiver .................................................. 13-4
  Configuring sFlow Receiver Instances ..................... 13-4
Configuring sFlow Using the Web Browser Interface .......... 13-7
  Manually Configuring sFlow Receiver Instances Using the
  Web Browser Interface ........................................... 13-8
  Manually Activating Flow Sampling ......................... 13-11
  Manually Activating Counter Polling ...................... 13-14
Overview

The Procurve Wireless Edge Services zl Module contains an sFlow agent. The sFlow agent samples traffic, treating the traffic that arrives on each adopted RP radio as a separate flow. In other words, the module’s sFlow agent monitors each radio much as a switch might monitor each physical interface.

The sFlow agent forwards traffic information to an sFlow collector. Another term for an sFlow collector is an sFlow receiver. For the rest of this chapter, this guide will use the term “sFlow receiver.”

The agent can create six separate instances for each flow, and forward the information for each instance to a different sFlow receiver.

The Wireless Edge Services zl Module supports the two sampling mechanisms of sFlow, which are designed to work together to produce an accurate picture of network traffic:
- flow sampling
- counter polling

An advantage of the module’s sFlow capabilities is that the picture not only details how much traffic radios handle, but also the types of traffic and the devices that generate it.

Flow Sampling by the sFlow Agent

Traffic analysis techniques differ in the way that agents collect and process traffic. Some techniques have the agent copy all traffic to the receiver, but this strategy can create prohibitive overhead. With other techniques, the agent groups traffic into flows, summarizes information about each flow, and sends the summary to the collector. However, this approach requires the agent to inspect all traffic and consumes significant resources within the agent.

The sFlow technology, rather than requiring the agent to inspect every packet that passes through, uses sample-based profiling. That is, the agent inspects approximately every “nth” packet from each data source available to sFlow. The sampling algorithm is designed to give a high certainty that the sampled traffic mirrors the total traffic within a small margin of error.
On the Wireless Edge Services zl Module, data sources are RP radios, and “n,” the packet sampling rate, is configurable per-radio and sampling instance (up to six per radio). In other words, the module orders radios to send approximately every “nth” packet to the module’s sFlow agent to be sampled, packaged, and sent to the sFlow receiver or receivers.

**Note**

Only 802.11 data frames are sampled. The sFlow agent does not sample management and control frames such as beacons.

The sFlow agent packages samples into small datagrams which include, among other information:

- sampled packets’ headers
  - The agent decrypts an encrypted header before sampling it.
- sampled packets’ inbound or outbound interface
  - For a wireless network, the inbound interface is the radio.
- information about how sampled packets are being forwarded

The extra information in the datagram helps an sFlow receiver to create a detailed, as well as accurate and up-to-date, picture of network activity. An advantage of sFlow is that datagrams are nonetheless compact and do not require a large amount of network bandwidth. The sampled packets are approximately 7 percent of the original packet size, and several samples can fit in a single datagram. The same datagrams that include packet samples can also include counters reported by polled radios (see “Counter Polling by the sFlow Agent” on page 13-3). Since only some packets are sampled, sFlow creates very little overhead. For example, if you set the sampling rate to one packet in 100, flow sampling only adds about .7 percent overhead.

The module uses datagram version 5, and the default datagram size is 1400 bytes. (The size is configurable although you should usually accept the default. See “Manually Configuring sFlow Receiver Instances Using the Web Browser Interface” on page 13-8 for more information.)

**Counter Polling by the sFlow Agent**

In addition to sampling approximately every “nth” packet, the Wireless Edge Services zl Module’s sFlow agent can sample the counters tracked by radios. These counters include traffic statistics such as the number of inbound frames, outbound frames, and retransmitted frames.
Counter polling works with flow sampling to create a more comprehensive picture of network traffic. The counters for total traffic supplement the more detailed information collected for samples.

The sFlow agent obtains the counters by periodically polling radios. The agent polls radios as needed to fill datagrams most efficiently. However, you can configure the maximum time that can elapse before a radio must be polled.

sFlow Receiver

The sFlow receiver, which receives samples from agents all over the network, combines and analyzes the samples to produce a picture of network activity. This picture can be quite detailed. For example, the sFlow receiver can determine not only how much traffic the Wireless Edge Services zl Module's RP radios are handling, but also which devices are contributing to that traffic—and which are contributing most.

Capabilities vary among sFlow receivers; some uses for sFlow include:

- establishing a baseline picture of network activity against which later activity can be compared and analyzed for signs of security breaches
- monitoring congestion and other Quality of Service (QoS) issues
- auditing and billing for network usage
- finding and diagnosing network problems

An sFlow receiver can effectively monitor a large network because sFlow's sampling techniques extract only the necessary data from the traffic streams on each data source, consuming minimal device and network resources in the process. This approach shifts the burden of data manipulation and analysis from the sFlow agent to the sFlow receiver. In addition, the receiver can generate an accurate picture of network traffic even when agents sample a relatively small percentage of traffic.

An example of an sFlow receiver is ProCurve Manager Plus (PCM Plus).

Configuring sFlow Receiver Instances

As described above, an sFlow agent forwards datagrams to an sFlow receiver. Each relationship between an agent and a receiver is called a receiver instance. Often the receiver uses the SNMP protocol to contact the agent, reserve a receiver instance, and configure sFlow. Alternatively, receiver instances can be set up on the agent itself.
The Wireless Edge Services zl Module can accommodate up to six sFlow receivers. The module’s receiver instances can be configured in one of three ways:

1. The sFlow receiver contacts the module’s agent and uses SNMP to reserve and configure a receiver instance (only instances 4, 5, and 6).

   The sFlow receiver reserves the instance by writing its owner string into that instance on the sFlow receiver table. The receiver also configures a receiver timeout value for itself. The agent counts down the receiver timeout; when the timeout nears expiration, the sFlow receiver can reset the timeout to a higher value if it wants to retain control of the instance. But if the receiver no longer needs samples from the agent, it allows the timeout to expire. The agent erases the sFlow receiver’s owner string and allows another sFlow receiver to claim the instance.

   When the sFlow receiver reserves a receiver instance, it also configures one or both of two types of sFlow instances. One type allows the receiver to receive flow samples, and the other allows it to receive counters from polled radios.

   When an sFlow receiver automatically configures sFlow, all settings are controlled through the sFlow receiver’s management software, including settings for flow sampling rates and counter polling intervals.

   You must ensure that the sFlow receiver can contact the Wireless Edge Services zl Module via SNMP, but you do not need to complete any steps to set up sFlow. (See “SNMP Support” on page 2-24 of Chapter 2: “Configuring the ProCurve Wireless Edge Services zl Module.”)

2. You configure the instance manually through the command line interface (CLI).

   Use this (or the next) option when the sFlow receiver cannot configure the receiver instance itself. You might also choose this option for increased security. You control to which sFlow receivers the Wireless Edge Services zl Module forwards datagrams.

   See Appendix A: “ProCurve Wireless Edge Services zl Module Command Line Reference.”

3. You configure the instance manually through the Web browser interface (only instances 4, 5, and 6).

   As with the CLI option, use this option when the sFlow receiver cannot configure the receiver instance itself or when you want more control.
You must specify all settings, including the sFlow receiver’s IP address and port, as well as owner string and timeout. To enable packet sampling or counter polling, you must configure an available sFlow instance of the appropriate type. Then match the instance to the receiver instance.

This chapter focuses on configuring sFlow manually through the Web browser interface.
Configuring sFlow Using the Web Browser Interface

The Wireless Edge Services zl Module’s sFlow agent is enabled by default. If your sFlow receiver (sometimes called an sFlow collector) can control the agent through SNMP, you do not need to configure the module further.

You can check the module’s sFlow agent and verify that it is compatible with your sFlow receiver’s SNMP capabilities. Select **Special Features > sFlow > Agent**.

![Special Features > sFlow > Agent Screen](image)

**Figure 13-1. Special Features > sFlow > Agent Screen**

In order to manage an sFlow agent, an sFlow receiver must know how the agent implements sFlow. The screen displays this information about the agent:
sFlow Agent
Configuring sFlow Using the Web Browser Interface

- **sFlow MIB Version**—the agent’s MIB version. The MIB specifies how the agent extracts and bundles sampled data, and the sFlow receiver must support the agent’s MIB. The Wireless Edge Services zl Module’s MIB version is 1.3, so your sFlow collector’s version must also be at least 1.3.

- **Organization**—HP. The sFlow receiver must also know the organization to identify the implementation of sFlow on this agent.

- **Revision**—the Wireless Edge Services zl Module’s current software image.

- **Address Type**—the protocol version for IP addresses.

- **Address**—the Wireless Edge Services zl Module’s management IP address. You should always configure a static address on the management interface when implementing sFlow.

If your sFlow receiver cannot configure the Wireless Edge Services zl Module’s sFlow agent, you must configure sFlow manually. Complete the following tasks to configure the Wireless Edge Services zl Module to act as an sFlow agent:

1. Configure up to three sFlow receiver instances through the Web browser interface.
   
   From the CLI, you can configure three more sFlow receiver instances.

2. Configure flow sampling instances for RP radios:
   a. To control where the agent sends this radio’s samples, match the flow sampling instances to receiver instances.
   b. Specify how frequently radios sample packets.

3. Configure counter polling instances for RP radios:
   a. To control where the agent sends this radio’s counters, match the counter polling instances to receiver instances.
   b. Specify how frequently radios are polled for the counters.

Manually Configuring sFlow Receiver Instances Using the Web Browser Interface

The Wireless Edge Services zl Module can forward sFlow datagrams to up to six sFlow receivers. For example, it could report to a PCM Plus server, to an Intrusion Detection System/Intrusion Prevention System (IDS/IPS), and to a server running a billing application.

Each receiver has its own receiver instance. Many receivers can configure the instance automatically. If you decide to configure instances manually, you can configure three receiver instances (1, 2, and 3) only through the CLI. (See
Appendix A: “ProCurve Wireless Edge Services zl Module Command Line Reference.”) The other receiver instances (4, 5, and 6), you can configure through the Web browser interface.

When you specify the receiver manually, you must configure a variety of settings that the sFlow receiver would otherwise configure itself. These settings include not only the receiver’s IP address and port, but also how the module’s sFlow agent packages the samples.

Follow these steps:

1. Select **Special Features > sFlow** and select the **Receiver** tab.

![Figure 13-2. Special Features > sFlow > Receiver Screen](image)

2. The three receiver instances available for configuration through the Web browser interface are listed by index number (4, 5, and 6). Highlight one of the instances.

3. Click the **Edit** button. The **Receiver Configuration** screen is displayed.
sFlow Agent
Configuring sFlow Using the Web Browser Interface

4. In the **Owner** field, enter a string to identify the sFlow receiver.

5. In the **Time Out** field, specify a value in seconds from 1 to 999999999 (roughly 31 years).
   The timeout reserves this receiver instance for the specified receiver for the set amount of time. Generally, when you configure an sFlow receiver instance manually, you should set the timeout very high (to days or weeks). All settings in the instance are erased when the timeout expires, and you do not want to reconfigure the instance frequently.
   Always set a timeout. If you attempt set the timeout field to 0, your settings are immediately lost.

6. In the **Maximum Datagram Size** field, enter the maximum size of an sFlow datagram in bytes.
   The valid range is from 800 to 1400 bytes, and the default is 1400. The primary reason to lower the size would be that devices between the Wireless Edge Services zl Module have low MTUs, but you do not want them to fragment the datagram.

7. In the **Receiver Address** field, enter the sFlow receiver’s IP address.

8. In the **Receiver Port** field, accept the default port (6343) or enter the UDP port used by this receiver.
   The valid range is from 1 to 65535.
9. From the **802.11 Map** drop-down menu, choose how the module's sFlow agent creates the sample.

   The default setting is **Unchanged**; the module creates the sample as specified by the 802.11 extensions to sFlow. For example, it includes the 802.11 header.

   If your sFlow receiver does not support the 802.11 extension, select **Convert to Ethernet** from the drop-down menu. The module's sFlow agent then packages 802.11 samples to appear as Ethernet samples.

   Note that some receivers, such as PCM Plus, automatically set this option to match their capabilities.

10. Click the **OK** button.

    The value in the **Time Out** field begins to decrement immediately. When the timeout reaches zero, the Wireless Edge Services zl Module erases the **Owner** and **Receiver Address** fields and returns all other fields to their default settings. Set the **Time Out** value high enough that the module can implement sFlow without frequent reconfiguration.

### Manually Activating Flow Sampling

The Wireless Edge Services zl Module's sFlow agent creates six separate sampling instances for each of its adopted RP radios. By default, however, flow sampling is disabled on all instances.

To view the configuration for flow sampling, select **Special Features** > **sFlow** and select the **Flow Sampling** tab.

The screen lists every radio adopted by this module. The **Data Source** column lists each radio's index number and name. As you can see in Figure 13-4, each radio is listed three times: once for each of the three flow sampling sFlow instances that are available for configuration through the Web browser interface. At factory defaults, the sampling instances have not been mapped to receiver instances and the sampling rate is 0—in other words, flow sampling is disabled.
The Wireless Edge Services zl Module’s sFlow agent begins sampling a flow when either of two conditions are met:

- An sFlow receiver contacts the module’s sFlow agent and claims an open flow sampling instance (the Receiver Instance column displays 0). In this case, the receiver configures the sampling rate.
- You map the flow sampling sFlow instance to a manually configured receiver instance. In this case, you set the sampling rate.

Follow these steps to enable flow sampling:

1. Select Special Features > sFlow and select the Flow Sampling tab.
2. Select one of the sFlow instances on the radio for which you want to sample the traffic.
3. Click the Edit button. The Flow Sampling Configuration screen is displayed.

This screen displays the radio in question in the Data Source field. The sFlow Instance field indicates which of the six instances for this radio you are configuring. (You cannot alter the number for the sFlow instance. To configure a different instance number, return to the main screen and select that instance instead.)
Configuring sFlow Using the Web Browser Interface

4. From the **Receiver Instance** drop-down menu, choose the receiver index number associated with the sFlow receiver to which the module should send the samples.

To easily track which settings apply to a specific sFlow collector, match the sFlow instance number to the receiver instance number. However, matching the numbers is not mandatory. Although you can choose one and only receiver for each flow, you can map multiple flows, even on the same radio, to the same receiver. For example, you could map different sFlow instances to the same receiver, but choose a different sampling rate for the flows.

5. Enter a value between 50 and 65535 in the **Packet Sampling Rate** field.

The value determines how often the radio sends the sFlow agent a packet to be sampled. In other words, the radio sends every “nth” packet, and “n” is the value entered in the **Packet Sampling Rate** field. For example, if you enter 100, the radio sends one percent of the packets to be sampled.

The accuracy of a sample increases as the absolute number of samples increases. One general guideline is to set the rate so that the radio sends about one sample per second. To determine the necessary rate, consider roughly how much traffic the radio typically handles. For example, if the radio handles about 1000 packets a second, you can set the rate to 1000. On the other hand, if the radio, on average, handles only 100 packets a second, it must sample traffic more frequently to achieve the same accuracy; set the rate to 100.
Of course, the activity on a radio changes over time, so there are no absolute rules for determining the best sampling rate.

6. Optionally, alter the value in the **Maximum Header Size** field to set the amount of data (in bytes) included in a sample.

The module samples the specified number of bytes. For example, if you set the **Maximum Header Size** to 100, the module places the first 100 bytes of every sampled frame in a datagram. The value should match the size of the frame and packet header so that the entire header is forwarded. The valid range is from 100 to 128 bytes, and the default is 128.

7. Click the **OK** button.

8. Click the **Save** link to copy the configuration to the startup-config.

---

**Manually Activating Counter Polling**

In addition to sampling specific packets, an sFlow agent can gather statistics about overall traffic flow, including:

- the number of inbound packets
- the number of outbound packets
- the number of retransmission attempts
- the number of transmission failures
- the number of packet errors

The agent periodically polls its data sources for these statistics; for the Wireless Edge Services zl Module, the data sources are its RP radios.

The module maintains six separate counter polling (sFlow) instances for each radio. You can view the three configurable from the Web browser interface in the **Special Features > sFlow > Counter Polling** screen.
Configuring sFlow Using the Web Browser Interface

The separate instances allow the agent to report counters to up to six sFlow receivers. By default, counter polling is disabled: the instances are not mapped to receivers and the polling interval is set to 0.

The sFlow agent begins polling radios when either of the following occurs:

- An sFlow receiver contacts the module’s sFlow agent and claims an available counter polling sFlow instance. (An instance is available if the receiver instance is set to 0.) The receiver controls the configuration and sets the polling interval.
- You manually set a polling interval greater than 0 in a counter polling sFlow instance. You also associate the polling sFlow instance with a manually configured sFlow receiver instance.

To manually activate counter polling on a radio, follow these steps:

1. Select **Special Features > sFlow** and select the **Counter Polling** tab.
2. Select one of the instances on the radio that you want to poll.
sFlow Agent
Configuring sFlow Using the Web Browser Interface

3. Click the **Edit** button. The **Counter Polling Configuration** screen is displayed.

   For the **Data Source**, the screen displays the index and name of the radio that the module’s agent polls. The **sFlow Instance** shows which of the six instances you are currently configuring.

   ![Counter Polling Configuration Screen](image)

   **Figure 13-7. Counter Polling Configuration**

4. Select 4, 5, or 6 from the **Receiver Instance** drop-down menu.

   The Wireless Edge Services zl Module’s sFlow agent sends the counters for this radio to the sFlow collector associated with the selected instance.

   You can map this sFlow instance to any receiver instance, even if that receiver is already mapped to another instance on this radio.

5. Enter a value between 20 and 65535 in the **Interval** field. This is the maximum length, in seconds, between polls on this radio.

   A lower value mandates more frequent polling. As always, balance the greater accuracy offered by frequent polling with the extra overhead.

6. Click the **OK** button.

7. Click the **Save** link to copy the configuration to the startup-config.
ProCurve Wireless Services zl Module
Command Line Reference

Contents

Overview ................................................................. A-7
Manager Commands .................................................. A-8
  acknowledge ......................................................... A-9
  archive .............................................................. A-10
  cd .................................................................... A-11
  change master passwd ........................................... A-11
  clear ............................................................... A-12
  configure .......................................................... A-13
  copy ............................................................... A-13
  debug .............................................................. A-14
  diff ................................................................. A-18
  dir ................................................................. A-19
  edit ................................................................. A-20
  erase .............................................................. A-21
  exit ................................................................. A-22
  help ........................................................-------- A-22
  halt ................................................................. A-23
  logout ............................................................. A-23
  mkdir .............................................................. A-24
  more ............................................................... A-24
  no ................................................................. A-25
  page ............................................................... A-29
  ping ............................................................... A-29
  pwd ............................................................... A-30
  redundancy-group-cli-config ................................. A-31
  reload ........................................................... A-31
# Contents

- `rename` .................................................. A-32
- `rmdir` .................................................. A-33
- `service` ................................................ A-33
- `show` .................................................... A-34
- `support` ................................................. A-44
- `telnet` .................................................... A-49
- `terminal` ............................................... A-50
- `upgrade` ............................................... A-51
- `upgrade-abort` ......................................... A-51
- `write` ................................................... A-52

## GlobalCommands ......................................... A-53

- `aaa` ................................................. A-54
- `access-list` .......................................... A-56
- `boot` .................................................. A-56
- `cls` .................................................... A-57
- `country-code` ........................................ A-57
- `crypto` ............................................... A-60
- `end` .................................................... A-64
- `exit` .................................................... A-64
- `fallback` ............................................. A-65
- `help` ................................................... A-66
- `hostname` ............................................ A-66
- `interface` ............................................ A-67
- `ip (global)` .......................................... A-68
- `licenses` ............................................. A-71
- `logging` .............................................. A-72
- `logout` ............................................... A-74
- `mac` .................................................... A-74
- `no` ...................................................... A-75
- `ntp` .................................................... A-76
- `password-encryption` ................................. A-78
- `proxyarp` ............................................ A-78
- `radius-server` ......................................... A-79
- `redundancy` .......................................... A-82
- `service` .............................................. A-84
# ProCurve Wireless Services zl Module Command Line Reference

## Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>A-84</td>
</tr>
<tr>
<td>show</td>
<td>A-86</td>
</tr>
<tr>
<td>snmp-server</td>
<td>A-96</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>A-100</td>
</tr>
<tr>
<td>time</td>
<td>A-100</td>
</tr>
<tr>
<td>timezone</td>
<td>A-101</td>
</tr>
<tr>
<td>upd-server</td>
<td>A-102</td>
</tr>
<tr>
<td>username</td>
<td>A-103</td>
</tr>
<tr>
<td>wireless</td>
<td>A-104</td>
</tr>
<tr>
<td>wlan-acl</td>
<td>A-104</td>
</tr>
</tbody>
</table>

### Interface Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>description (interface)</td>
<td>A-105</td>
</tr>
<tr>
<td>ip (interface)</td>
<td>A-106</td>
</tr>
<tr>
<td>management</td>
<td>A-107</td>
</tr>
<tr>
<td>mtu</td>
<td>A-107</td>
</tr>
</tbody>
</table>

### Wireless Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt-unconf-radio</td>
<td>A-108</td>
</tr>
<tr>
<td>adoption-pref-id</td>
<td>A-109</td>
</tr>
<tr>
<td>advanced-config</td>
<td>A-110</td>
</tr>
<tr>
<td>ap-detection</td>
<td>A-110</td>
</tr>
<tr>
<td>dot11-shared-key-auth</td>
<td>A-112</td>
</tr>
<tr>
<td>ids</td>
<td>A-112</td>
</tr>
<tr>
<td>mac-auth-local</td>
<td>A-113</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>A-114</td>
</tr>
<tr>
<td>radio</td>
<td>A-115</td>
</tr>
<tr>
<td>self-heal</td>
<td>A-119</td>
</tr>
<tr>
<td>wlan</td>
<td>A-120</td>
</tr>
<tr>
<td>wlan-prioritization</td>
<td>A-127</td>
</tr>
</tbody>
</table>
ProCurve Wireless Services zl Module Command Line Reference

Contents

Show Commands ..................................................... A-128
Show Commands (All Contexts) ................................. A-130
  show access-list .............................................. A-130
  show aclstats ................................................ A-130
  show alarm-log .............................................. A-131
  show commands .............................................. A-132
  show crypto .................................................. A-133
  show debug .................................................. A-134
  show dhcp .................................................... A-135
  show file ..................................................... A-135
  show flash ................................................... A-136
  show ftp ...................................................... A-137
  show history ................................................ A-137
  show hostname .............................................. A-138
  show interfaces ............................................ A-138
  show ip ...................................................... A-139
  show layer3-mobility ...................................... A-141
  show ldap ..................................................... A-142
  Manager ...................................................... A-142
  show licenses .............................................. A-143
  show logging ............................................... A-143
  show mac ..................................................... A-144
  show management ......................................... A-144
  show ntp ..................................................... A-145
  show password-encryption ............................... A-146
  show privilege ............................................. A-146
  show proxy-arpdb .......................................... A-147
  show radius ................................................ A-147
  show redundancy-group ................................. A-148
  show redundancy-history ............................. A-149
  show redundancy-members .......................... A-150
  show running-config ................................. A-151
  show securitymgr ....................................... A-153
  show sflow ................................................ A-153
  show snmp ................................................ A-154
show snmp-server ............................................. A-156
show snmp .................................................. A-156
show startup-config ...................................... A-157
show terminal ............................................. A-158
show time ................................................... A-158
show timezone .......................................... A-159
show upd-server .......................................... A-159
show upgrade-status .................................... A-160
show version ............................................... A-161
show users ................................................. A-162
show vlans .................................................. A-163
Show Commands (Wireless) .............................. A-164
  show wireless ap-detection-config .................. A-164
  show wireless approved-aps .......................... A-164
  show wireless channel-power ....................... A-165
  show wireless config ................................ A-166
  show wireless country-code-list ................... A-167
  show wireless ids ..................................... A-168
  show wireless mac-auth-local ...................... A-168
  show wireless multicast-packet-limit ............. A-169
  show wireless phrase-to-key ....................... A-170
  show wireless qos-mapping ......................... A-170
  show wireless radio ................................ A-171
  show wireless radio-status ......................... A-172
  show wireless regulatory ............................ A-173
  show wireless rp ....................................... A-176
  show wireless rp-images .............................. A-177
  show wireless rp-unadopted ......................... A-178
  show wireless self-heal-config .................... A-178
  show wireless station ............................... A-179
  show wireless unapproved-aps ...................... A-180
  show wireless web-auth-config .................... A-181
  show wireless wireless-module-statistics ....... A-182
  show wireless wlan .................................... A-183
Contents

Support Commands ................................................. A-185

Support Commands (All Contexts) ............................... A-187
  support clear .................................................. A-187
  support copy .................................................. A-187
  support diag .................................................. A-188
  support diag-shell ............................................ A-190
  support encrypt ............................................... A-190
  support pm ................................................... A-191
  support prompt ............................................... A-191
  support save-cli ............................................. A-192
  support set .................................................. A-192
  support show ................................................ A-193

Support Commands (Wireless) .................................... A-196
  support wireless dump-core ................................. A-196
  support wireless dump-state ............................... A-196
  support wireless rate-scale ............................... A-197
  support wireless request-rp-log ......................... A-197
Overview

This chapter describes the commands provided by the CLI.

The CLI commands can be broken down into their respective context groups.

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>Commands run from the Manager Context.</td>
<td>A-8</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>Commands run from the Global Context.</td>
<td>A-53</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>Commands run from the Interface Context.</td>
<td>A-105</td>
</tr>
<tr>
<td>Wireless Configuration</td>
<td>Commands run from the Wireless Context.</td>
<td>A-108</td>
</tr>
<tr>
<td>Show Commands</td>
<td>Show commands from all contexts and the Wireless Context.</td>
<td>A-128</td>
</tr>
<tr>
<td>Support Commands</td>
<td>Support commands from all contexts and the Wireless Context.</td>
<td>A-185</td>
</tr>
</tbody>
</table>


Manager Commands

These commands are used to configure the manager commands on the radio port.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>acknowledge alarm-log (all</td>
<td>Acknowledges alarms.</td>
<td>A-9</td>
</tr>
<tr>
<td>&lt;1-65535&gt;) )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>archive tar (create</td>
<td>Creates, lists, or extracts a tar file.</td>
<td>A-10</td>
</tr>
<tr>
<td>table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xtract)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cd (DIR</td>
<td>) Changes directory.</td>
<td>A-11</td>
</tr>
<tr>
<td>clear (alarm-log</td>
<td>Clears cache and reporting logs.</td>
<td>A-12</td>
</tr>
<tr>
<td>arp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wireless-statistics)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>configure (terminal) Enters configure context.</td>
<td>A-13</td>
<td></td>
</tr>
<tr>
<td>copy FILE</td>
<td>Copies from one file to another.</td>
<td>A-13</td>
</tr>
<tr>
<td>URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] debug (Negate) Provides debugging functions.</td>
<td>A-14</td>
<td></td>
</tr>
<tr>
<td>diff (FILE</td>
<td>URL) (FILE</td>
<td>URL) Displays differences between two files.</td>
</tr>
<tr>
<td>dir (all</td>
<td>Displays list of available files in the system.</td>
<td>A-19</td>
</tr>
<tr>
<td>recursive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>) (DIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>all-filesystems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>edit FILE Edits an existing file or creates a new text file.</td>
<td>A-20</td>
<td></td>
</tr>
<tr>
<td>erase FILES Deletes specified file from the system.</td>
<td>A-21</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Ends current mode.</td>
<td>A-64</td>
</tr>
<tr>
<td>halt</td>
<td>Halts the wireless module.</td>
<td>A-23</td>
</tr>
<tr>
<td>help</td>
<td>Describes the interactive help system.</td>
<td>A-66</td>
</tr>
<tr>
<td>logout</td>
<td>Terminates the CLI session.</td>
<td>A-23</td>
</tr>
<tr>
<td>mkdir DIR</td>
<td>Creates a directory.</td>
<td>A-24</td>
</tr>
<tr>
<td>more FILE Displays the contents of a file.</td>
<td>A-24</td>
<td></td>
</tr>
<tr>
<td>[no] page (Negate) Pauses output to the screen.</td>
<td>A-29</td>
<td></td>
</tr>
<tr>
<td>ping WORD Sends ICMP echo request packets to another node on the network</td>
<td>A-29</td>
<td></td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current directory.</td>
<td>A-30</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>redundancy-group-cli-config</td>
<td>Enables redundancy group config context.</td>
<td>A-31</td>
</tr>
<tr>
<td>reload</td>
<td>Performs a cold restart.</td>
<td>A-31</td>
</tr>
<tr>
<td>rename FILENAME NEWFILENAME</td>
<td>Renames a file.</td>
<td>A-32</td>
</tr>
<tr>
<td>rmdir DIR</td>
<td>Deletes a directory.</td>
<td>A-33</td>
</tr>
<tr>
<td>service</td>
<td>Enables service commands.</td>
<td>A-33</td>
</tr>
<tr>
<td>show</td>
<td>Shows running system information.</td>
<td>A-86</td>
</tr>
<tr>
<td>support</td>
<td>Enables support functions.</td>
<td>A-44</td>
</tr>
<tr>
<td>telnet WORD</td>
<td>WORD PORT</td>
<td>Opens a telnet connection.</td>
</tr>
<tr>
<td>terminal length</td>
<td>width</td>
<td>Sets width and length parameters on a screen.</td>
</tr>
<tr>
<td>upgrade URL</td>
<td>Upgrades the software image.</td>
<td>A-51</td>
</tr>
<tr>
<td>upgrade-abort</td>
<td>Aborts an ongoing upgrade.</td>
<td>A-51</td>
</tr>
<tr>
<td>write (memory</td>
<td>terminal )</td>
<td>Writes running configuration to memory or terminal.</td>
</tr>
</tbody>
</table>

**acknowledge**

This command acknowledges the presence of a specified alarm.

**Syntax**

```
acknowledge alarm-log (all | <1-65535>)
```

- **alarm-log** - Acknowledge the alarm logs.
  - **all** - Acknowledge all alarms.
  - **<1-65535>** - Acknowledge specific alarm ID

**Default Setting**

N/A

**Command Mode**

Manager
Example

HPswitch#acknowledge alarm-log 65535
HPswitch#

archive

This command creates, lists, or extracts a tar file.

Syntax

archive tar /[create | table | xtract]

• create - Create a tar file.
  – FILE - File or dir to archive [archive tar /create (FILE|URL) .FILE]
  – URL - Tar file URL URLs: tftp:///path/file ftp://:@/path/file http:///path/file sftp://:@/path/file

• table - List files from a tar file.
  – FILE - Tar filename Files: flash:/path/file [archive tar /table (FILE|URL)]
  – URL - Tar file URL URLs: tftp:///path/file ftp://:@/path/file http:///path/file sftp://:@/path/file [archive tar /table (FILE|URL)]

• xtract - Extract files from a tar file into a directory.
  – FILE - Tar filename Files: flash:/path/file.
  – DIR - Dir to extract files into [archive tar /xtract (FILE|URL) DIR]
  – DIR - Dir to extract files into [archive tar /xtract (FILE|URL) DIR]

Default Setting

N/A

Command Mode

Manager

Example

HPswitch#archive tar create flash:/path/file
HPswitch#
cd

This command changes the current directory.

Syntax

```
cd (DIR | )
```

- DIR - Change current directory to DIR.

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#cd
HPswitch#
HPswitch#cd TESTDIR
```

change master passwd

This command changes the password of the logged-in user.

Syntax

```
change-master-psswd (PASSWD)
```

- change-master-passwd

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#change-master-psswd
HPswitch#
```

clear

This command resets specified cache and reporting logs.

Syntax

clear (alarm-log | arp | crypto | ip | layer3-mobility | logging | wireless-statistics )

- **alarm-log** (<1-65535> | acknowledged | all | new) - Clear alarm log.
  - <1-65535> - Clear specific alarm id.
  - acknowledged - Clear acknowledged alarms.
  - all - Clear all alarms.
  - new - Clear new alarms.

- **arp** - Clear arp cache.

- **crypto** (ipsec | isakmp) - Clear encryption subsystem.
  - ipsec - Flush the IPSec SA
    + sa - Clear all IPSec SAs.
    + A.B.C.D - Clear all IPSec SAs for a given peer.
  - isakmp - Flush the ISAKMP database.
    + sa - Clear all IKE SAs.
    + A.B.C.D - Clear all IKE SAs for a given peer.

- **ip** (dhcp) - Internet protocol
  - dhcp - DHCP server configuration.
    + binding - DHCP address bindings.
    + * - Clear all bindings.
    + A.B.C.D - Clear a specific binding.

- **layer3-mobility** (event-log | peer-statistics | station) - Clear mobility attributes.
  - event-log - Event log.
    + peer - Peer event-logs.
    + station - Station event-logs.
  - peer-statistics - Clear mobility peer statistics.
    + A.B.C.D - IP address of peer.
  - station - Clear station.
    + AA-BB-CC-DD-EE-FF - MAC address of the station.
    + all - All stations (home and foreign.
    + foreign-database - Stations present in the foreign station database.
    + home-database - Stations present in the home station database.

- **logging** - Modify message logging facilities.

- **wireless-statistics** - Clear all wireless statistics.
Default Setting

Command Mode
Manager

Example

HPswitch#clear arp
HPswitch#
HPswitch#clear logging
HPswitch#
HPswitch#clear layer3-mobility station all

**configure**

This command enters the configure context.

**Syntax**

```
configure (terminal|)
```

- **terminal** - Configure from the terminal (optional).

**Default Setting**

N/A

**Command Mode**
Manager

**Example**

```
HPswitch#configure terminal
ProCurve (wireless-services-B)(config)#
```

**copy**

This command copies from one file to another.

**Syntax**

```
copy FILE | URL
```

- **FILE** - File from which to copy.
Manager Commands

- Files:
  flash: /path/file
  nvram: startup-pconfig
  system: running-config
  Filenames are case sensitive and limited to 45 chars.

- **URL** - URL from which to copy.
  - URLs:
    tftp://<hostname or IP> /path/file
    ftp://<user>:<passwd>@<hostname or IP> /path/file
    Filenames are case sensitive and limited to 45 chars.

Default Setting

| N/A |

Command Mode

Manager

Example

```
HPswitch# copy ftp://ftp:ftp@172.20.15.5/test.conf
switch:my.conf
ProCurve  (wireless-services-B)#
```

debug

This command provides debugging functions. The no command negates the trace.

Syntax

```
debug {all | cc | ccstats | certmgr | dhcpsvr | imi | ip | logging | mgmt | mobility | nsm | pktdrvr | pm | radius | redundancy | securitymgr | sflow | upd-server}
```

- **all** Enable all debugging
- **cc** Cell controller (wireless) debugging messages.
  - **all** All modules
  - **alt** Address lookup logs
  - **ap-detect** Rogue AP detection logs
  - **capwap** CAPWAP logs
  - **cluster** Cluster-related logs
  - **config** Configuration change logs
  - **dot 11** Datapath logs
  - **eap** 802.1x/Eap logs
  - **ids** Intrusion detection logs
  - **kerberos** Kerberos logs
Manager Commands

- **13-mob**  Layer3 mobility logs
- **media**  Encapsulation media logs
- **radio**  Radio logs
- **radio-port**  Radio-port logs
- **radius**  Radius client logs
- **self-heal**  Self-healing logs
- **snmp**  SNMP logs
- **station**  Station logs
- **system**  System call logs
- **wips**  WIPS sensor logs
- **wisp**  WISP logs

- **ccstats**  Cell controller (Wireless) debugging messages
  - **word**  CCStats module to be debugged

- **certmgr**  Certificate manager debugging messages
  - **all**  trace error and info messages from Certificate Manager
  - **error**  trace error messages from Certificate Manager
  - **info**  trace informational messages from Certificate Manager

- **dhepsvr**  DHCP Conf Server Debugging Messages
  - **all**  trace error and info messages from DHCP Conf Server
  - **error**  trace error messages from DHCP Conf Server
  - **info**  trace informational messages from DHCP Conf Server

- **imi**  Integrated Management Interface
  - **all**  All debugging
  - **cliclient**  CLI responses from protocol modules to IMI server
  - **cliserver**  CLI commands from IMI server to protocol module
  - **errors**  Errors
  - **init**  Initialization process
  - **ntp**  NTP debug messages

- **ip**  Internet Protocol (IP)
  - **https**  Secure HTTP (HTTPS) server

- **logging**  Modify message logging facilities
  - **all**  All debugging
  - **errors**  Errors
  - **monitor**  Logging to monitors
  - **subagent**  Subagent

- **mgmt**  Mgmt daemon
  - **all**  All debugging
  - **cgi**  CGI
  - **err**  Errors
  - **sys**  System

- **mobility**  L3 Mobility
  - **all**  All debugging (except "forwarding")
Manager Commands

- cc   ccservers events
- error Error
- forwarding Dataplane forwarding
  AA-BB-CC-DD-EE-FF  MAC address of the Station
- mu   MU events and state changes
- packet Control Packets
- peer Peer establishment
- system System events

- nsm Network Service Module (NSM)
  - all Enable all debugging
  - events NSM events
  - kernel NSM kernel
  - packet NSM packets
    + detail Detailed information display
    + recv NSM receive packets
    - detail Detailed information display
    ++ send NSM send packets
      +++ detail Detailed information display

- pktdrvr PktDrv (kernel wireless) debugging messages
  - all trace all messages from pktdrvr, including debugging ones
    (Note: setting this level will make the switch interfaces very slow. This is only for testing in an environment with extremely low, controlled traffic)
  - err trace error messages from pktdrvr (default if no parameter is specified)
  - info trace error, warning, and informational messages from pktdrvr
  - ratelimit log message ratelimiting
  - skippacketfilter dont call the packet filtering API when rx/tx frames
  - warn trace error and warning messages from pktdrvr

- pm Process Monitor
  - all All debugging
  - errors Errors
  - heartbeats Heartbeats processing
  - init Initialization process
  - proc Process state machine
  - shutdown Shutdown process
  - subagent Subagent
  - sys System state machine

- radius RADIUS server debugging messages
  - all trace all messages from radius server
Manager Commands

- **err**  trace error messages from local radius server
- **info**  trace error, warning and informational messages from radius server
- **warn**  trace error and warning messages from radius server

- **redundancy**  Redundancy Protocol debugging messages
  - **all**  Debugging all
  - **ccmsg**  Msg exchange with CC
  - **config**  Configuration processing
  - **errors**  Errors
  - **general**  General
  - **heartbeats**  Heartbeats processing
  - **init**  Redundancy initialization
  - **packets**  Packet processing
  - **proc**  Process flow
  - **shutdown**  Shutdown process
  - **states**  Redundancy state machine
  - **subagent**  Subagent
  - **timer**  Timer handling
  - **warnings**  Warnings

- **securitymgr**  Security Manager Debugging Messages
  - **all**  Trace all messages from SecurityManager
  - **debug**  Trace general debug messages from SecurityManager
  - **error**  Trace general error messages from SecurityManager
  - **ikeerror**  Trace debug messages for Ike
  - **ipsec**  Trace Policy Manager messages
  - **+ kernel**  Trace Kernellevel Policy Manager messages
    - **- WORD**  Kernellevel debug string
    - **++ user**  Trace Userlevel Policy Manager messages
      - **+++ WORD**  Userlevel debug string
  - **pmdebug**  Trace debug messages for PolicyManager
  - **pmerror**  Trace error messages for PolicyManager

- **sflow**  sFlow Debugging Messages
  - **error**  trace error messages from sFlow sampling agent
  - **info**  trace informational messages from sFlow sampling agent

- **updserver**  Update server
  - **all**  All updserver traces
  - **autoinstall**  Autoinstall
  - **cli**  CLI
  - **espd**  ESPd
  - **shim**  Shim
  - **subagent**  Subagent

- **wirelessstatistics**  wireless statistics
Manager Commands

- `all` trace all messages from wirelessstatistics
- `error` trace error messages from wirelessstatistics
- `info` trace info messages from wirelessstatistics

Default Setting
N/A

Command Mode
Manager

Example

```
HPswitch# debug mgmt cgi
HPswitch#
HPswitch# no debug mgmt sys
HPswitch#
```

diff

This command displays differences between two files.

Syntax

diff (FILE | URL) (FILE | URL)

- `FILE` - Display the differences between FILE.
- `URL` - Display the differences between URL.

Default Setting
N/A

Command Mode
Manager
Example

HPswitch# `diff TESTFILE TESTFILE2`
--- TESTFILE
+++ TESTFILE2
@@ -1 +1 @@
-testing edit, view, and delete file.
+testing edit, erase, and contents of file.
HPswitch#

dir

This command displays list of available files on the filesystem.

Syntax

```
    dir (all | recursive |) (DIR | all-filesystems |)
```

- **all** - Display all available files.
- **recursive** - Display recursive files.
- **DIR** - Display list of all available files in the file path.
- **all-filesystems** - Display list of all available filesystems.

Default Setting

N/A

Command Mode

Manager

Example One

```
HPswitch# dir all

Directory of flash:/
  drwx 1024 Wed Dec 7 17:06:32 2005 hotspot
  drwx 1024 Thu Dec 8 09:31:07 2005 crashinfo
  drwx 80 Mon Feb 13 09:35:10 2006 log

Directory of nvram:/
  -rw- 625 Thu Dec 2 08:53:36 2006 startup-config

Directory of system:/
  -rw- running-config

HPswitch#
```
Example Two

HPswitch# dir /recursive
-------------------------------------------------------------------
Directory of flash:/
  drwx 1024 Wed Dec 7 17:06:32 2005 hotspot
drwx 1024 Thu Dec 8 09:31:07 2005 crashinfo
drwx 80 Mon Feb 13 09:35:10 2006 log
Directory of flash:/hotspot
dwx 1024 Wed Feb 1 17:19:19 2006 lib
dwx 1024 Wed Feb 1 17:19:19 2006 cgi-bin
Directory of flash:/hotspot/lib
  -rwx 58476 Tue Jan 31 13:12:09 2006 libpthread.so.0
  -rwx 124572 Tue Jan 31 13:12:09 2006 libc.so.6
  -rwx 90776 Tue Jan 31 13:12:09 2006 ld-linux.so.2
  -rwx 28400 Tue Jan 31 13:12:09 2006 librt.so.1
  -rwx 138088 Tue Jan 31 13:12:09 2006 libm.so.6
Directory of flash:/hotspot/cgi-bin
  -rwx 18248 Tue Jan 31 13:12:17 2006 hslogin.cgi
  -rwx 16296 Tue Jan 31 13:12:18 2006 hslogout.cgi
Directory of flash:/crashinfo
  No files in dir flash:/crashinfo
Directory of flash:/log
  -rw- 0 Mon Feb 13 09:35:10 2006 messages.log
  -rw- 11404 Mon Feb 13 09:35:18 2006 startup.log

edit
This command edits an existing file or creates a new text file.

Syntax
  edit FILE
  •  FILE -Name of file to edit or create.

Default Setting
  N/A

Command Mode
  Manager
Example

HPswitch# edit TESTFILE

GNU nano 1.2.4 File: TESTFILE

testing edit, erase, and view file

[ New File ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Txt ^T To Spell
[PRESS CNTRL X]

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?Y
Y Yes
N No ^C Cancel

File Name to Write: TESTFILE [PRESS ENTER]
^G Get Help ^P Prepend
M-A Append ^C Cancel

testing edit, erase, and view file

[ Wrote 1 line ]

HPswitch#

erase

This command deletes aspecified file from the system.

Syntax

erase [/force | /recursive | FILE]

- /force - Force deletion without prompt
- /recursive - Recursive delete
- FILE Filename(s) to be deleted. Files: flash/path/file startupconfig
  (resets configuration to factory default) * is accepted as a wildcard

Default Setting
N/A

Command Mode
Manager
Example

```
HPswitch# erase FILE
HPswitch
```

exit

This command ends current mode and reverts to previous mode.

Syntax

```
exit
```

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch# exit
HPswitch
```

help

This command provides a description of the interactive help system.

Syntax

```
help
```

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch# help
HPswitch
```
halt
This command halts the wireless module.

Syntax
halt

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#hal
Wireless module will be halted, do you want to continue? y
ProCurve (config)#

logout
This command exits from the CLI.

Syntax
logout

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#logout
Do you want to log out [y/n]? y
ProCurve(config)#
mkdir

This command creates a directory.

Syntax

```
mkdir DIR
```

• `DIR` - Directory name.

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#mkdir TESTDIR
HPswitch#
```

more

This command displays the contents of a file.

Syntax

```
more FILE
```

• `FILE` - File name.

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#more TESTFILE
testing edit, erase, and view file
HPswitch#
```
NO

This command negates a command or sets its defaults.

**Syntax**

```plaintext
no (clustercli | debug | page | service | support | upgrade)
```

- **clustercli**  Cluster context
  - `enable`  Disable cluster context
- **debug**  Debugging functions
  - `all`  Enable all debugging
  - `cc`  Cellcontroller (wireless) debugging messages
    - `+ WORD`  Name of module for which debugging is to be turned off
  - `certmgr`  Certificate Manager Debugging Messages
    - `+ all`  trace error and informational messages from Certificate Manager
    - `+ error`  trace error messages from Certificate Manager
    - `+ info`  trace informational messages from Certificate Manager
  - `dhcpsvr`  DHCP Conf Server Debugging Messages
    - `+ all`  trace error messages from DHCP Conf Server
    - `+ error`  trace informational messages from DHCP Conf Server
    - `+ info`  trace error and info messages from DHCP Conf Server
  - `imi`  Integrated Management Interface
    - `+ all`  All debugging
    - `+ cliclient`  CLI responses from protocol modules to IMI server
    - `+ cliserver`  CLI commands from IMI server to protocol module
    - `+ errors`  Errors
    - `+ init`  Initialization process
    - `+ ntp`  NTP debug messages
  - `ip`  Internet Protocol (IP)
    - `+ https`  Secure HTTP (HTTPS) server
  - `logging`  Modify message logging facilities
    - `+ all`  All debugging
    - `+ errors`  Errors
    - `+ monitor`  Logging to monitors
    - `+ subagent`  Subagent
  - `mgmt`  Mgmt daemon
    - `+ all`  All debugging
Manager Commands

- **cgi** CGI
- **err** Errors
- **sys** System

- **mobility** L3 Mobility
  - **+ all** All debugging (except "forwarding")
  - **+ cc** ccserver events
  - **+ error** Error
  - **+ forwarding** Dataplane forwarding
    - **- AA-BB-CC-DD-EE-FF** MAC address of the Station
  - **+ mu** MU events and state changes
  - **+ packet** Control Packets
  - **+ peer** Peer establishment
  - **+ system** System events

- **nsm** Network Service Module (NSM)
  - **+ all** Enable all debugging
  - **+ events** NSM events
  - **+ kernel** NSM kernel
  - **+ packet** NSM packets
    - **- detail** Detailed information display
    - **- recv** NSM receive packets
    - **++ detail** Detailed information display
    - **+ send** NSM send packets
      - **++ detail** Detailed information display
  - **- pktdrvr** Pktdrv (kernel wireless) debugging messages
    - **+ rate limit** log message ratelimiting
    - **+ skippacketfilter** Reenable packet filtering API (ON by default)

- **pm** Process Monitor
  - **+ all** All debugging
  - **+ errors** Errors
  - **+ heartbeats** Heartbeats processing
  - **+ init** Initialization process
  - **+ proc** Process state machine
  - **+ shutdown** Shutdown process
  - **+ subagent** Subagent
  - **+ sys** System state machine

- **radius** RADIUS server debugging messages
A-27

ProCurve Wireless Services 21 Module Command Line Reference
Manager Commands

+ all  Turn off all the debugging for radius
– redundancy  Redundancy Protocol Debugging messages
  + all  Debugging all
  + ccmgr  Msg exchange with CC
  + config  Configuration processing
  + errors  Errors
  + general  General
  + heartbeats  Heartbeats processing
  + init  Redundancy initialization
  + packets  Packet processing
  + proc  Process flow
  + shutdown  Shutdown process
  + states  Redundancy state machine
  + subagent  Subagent
  + timer  Timer handling
  + warnings  Warnings
– securitymgr  Security Manager Debugging Messages
  + all  Trace all messages from SecurityManager
  + debug  Trace general debug messages from SecurityManager
  + error  Trace general error messages from SecurityManager
  + ikeerror  Trace debug messages for Ike
  + ipsec  Trace Policy Manager messages
    - kernel  Trace Kernellevel Policy Manager messages
    - user  Trace Userlevel Policy Manager messages
  + pmdebug  Trace debug messages for PolicyManager
  + pmerror  Trace error messages for PolicyManager
– sflow  sFlow Debugging Messages
  + error  Trace error messages from sFlow sampling agent
  + info  Trace informational messages from sFlow sampling agent
– updserver  Update server
  + all  All updserver traces
  + autoinstall  Autoinstall
  + cli  CLI
  + espd  ESPd
  + shim  Shim
Manager Commands

+ subagent Subagent
  – wirelessstatistics wireless statistics
  + all trace all messages from wirelessstatistics
  + error trace error messages from wirelessstatistics
  + info trace info messages from wirelessstatistics

• page Toggle paging

• service Support Commands
  – radius Disable radius server

• support Support Commands
  – diag Diagnostics
    + enable Disable in service diagnostics
    + period Set to default period
    + watchdog disable the watchdog
  – pm Process Monitor
    + maxsysrestarts Maximum number of times PM will restart the system because of a failed processes
    + sysrestart Disable PM from restarting the system when a processes fails
  – prompt Disable crashinfo prompt
    + crashinfo Disable crashinfo prompt
  – securitymgr Securitymgr parameters
    + enablehttpstats Disable securitymgr HTTP statistics interface
  – set Set service parameters
    + commandhistory Reset size of command history to default (200)
    + reboothistory Reset size of reboot history to default (50)
    + upgradehistory Reset size of upgrade history to default (50)
  – wireless Wireless parameters
    + config Delete all wireless configuration and disable wireless services
    + muhistory Disable mu association history (default)
    + ratescale Disable wireless rate scaling

• upgrade Name of the patch to remove
  – WORD Name of patch to remove

Default Setting

N/A
Command Mode
Manager

Example

```
HPswitch#no debug
HPswitch
```

page
This command enables pausing of output to the screen. The no command disables the pausing of the output.

Syntax
```
page
```

Default Setting
N/A

Command Mode
Manager

Example

```
HPswitch#page
HPswitch#
```

ping
This command sends ICMP echo request packets to another node on the network.

Syntax
```
ping WORD
```

- **WORD** - Hostname or IP address of the host.

Default Setting
N/A

Command Mode
Manager
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. ?? repetition <1-1000> timeout <1-256>
  - **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

```
HPswitch#ping 10.1.0.9
PING 10.1.0.9 (10.1.0.9): 100 data bytes
108 bytes from 10.1.0.9: icmp_seq=0 ttl=64 time=2.1 ms
108 bytes from 10.1.0.9: icmp_seq=1 ttl=64 time=1.2 ms
108 bytes from 10.1.0.9: icmp_seq=2 ttl=64 time=0.7 ms
108 bytes from 10.1.0.9: icmp_seq=3 ttl=64 time=1.5 ms
108 bytes from 10.1.0.9: icmp_seq=4 ttl=64 time=1.1 ms
--- 10.1.0.9 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.3/2.1 ms
HPswitch#
```

**pwd**

This command displays the current directory.

**Syntax**

```
pwd
```

**Default Setting**

N/A

**Command Mode**

Manager
redundancy-group-cli-config

This command enables redundancy group configuration context.

Syntax

redundancy-group-cli-config (enable)

- enable  Enable redundancy group config context

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch# pwd
flash:/
HPswitch#
```

reload

This command halts and performs a warm reboot.

Syntax

reload

Default Setting

N/A

Command Mode

Manager
Example

HPswitch#reload
Wireless module will be rebooted, do you want to continue?
(y/n): y
Do you want to save current configuration? (y/n): y
ProCurve(config)#

rename

This command renames a file.

Syntax

rename FILE

  • FILE - File to be renamed.
    – FILE - New file name.

Default Setting

N/A

Command Mode

Manager

Example

To validate the name change, use the DIR command.

HPswitch#rename TESTFILE3 TESTFILE2
HPswitch#
HPswitch#dir
Directory of flash:/

drwx 1024 Tue Oct 1 00:14:16 2002 hotspot
drwx 1024 Thu Feb 16 15:37:09 2006 crashinfo
drw 80 Fri Feb 17 12:48:10 2006 log
drwx 1024 Fri Feb 17 09:48:19 2006 TESTDIR
-rw- 43 Fri Feb 17 10:19:52 2006 TESTFILE2
-rw- 37 Fri Feb 17 10:20:47 2006 TESTFILE

HPswitch#
rmdir

This command deletes a directory.

**Syntax**

rmdir DIR

- **DIR** - Directory to be deleted.

**Default Setting**

N/A

**Command Mode**

Manager

**Example**

To validate the directory is deleted, use the DIR command.

```
HPswitch#rmdir TESTDIR
HPswitch#dir
Directory of flash:/

   drwx 1024 Tue Oct 1 00:14:16 2002 hotspot
   drwx 1024 Thu Feb 16 15:37:09 2006 crashinfo
   drwx  80 Fri Feb 17 12:48:10 2006 log
   -rw-  43 Fri Feb 17 10:19:52 2006 TESTFILE2
   -rw-  37 Fri Feb 17 10:20:47 2006 TESTFILE
```

service

This command enables service commands.

**Syntax**

service (radius)

- **radius** - Enable radius server
  - **restart** - Restart the radius server with updated configuration

**Default Setting**

N/A
**Command Mode**

Manager

**Example**

```
HPswitch#service radius restart
HPswitch
```

**show**

This command shows running system information.

**Syntax**

```
show (accesslist | aclstats | alarmlog | commands | crypto | debug | dhcp | file | flash | ftp | history | hostname | interfaces | ip | layer3mobility | ldap | licenses | logging | mac | management | ntp | passwordecryption | privilage | proxyarpdb | radius | redundancy-group | redundancyhistory | redundancymembers | runningconfig | securitymgr | sflow | snmp | snmpserver | sntp | startupconfig | terminal | time | timezone | updserver | updatestatus | users | version | vlans | wireless)
```

- **accesslist**  Internet Protocol (IP)
  -  `<199>`  IP standard access list
  -  `<100199>`  IP extended access list
  -  `<13001999>`  IP standard access list (expanded range)
  -  `<20002699>`  IP extended access list (expanded range)
  -  **WORD**  Name of ACL
  -  **radius**  IDM/Radius Assigned
    -  **+ MAC**  Specify the user mac in AA-BB-CC-DD-EE-FF format
    -  **- detail**  Details of all the IDM/Radius assigned attributes
- **aclstats**  Show ACL Statistics information
  -  **IFNAME**  Interface Name
  -  **vlan**  Vlan Interface
    -  `<14094>`  Vlan Id
- **alarmlog**  Display all alarms currently in the system
  -  `<165535>`  Display details for specific alarm id
  -  **acknowledged**  Display acknowledged alarms currently in the system
  -  **all**  Display all alarms currently in the system
  -  **count**  Display count of alarms currently in the system
  -  **new**  Display new alarms currently in the system
  -  **severitytolimit**  Display all alarms having specified or higher severity
    -  **+ critical**  Display all critical alarms
Manager Commands

+ **informational**  Display all informational or higher severity alarms
+ **major**  Display all major or higher severity alarms
+ **normal**  Display all normal or higher severity alarms
+ **warning**  Display all warning or higher severity alarms

- **commands**  Show command lists
- **crypto**  encryption module
  - **ipsec**  Show IPSEC policy
    + **sa**  IPSec Security Association
    + **securityassociation**  securityassociation
      - **lifetime**  lifetime
    + **transformset**  transformset
      - **WORD**  transform set name or all transform sets
  - **isakmp**  Show ISAKMP
    + **policy**  policy
      - **<110000>**  priorityall isakmp policies
    + **sa**  All Crypto ISAKMP Security Association
  - **key**  Authentication key management
    + **mypubkey**  Show public keys associated with the switch
      - **rsa**  Show RSA public keys
  - **map**  Crypto maps
    + **interface**  Crypto maps for an interface.
      - **WORD**  interface name
    + **tag**  Crypto maps with a given tag
      - **WORD**  crypto map name
  - **pki**  Public Key Infrastructure commands
    + **request**  Show certificate request
      - **WORD**  Trustpoint Name
    + **trustpoints**  Show trustpoints configured and configuration
- **debug**  Display debugging setting
- **dhcp**  DHCP Server Configuration
  - **config**  Display DHCP Server configuration
  - **status**  Display whether DHCP Server is running or not
- **file**  Display filesystem information
  - **information**  Display file information
    + **FILE**  Display information on FILE
  - **systems**  List filesystems
Manager Commands

- **flash** Display boot status.
- **ftp** Display FTP Server configuration
- **history** Display the session command history
- **hostname** Display system's network name
- **interfaces** Interface status and configuration
  - **IFNAME** Interface name
  - **dnlink** Dlink Interface
  - **tunnel** Tunnel Interface
    + `<132>` Tunnel Id
  - **uplink** Uplink Interface
  - **vlan** Vlan Interface
    + `<14094>` Vlan Id
- **ip** Internet Protocol (IP)
  - **accessgroup** Display ACLs attached to an interface
    + **IFNAME** Interface name
    + **dnlink** Ethernet Interface Id
    + **uplink** Ethernet Interface
    + **vlan** Vlan Interface
      - `<14094>` Vlan Id
  - **accesslist** List IP access lists
  - **arp** Address Resolution Protocol (ARP)
  - **ddns** DDNS Configuration
    + **binding** DNS Address bindings
  - **dhcp** DHCP Server Configuration
    + **binding** DHCP Address bindings
    + **pool** DHCP Pools
      - **WORD** DHCP pool name
  - **dhcpvendornoptions** DHCP Option 43 parameters received from DHCP server
  - **dns** DNS nameservers
  - **domain** Default domain for DNS
  - **interface** IP interface status and configuration
    + **IFNAME** Interface name
    + **tunnel** Tunnel Interface
      - `<132>` Tunnel Id
    + **vlan** Vlan Interface
      - `<14094>` Vlan Id
  - **nat** Network Address Translation (NAT)
    + **interfaces** NAT Configuration on Interfaces
+ translations  NAT translations
- inside  Inside
  ++ destination  Destination
  ++ source  Source
- outside  Outside
  ++ destination  Destination
  ++ source  Source
- verbose  NAT Translations in realtime
  – route  IP routing table
    + A.B.C.D  Network in the IP routing table to display
    + A.B.C.D/M  IP prefix /, e.g., 35.0.0.0/8
    + detail  IP routing table in detail
  – routing  IP routing status
  – securewebmanagement  Secured web server
  – telnet  Telnet server
  – webmanagement  Web server
• layer3mobility  Display Mobility parameters
   – eventlog  Event Log
     + peer  Peer eventlogs
     + station  Mobileunit eventlogs
  – forwarding  Stations in the Forwarding Plane
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
  – global  Global Mobility parameters
  – peer  Mobility peers
    + A.B.C.D  IP address of Peer
    + detail  Detailed information display
  – station  Stations in the Mobility Database
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
    + detail  Detailed information display
  – statistics  Mobility statistics
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
• ldap  LDAP server
  – configuration  LDAP server configuration parameters
    + primary  primary LDAP server
    + secondary  secondary LDAP server
• licenses  Installed licenses
  – uninstalled  uninstalled licenses
• logging  Show logging configuration and buffer
Manager Commands

• **mac**  Media Access Control
  – **accesslist**  List MAC access lists

• **management**  Display L3 Management Interface name

• **ntp**  Network time protocol
  – **associations**  NTP associations
    + **detail**  Show detail
  – **status**  NTP Status

• **passwordencryption**  password encryption
  – **status**  Display passwordencryption status

• **privilege**  Show current privilege level

• **proxyarpdb**  Display proxyARP entries in ARP database

• **radius**  RADIUS configuration commands
  – **configuration**  radius server configuration parameters
  – **eap**  Eap parameters
    + **configuration**  Eap configuration
  – **group**  Radius group configuration
    + **WORD**  Existing radius group in the local radius database
  – **nas**  client information
    + **A.B.C.D/M**  client ip address / mask
  – **proxy**  proxy information
    + **WORD**  proxy realm name
  – **raduser**  Radius user information
    + **WORD**  Existing User name in the local radius database
  – **trustpoint**  Radius trustpoint configuration
  – **config**  Display configured redundancy group information.

• **redundancygroup**  Display redundancy group parameters
  – **runtime**  Display runtime redundancy group information.

• **redundancyhistory**  Display state transition history of the wireless module.

• **redundancymembers**  Display redundancy group members in detail
  – **A.B.C.D**  IP address of member module
  – **brief**  Display members in brief

• **runningconfig**  Current Operating configuration
  – **includefactory**  Include Factory Defaults

• **securitymgr**  Securitymgr parameters
  – **eventlogs**  Display securitymgr event logs

• **sflow**  Display sFlow parameters
  – **<16>**  Select one of six possible sFlow receiver tables
+ destination Displays information about the collector/managementstation to which the samplingpolling data is sent
+ samplingpolling Displays information about sampling and polling
  - <11000> A single radio index
  - RADIO A list (eg: 1,3,7) or range (eg: 37) of radio indices
    - agent Displays readonly agent information

• snmp Display SNMP engine parameters
  - user snmp user to show
    + manager show manager info
    + operator show operator info
    + snmptrap show trap info

• snmpserver Display SNMP engine parameters
  - traps Display Trap enable flags
    + wirelessstatistics Display wirelessstats rate traps
      - radio Display radio rate traps
      - station Display station rate traps
    - wirelessmodule Display wirelessmodule rate traps
    - wlan Display wlan rate traps

• snntp Display simple NTP configuration
• startupconfig Contents of startup configuration
• terminal Display terminal configuration parameters
• time Display system clock
• timezone Display timezone
• updserver Display update server parameters.
• upgradestatus Display last image upgrade status
  - detail Last image upgrade log
• users Display information about terminal lines
• version Display software & hardware version
  - verbose Display software & hardware details
• vlans VLAN Information
• wireless Wireless configuration commands
  - apdetectionconfig DetectedAP Configuration Parameters
  - approvedaps Approved APs seen by radiodetector scans
  - channelpower List of available channel and power levels for a radio
    + 11a radio is of type 802.11a
      - indoor radio is placed indoor
- **outdoor** radio is placed outdoor

+ **11bg** radio is of type 802.11bg

- **indoor** radio is placed indoor

- **outdoor** radio is placed outdoor

- **config** Wireless Configuration Parameters

- **ids** Intrusion detection parameters

+ **filterlist** Display the list of currently filtered stations

- **macauthlocal** list out the macauthlocal entries

+ **<11000>** macauthlocal entry to display

- **multicastpacketlimit** multicastpacketlimit

- **phrasetokey** display the WEP keys generated by a passphrase

+ **wep128** display WEP128 keys

- **LINE** the passphrase (between 4 and 32 characters)

+ **wep64** display WEP64 keys

- **LINE** the passphrase (between 4 and 32 characters)

- **qosmapping** Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags

+ **wiredtowireless** Mappings used when traffic is switched from wired to the wireless side

+ **wirelesstowired** Mappings used when traffic is switched from wireless to the wired side

- **radio** Radio related commands

+ **beacontable** The RadioToRadio beacon table

+ **config** Radio configuration

- **<11000>** A single radio index

- **default11a** default 11a configuration template

- **default11bg** default 11bg configuration template

+ **monitortable** The RadioToRadio monitoring table

+ **statistics** Radio statistics

- **<11000>** A single radio index <11000>

  ++ **detail** Detailed radio statistics

+ **unadopted** List of unadopted radios

- **radiostatus** Status of all radios that are adopted or in the process of adoption

+ **<11000>** A single radio index

- **regulatory** Regulatory (allowed channel/power) information for a particular country

+ **ae** United Arab Emirates
+ ht  Haiti
+ hu  Hungary
+ id  Indonesia
+ ie  Ireland
+ il  Israel
+ in  India
+ is  Iceland
+ it  Italy
+ jo  Jordan
+ jp  Japan
+ kr  South Korea
+ kw  Kuwait
+ kz  Kazakhstan
+ li  Liechtenstein
+ lk  Sri Lanka
+ lt  Lithuania
+ lu  Luxembourg
+ lv  Latvia
+ ma  Morocco
+ mt  Malta
+ mx  Mexico
+ my  Malaysia
+ nl  Netherlands
+ no  Norway
+ nz  New Zealand
+ om  Oman
+ pe  Peru
+ ph  Philippines
+ pk  Pakistan
+ pl  Poland
+ pt  Portugal
+ qa  Qatar
+ ro  Romania
+ ru  Russia
+ sa  Saudi Arabia
+ se  Sweden
+ sg  Singapore
+ si  Slovenia
+ sk  Slovak Republic
+ th  Thailand
+ tr  Turkey
+ tw  Taiwan
+ ua  Ukraine
+ us  United States
+ uy  Uruguay
+ ve  Venezuela
+ vn  Vietnam
+ za  South Africa

- rp  Status of adopted radioport
  + <148>  The index of the radioport for detailed information
  + AA-BB-CC-DD-EE-FF  The MAC address of a radioport for detailed information

- rpimages  List of radioport images on the wireless module
- rpunadopted  List of unadopted radioport
- selfhealconfig  SelfHealing Configuration Parameters
  + <11000>  A single radio index
  + all  All Configured radios

- station  Details of associated stations
  + <14096>  Index of station
  + AA-BB-CC-DD-EE-FF  MAC address of station
- radio  Show mobileunits associated to this radio
  - <11000>  A single radio index
  + statistics  station rf statistics
    - AA-BB-CC-DD-EE-FF  MAC address of station
      ++ detail  Detailed station statistics
  + wlan  Show mobileunits associated to this wlan
    - WLAN_RANGE  A wlan index <132>

- stationprobehistory  Display station probehistory
- unapprovemsaps  Unapproved APs seen by radioport or station scans
- webauthconfig  Wlan webauth configuration
  + <132>  A wlan index <132>
- wiredwebauth  Wired web authentication
ProCurve Wireless Services zl Module Command Line Reference
Manager Commands

+ clients Wired web authentication clients
+ config Wired web authentication configuration parameters
  – wirelessmodulestatistics wirelessmodule statistics
+ detail Detailed wirelessmodule statistics
  – wlan Wireless LAN related parameters
  + config Wlan configuration
    - <132> A wlan index <132>
    - all All wlans in configuration
    - enabled Only wlans that are currently enabled
  + statistics WLAN statistics
    - <132> A wlan index <132>
  ++ detail Detailed wlan statistics

Default Setting
N/A

Command Mode
Manager

Example

```
HPswitch#show aclstats vlan
HPswitch
```

support

This command enables support functions.

Syntax

```
support {clear | copy | diag | diagshell | encrypt | pm | prompt | rp | savecli | securitymgr | set | show | tethereal | wireless}

• clear Reset functions
  – all Remove all core, dump and panic files
  – clitree Remove clitree.html (created by the savecli command)
  – cores Remove all core files
  – dumps Remove all dump files
  – panics Remove all kernel panic files
  – pm Process Monitor
  + statistics Heartbeat counters and statistics
    - sysrestartcount Number of times that PM restarted the system
```
- **copy**  Copy from one file to another
  - **techsupport**  Copy extensive system information useful to technical support for troubleshooting a problem
    - **URL**  URL to which to copy URLs: tftp:///path/file ftp://@/path/file http:///path/file
- **diag**  Diagnostics
  - **enable**  Enable in service diagnostics
  - **limit**  Diagnostic limit command
    - **buffer**  Buffer usage warning limit
      - **128**  128 byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **128k**  128k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **16k**  16k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **1k**  1k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **256**  256 byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **2k**  2k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **32**  32 byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **32k**  32k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **4k**  4k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **512**  512 byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **64**  64 byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **64k**  64k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
      - **8k**  8k byte buffer limit
        - **<065535>**  buffer usage warning limit 065535
+ **fan**  Fan speed limit
  - `<11>`  Fan number
    + **low**  Low speed limit
      -- `<100015000>`  Limit value from 1000 to 15,000

+ **filesys**  file system freespace limit
  - **etc2**  `/etc2` file system
    + **WORD**  limit as a percentage
  - **flash**  `/flash` file system
    + **WORD**  limit as a percentage
  - **ram**  `/ram` file system
    + **WORD**  limit as a percentage

+ **inodes**  file system inode limit
  - **etc2**  `/etc2` file system
    + **WORD**  limit as a percentage
  - **flash**  `/flash` file system
    + **WORD**  limit as a percentage
  - **ram**  `/ram` file system
    + **WORD**  limit as a percentage

+ **load**  aggregate processor load
  - **1**  during the previous minute
    + **WORD**  percentage load from 0.0 to 100.0
  - **15**  during the previous 15 minutes
    + **WORD**  percentage load from 0.0 to 100.0
  - **5**  during the previous five minutes
    + **WORD**  percentage load from 0.0 to 100.0

+ **maxFDs**  maximum number of file descriptors
  - `<032767>`  032767

+ **pkbuffers**  packet buffer head cache
  - `<065535>`  limit from 065535

+ **procRAM**  percent RAM used by a process
  - **WORD**  limit from 0.0100.0

+ **ram**  percent free RAM
  - **WORD**  limit from 0.0100.0

+ **routecache**  IP route cache usage
  - `<065535>`  limit from 065535
+ temperature  temperature limit
- <18>  temperature sensor number
  ++ critical  critical temperature limit
    -- WORD  0.0  250.0
  ++ high  high temperature limit
    -- WORD  0.0  250.0
  ++ low  low temperature limit
    -- WORD  0.0  250.0
– period  Set diagnostics period
  + <10030000>  Diagnostics period <10030000> default 1000 milliseconds
– watchdog  enable the watchdog

• diagshell  Provide diag shell access
• encrypt  Encrypt password or key with secret
  – secret  Encrypt passwords/keys with secret phrase
    + 2  Type of encryption SHA256AES256
    - WORD  Passphrase for encryption
    ++ plaintext  Plaintext password or key to encrypt
      -- LINE  Plaintext to be encrypted with given secret
• pm  Process Monitor
  – maxsysrestarts  Maximum number of times PM will restart the system because of a failed processes
    <15>  Maximum number of system restarts
  – sysrestart  Enable PM to restart the system when a processes fails
• prompt  Enable crashinfo prompt
  – crashinfo  Enable crashinfo prompt
• rp  radioprt serviceability parameters
  – forcedump  trigger the radioprt to send a crashdump to the wirelessmodule
• savecli  Save CLI tree for all modes in html format
• securitymgr  Securitymgr parameters
  – dumpcore  Create a core file of the securitymgr process
  – enablehttpstats  Enable securitymgr HTTP statistics interface
• set  Set service parameters
  – commandhistory  Set size of command history (default: 200)
    + <10300>  History size
  – reboothistory  Set size of reboot history (default: 50)
    + <10100>  History size
Manager Commands

- `upgradehistory`  Set size of upgrade history (default: 50)
  + `<10100>` History size

- `show`  Show running system information
  - `autoinstallstatus`  Autoinstall status
  - `chassisd`  Chassis Details
  - `cli`  Show CLI tree of current mode
  - `commandhistory`  Display command (except show commands) history.
  - `cpu`  Display system load
  - `crashinfo`  Display information about core, panic and AP dump files
    + `PANIC_FILENAMEx`  Show contents of specified kernel panic file
  - `diag`  Diagnostics
    + `hardware`  Show the system hardware configuration
    + `limits`  Show limit values
    + `period`  Show the period (ms) for the in service diagnostics
    + `stats`  Show the curent diagnostics statistics
    + `top`  Show top processes (sorted by memory usage)
    + `watchdog`  Show watchdog status
  - `info`  Show snapshot of available support information
  - `lastpasswd`  Display last password used to enter shell
  - `memory`  Show memory statistics
  - `pm`  Process Monitor
    + `history`  State changes for a process, the time they happened and the events that triggered them
      - `WORD`  Process name
      - `all`  All processes
    - `process`  Show processes (sorted by memory usage)
    - `reboothistory`  Show reboot history
    - `rp`  radioport serviceability parameters
      + `beaconcount`  radioport beacon count (cumulative number of beacons sent)
    - `startuplog`  Show startup log
    - `temperature`  Display CPU temperature
    - `upgradehistory`  Show upgrade history
    - `wireless`  Wireless parameters
      + `rp`  radioport serviceability parameters
        - `history`  radioport history
          + XX.XXXXXXXX radioport MAC
+ **station**  station serviceability parameters
- **history**  station history
  ++ **XXXXXXXXXXXX**  station MAC

- **tethereal**  Dump and analyze network traffic
  - **LINE**  tethereal options in the format [V (print detailed packet)]
    [x (hex dump of packet)] [p (no promiscuous mode for interface)]
    [n (disable name resolution)] [c ] [h (detailed help)] [E (to capture
    ESPD)] [e (capture nonEspd packets)] [f ] [i ] [W (wisp packet
    only)] [s ] [r (read contents of specified file)] [w (save capture in
    specified file) ] [X (for examples on tethereal capture filter) ]

- **wireless**  Wireless parameters
  - **dumpcore**  Create a core file of the ccsrvr process
  - **dumpstate**  Create a ccsrvr.dump file in nvram with internal
    state information
  - **muhistory**  Enable mu association history
  - **muhistoryclear**  Delete all mu association history files
  - **ratescale**  Enable wireless rate scaling (default)
  - **requestrplog**  Request rp Log
    + **<148>**  rp index
      - **file**  output to file
      - **log**  output to syslog

**Default Setting**

N/A

**Command Mode**

Manager

**Example**

```
HPswitch#support clear all
HPswitch
```

telnet

This command opens a telnet connection.

**Syntax**

telnet **WORD**

  - **WORD**  - IP address or hostname of a remote system.
    - **PORT**  - TCP Port number.
Default Setting
N/A

Command Mode
Manager

Example
This example displays an incomplete route telnet message.

```
HPswitch#telnet 10.1.0.9 23
telnet: Unable to connect to remote host (10.1.0.9): No route to host
HPswitch#
```

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
```
HPswitch#terminal length 1000
HPswitch#
HPswitch#terminal width 1900
HPswitch#
```
upgrade

This command upgrades the software image.

Syntax

```
upgrade URL
```

- **URL** - Location of firmware image.
  - URLs: tftp://<hostname or IP>/path/file
    ftp://<user>:<passwd>@<hostname or IP>/path/file

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#upgrade tftp://192.168.1.10/WS.00.01.img
HPswitch#
```

upgrade-abort

This command aborts an ongoing upgrade.

Syntax

```
upgrade-abort
```

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#upgrade-abort
HPswitch#
```
write

This command writes the running configuration to memory or terminal.

Syntax
write memory | terminal
- memory - Write to NV memory.
- terminal - Write to terminal.

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#write terminal
!
! configuration of ProCurveWLANModule Wireless Services
version WS.01.XX.05518w6
!
version 1.0
!
ip web-management
snmp-server manager v2
snmp-server manager v3
snmp-server user manager v3 encrypted auth md5
0x709f649df8ba589f178416c291fca0
snmp-server user operator v3 encrypted auth md5
0x777da3446d4dcea9e722cfaa520021
!
wireless
no country-code
!
interface vlan1
  ip address dhcp
!
end

HPswitch#
GlobalCommands

These commands are used to configure the global commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>Enables authentication, authorization and accounting configuration parameters.</td>
<td>A-54</td>
</tr>
<tr>
<td>acess-list</td>
<td>Adds an access control list (ACL) entry.</td>
<td>A-56</td>
</tr>
<tr>
<td>boot</td>
<td>Reboots wireless module.</td>
<td>A-56</td>
</tr>
<tr>
<td>cls</td>
<td>Clears the display screen.</td>
<td>A-57</td>
</tr>
<tr>
<td>country-code</td>
<td>Configures the country code.</td>
<td>A-57</td>
</tr>
<tr>
<td>crypto</td>
<td>Encryption related commands.</td>
<td>A-60</td>
</tr>
<tr>
<td>end</td>
<td>Ends current mode and changes back to Manager mode.</td>
<td>A-64</td>
</tr>
<tr>
<td>exit</td>
<td>Ends current mode.</td>
<td>A-64</td>
</tr>
<tr>
<td>[no] fallback</td>
<td>(Negates) Configures software fallback commands.</td>
<td>A-65</td>
</tr>
<tr>
<td>help</td>
<td>Displays the interactive help system.</td>
<td>A-66</td>
</tr>
<tr>
<td>[no] hostname</td>
<td>(Negates) Sets system's network name.</td>
<td>A-66</td>
</tr>
<tr>
<td>[no] interface</td>
<td>(Negates) Selects an interface to configure.</td>
<td>A-67</td>
</tr>
<tr>
<td>[no] ip</td>
<td>(Negates) Interface protocol.</td>
<td>A-68</td>
</tr>
<tr>
<td>licenses</td>
<td>Licensing commands.</td>
<td>A-71</td>
</tr>
<tr>
<td>[no] logging</td>
<td>(Negates) Modify message logging facilities.</td>
<td>A-72</td>
</tr>
<tr>
<td>logout</td>
<td>Exits user from the CLI.</td>
<td>A-74</td>
</tr>
<tr>
<td>mac</td>
<td>Enables configuration of MAC access lists.</td>
<td>A-75</td>
</tr>
<tr>
<td>management</td>
<td>Set properties of the management interface.</td>
<td>A-75</td>
</tr>
<tr>
<td>no</td>
<td>Negates a command or set its defaults</td>
<td>A-75</td>
</tr>
<tr>
<td>ntp</td>
<td>Configure NTP.</td>
<td>A-76</td>
</tr>
<tr>
<td>[no] password-encryption</td>
<td>(Negates) Encrypts passwords in configuration.</td>
<td>A-78</td>
</tr>
</tbody>
</table>
### GlobalCommands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server</td>
<td>Enables radius server mode.</td>
<td>A-79</td>
</tr>
<tr>
<td>[no]redundancy</td>
<td>(Negates) Configures redundancy group parameters.</td>
<td>A-82</td>
</tr>
<tr>
<td>service</td>
<td>Control the use of network services.</td>
<td>A-33</td>
</tr>
<tr>
<td>sflow</td>
<td>Configures or unclaims an sflow sampling receiver.</td>
<td>A-84</td>
</tr>
<tr>
<td>show</td>
<td>Shows running system information.</td>
<td>A-86</td>
</tr>
<tr>
<td>[no] snmp-server</td>
<td>(Negates) Modify SNMP server parameters.</td>
<td>A-96</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Spanning tree commands.</td>
<td>A-96</td>
</tr>
<tr>
<td>time</td>
<td>Configures software system clock.</td>
<td>A-100</td>
</tr>
<tr>
<td>[no] timezone</td>
<td>(Negates) Configures the timezone.</td>
<td>A-101</td>
</tr>
<tr>
<td>username</td>
<td>Enables user name authentication</td>
<td>A-102</td>
</tr>
<tr>
<td>wireless</td>
<td>Configures wireless parameters.</td>
<td>A-103</td>
</tr>
<tr>
<td>wlan-acl</td>
<td>Apply an ACL on a WLAN.</td>
<td>A-104</td>
</tr>
</tbody>
</table>

### aaa

This command enables authentication, authorization and accounting configuration parameters.

**Syntax**

```
aaa (authentication | nas | vpnauthentication)
```

- **authentication** Authentication configuration parameters
  - **login** Set authentication lists for logins
    - **default** The default authentication list
      - **local** Use local user database
      - **none** No authentication
      - **radius** Use external radius server
• **nas** identifies the NAS originating the RADIUS access request (for VPN only)
  - **WORD** A string of up to 64 characters

• **vpnauthentication** RADIUS setting
  - **primary** primary radius server
    + **A.B.C.D** IP Address
      - **key** RADIUS client preshared key; this should match with RADIUS server
        ++ 0 Password is specified UNENCRYPTED
        -- **WORD** shared secret upto 32 characters
        +++ **authport** RADIUS server authentication port
          --- **PORT_RANGE** port: range <102465535>
        ++ 2 Password is encrypted with passwordencryption secret
        -- **WORD** shared secret upto 32 characters
        +++ **authport** RADIUS server authentication port
          --- **PORT_RANGE** port: range <102465535>
        ++ **WORD** shared secret upto 32 characters
        -- **authport** RADIUS server authentication port
          +++ **PORT_RANGE** port: range <102465535>
  - **secondary** secondary radius server
    + **A.B.C.D** IP Address
      - **key** RADIUS client preshared key; this should match with server
        ++ 0 Password is specified UNENCRYPTED
        -- **WORD** shared secret upto 32 characters
        +++ **authport** RADIUS server authentication port
          --- **PORT_RANGE** port: range <102465535>
        ++ 2 Password is encrypted with passwordencryption secret
        --- **WORD** shared secret upto 32 characters
        +++ **authport** RADIUS server authentication port
          --- **PORT_RANGE** port: range <102465535>
        -- **WORD** shared secret upto 32 characters
        +++ **authport** RADIUS server authentication port
          --- **PORT_RANGE** port: range <102465535>
Default Setting
N/A

Command Mode
Global

Example

HPswitch#aaa authentication login default local
HPswitch

access-list

This command adds an access control list (ACL) entry.

Syntax
access-list

(See switch reference.)

Default Setting
N/A

Command Mode
Global

Example

HPswitch#access-list
HPswitch

boot

This command reboots the wireless module.

Syntax
boot flash (primary | secondary )

• flash - Specifies the boot image to use after reboot.
  – primary - Primary image.
  – secondary - Secondary image.

Default Setting
N/A
Command Mode

Global Configuration

Example

```plaintext
HPswitch#configure
HPswitch(config)#boot flash primary
Wireless module will be rebooted, do you want to continue? (y/n): y
Do you want to save current configuration? (y/n): n
ProCurve(config)#
```

**cls**

This command clears the display screen.

**Syntax**

cls

**Default Setting**

N/A

**Command Mode**

Global

**Example**

```plaintext
HPswitch#cls
HPswitch
```

country-code

This command configures the country of operation. All existing radio configuration will be erased.

**Syntax**

country <country_code>

- **country_code** - A two character code that identifies the country of operation. See Table A-1 on page A-58 for a full list of the codes.
Table A-1. Country Codes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>AF</td>
<td>Egypt</td>
<td>EG</td>
<td>Lebanon</td>
<td>LB</td>
</tr>
<tr>
<td>Albania</td>
<td>AL</td>
<td>El Salvador</td>
<td>SV</td>
<td>Lesotho</td>
<td>LS</td>
</tr>
<tr>
<td>Algeria</td>
<td>DZ</td>
<td>Estonia</td>
<td>EE</td>
<td>Libyan Arab Jamahiriya</td>
<td>LY</td>
</tr>
<tr>
<td>Andorra</td>
<td>AD</td>
<td>Finland</td>
<td>FI</td>
<td>Liechtenstein</td>
<td>LI</td>
</tr>
<tr>
<td>Angola</td>
<td>AO</td>
<td>France</td>
<td>FR</td>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Argentina</td>
<td>AR</td>
<td>French Guiana</td>
<td>GF</td>
<td>Luxembourg</td>
<td>LU</td>
</tr>
<tr>
<td>Armenia</td>
<td>AM</td>
<td>Georgia</td>
<td>GE</td>
<td>Macau</td>
<td>MO</td>
</tr>
<tr>
<td>Australia</td>
<td>AU</td>
<td>Germany</td>
<td>DE</td>
<td>Macedonia, The Former Yugoslav Republic Of</td>
<td>MK</td>
</tr>
<tr>
<td>Austria</td>
<td>AT</td>
<td>Gibraltar</td>
<td>GI</td>
<td>Malaysia</td>
<td>MY</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>AZ</td>
<td>Greece</td>
<td>GR</td>
<td>Malta</td>
<td>MT</td>
</tr>
<tr>
<td>Bahamas</td>
<td>BS</td>
<td>Guam</td>
<td>GU</td>
<td>Mauritius</td>
<td>MU</td>
</tr>
<tr>
<td>Bahrain</td>
<td>BH</td>
<td>Guatemala</td>
<td>GT</td>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>BD</td>
<td>Guyana</td>
<td>GY</td>
<td>Moldova, Republic Of</td>
<td>MD</td>
</tr>
<tr>
<td>Belarus</td>
<td>BY</td>
<td>Haiti</td>
<td>HI</td>
<td>Monaco</td>
<td>MC</td>
</tr>
<tr>
<td>Belgium</td>
<td>BE</td>
<td>Holy See</td>
<td>VA</td>
<td>Mongolia</td>
<td>MN</td>
</tr>
<tr>
<td>Belize</td>
<td>BZ</td>
<td>Honduras</td>
<td>HN</td>
<td>Morocco</td>
<td>MA</td>
</tr>
<tr>
<td>Bermuda</td>
<td>BM</td>
<td>Hong Kong</td>
<td>HK</td>
<td>Mozambique</td>
<td>MZ</td>
</tr>
<tr>
<td>Bolivia</td>
<td>BO</td>
<td>Hungary</td>
<td>HU</td>
<td>Myanmar</td>
<td>MM</td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td>BA</td>
<td>Iceland</td>
<td>IS</td>
<td>Namibia</td>
<td>NA</td>
</tr>
<tr>
<td>Botswana</td>
<td>BW</td>
<td>India</td>
<td>IN</td>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
<td>Indonesia</td>
<td>ID</td>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: All codes are two-letter codes as per the ISO 3166 standard.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Brunei Darussalam</td>
<td>BN</td>
<td>Iran, Islamic Republic Of</td>
<td>IR</td>
<td>Nicaragua</td>
<td>NI</td>
<td>Turkmenistan</td>
<td>TM</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>BG</td>
<td>Iraq</td>
<td>IQ</td>
<td>Nigeria</td>
<td>NG</td>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>Cambodia</td>
<td>KH</td>
<td>Ireland</td>
<td>IE</td>
<td>Norway</td>
<td>NO</td>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
<td>Israel</td>
<td>IL</td>
<td>Oman</td>
<td>OM</td>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
<td>Italy</td>
<td>IT</td>
<td>Pakistan</td>
<td>PK</td>
<td>United States</td>
<td>US</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
<td>Jamaica</td>
<td>JM</td>
<td>Palestinian</td>
<td>PS</td>
<td>Uruguay</td>
<td>UY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Territory, Occupied</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td>CO</td>
<td>Japan</td>
<td>JP</td>
<td>Panama</td>
<td>PA</td>
<td>Uzbekistan</td>
<td>UZ</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
<td>Jordan</td>
<td>JO</td>
<td>Paraguay</td>
<td>PY</td>
<td>Venezuela</td>
<td>VE</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
<td>Kazakhstan</td>
<td>KZ</td>
<td>Peru</td>
<td>PE</td>
<td>Vietnam</td>
<td>VN</td>
</tr>
<tr>
<td>Cuba</td>
<td>CU</td>
<td>Korea, Democratic People Republic Of</td>
<td>KP</td>
<td>Philippines</td>
<td>PH</td>
<td>Yemen</td>
<td>YE</td>
</tr>
<tr>
<td>Cyprus</td>
<td>CY</td>
<td>Korea, Republic Of</td>
<td>KR</td>
<td>Poland</td>
<td>PL</td>
<td>Zambia</td>
<td>ZM</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>CZ</td>
<td>Kuwait</td>
<td>KW</td>
<td>Portugal</td>
<td>PT</td>
<td>Zimbabwe</td>
<td>ZW</td>
</tr>
<tr>
<td>Denmark</td>
<td>DK</td>
<td>Kyrgyzstan</td>
<td>KG</td>
<td>Puerto Rico</td>
<td>PR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>DO</td>
<td>Lao People's Democratic Republic</td>
<td>LA</td>
<td>Qatar</td>
<td>QA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecuador</td>
<td>EC</td>
<td>Latvia</td>
<td>LV</td>
<td>Romania</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Default Setting**

No country code set

**Command Mode**

Global Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#country-code us
HPswitch(config)#
```
crypto

This command cconfigures encryption related commands.

Syntax

crypto (ipsec | transformset | isakmp | key | map | pki)

- **ipsec** Configure IPSEC policy
  - **securityassociation** Security association parameters
    + **lifetime** security association lifetime
      - **kilobytes** Volumebased key duration minimum is 500 KB maximum is 2147483646
      + **WORD** Security association duration in seconds/kilobytes
      - **seconds** Timebased key duration minimum is 90 sec maximum is 2147483646
      + **WORD** Security association duration in seconds/kilobytes

- **transformset** Define transform and settings
  - **WORD** Transform set tag
    + **ahmd5hmac** AHHMACMD5 transform
      - **esp3des** ESP transform using 3DES cipher (168 bits)
      - **espaes** ESP transform using AES cipher
      - **espaes192** ESP transform using AES cipher (192 bits)
      - **espaes256** ESP transform using AES cipher (256 bits)
      - **espdes** ESP transform using DES cipher (56 bits)
    + **ahshahmac** AHHMACSHA transform
      - **esp3des** ESP transform using 3DES cipher (168 bits)
      - **espaes** ESP transform using AES cipher
      - **espaes192** ESP transform using AES cipher (192 bits)
      - **espaes256** ESP transform using AES cipher (256 bits)
      - **espdes** ESP transform using DES cipher (56 bits)
    + **espmd5hmac** ESP transform using HMACMD5 auth
GlobalCommands

- esp3des ESP transform using 3DES cipher (168 bits)
- espaes ESP transform using AES cipher
- espaes192 ESP transform using AES cipher (192 bits)
- espaes256 ESP transform using AES cipher (256 bits)
- espdes ESP transform using DES cipher (56 bits)

+ espshahmac ESP transform using HMACSHA auth

- esp3des ESP transform using 3DES cipher (168 bits)
- espaes ESP transform using AES cipher
- espaes192 ESP transform using AES cipher (192 bits)
- espaes256 ESP transform using AES cipher (256 bits)
- espdes ESP transform using DES cipher (56 bits)

• isakmp Configure ISAKMP policy
  – client Modeconfig or IPSec/L2TP settings
    + configuration configuration pushed to the client
      - group group (currently only one is supported)
        ++ default default group tag
  – keepalive Set a keepalive interval for use with remote peers
    + <103600> Number of seconds between keep alives
  – key Set preshared key for remote peer
    + 0 Password is specified UNENCRYPTED
      - WORD user password
        ++ address define shared key with IP address
        -- A.B.C.D Peer IP address
        ++ hostname define shared key with hostname
        -- WORD hostname of peer with whom the key is shared
    + 2 Password is encrypted with passwordencryption secret
      - WORD user password
        ++ address define shared key with IP address
        -- A.B.C.D Peer IP address
        ++ hostname define shared key with hostname
        -- WORD hostname of peer with whom the key is shared
    + WORD user password
      - address define shared key with IP address
        ++ A.B.C.D Peer IP address
      - hostname define shared key with hostname
        ++ WORD hostname of peer with whom the key is shared
– peer remote peer
  + address Identity of remote peer is ipaddress
    - A.B.C.D ip address
  + dn Identity of remote peer is Distinguished Name
    - WORD Name
  + hostname Identity of remote peer is hostname
    - WORD hostname
  + policy Set policy for an ISAKMP protection suite
    - <110000> Priority of protection suite

• key Authentication key management
  – export Export keypair related configuration
    + rsa Export rsa keypair
      - WORD Name of the rsa keypair to be exported
        ++ URL URL to send the key to URLs: tftp:///path/file ftp://
        :@/path/file
        -- WORD Pass Phrase to be associated to the Keypair
  – generate Generate keypair
    + rsa Generate rsa keypair
      - WORD Keypair name
        ++ <10242048> Size of keypair in bits
  – import Import keypair related configuration
    + rsa Import rsa keypair
      - WORD Name to which to import the rsakey
        ++ URL URL to get the key from URLs: tftp:///path/file ftp://
        :@/path/file
        -- WORD Pass phrase to be associated to the Keypair
  – zeroize Delete keypair
    + rsa Delete rsa keypair
      - WORD Name of the rsa keypair to be deleted

• map Enter a crypto map
  – WORD Crypto map tag  32 character length
    + <11000> Sequence to insert into crypto map entry
      - ipsecisakmp IPSEC w/ISAKMP
        ++ dynamic dynamic map entry for XAUTH with mode-
        config or ipsec12tp configuration
      - ipseccmanual IPSEC w/manual keying
++ dynamic  dynamic map entry for XAUTH with mode-config or ipsecl2tp configuration

- pki  Public Key Infrastructure commands
  - authenticate  Authenticate and import ca certificate
    + WORD  Trustpoint Name
    - URL  URL to get the ca certificate from URLs: tftp:///path/file ftp://:@/path/file
    - terminal  Copy & Paste mode of enrollment
    + WORD  Trustpoint Name enroll  Generate certificate request or selfsigned certificate for the trustpoint
    - request  Certificate request mode of enrollment
    - selfsigned  Selfsigned mode of enrollment
  - export  Export trustpoint related configuration
    + WORD  Trustpoint Name
    - request  Export certificate request for the trustpoint
      ++ URL  URL to send the certificate request to URLs: tftp:///path/file ftp://:@/path/file
    - trustpoint  Export trustpoint configuration including either certificate request and key or ca certificate or both
      ++ URL  URL to send the trustpoint configuration to URLs: tftp:///path/file ftp://:@/path/file
  - import  Import trustpoint related configuration
    + WORD  Trustpoint Name
    - certificate  Import Server certificate for the trustpoint
      ++ URL  URL to get the server certificate from URLs: tftp:///path/file ftp://:@/path/file
      ++ terminal  Copy & Paste mode of enrollment
    - crl  Certificate Revocation list
      ++ URL  URL to get the server certificate from URLs: tftp:///path/file ftp://:@/path/file
      -- <1168>  Duration to replay the command in hours
    - trustpoint  Import trustpoint including either private key and server certificate or ca certificate or both
      ++ URL  URL to get the trustpoint configuration from URLs: tftp:///path/file ftp://:@/path/file
  - trustpoint  Create and configure a trustpoint
    + WORD  Trustpoint Name
**end**

This command ends the current mode and changes to the Manager mode.

**Syntax**

```
end
```

**Default Setting**

N/A

**Command Mode**

Global Configuration

**Example**

```
HPswitch# configure
HPswitch(config)# end
HPswitch#
```

**exit**

This command ends current mode and down to previous mode.

**Syntax**

```
exit
```

**Default Setting**

N/A

**Command Mode**

Global
Example

This example shows how to return to the previous command levels starting from the Manager Configuration mode and finally logging out of the CLI session.

```
HPswitch#exit
ProCurve (config)#exit
ProCurve#exit
ProCurve>exit
Do you want to log out [y/n]?y
Do you want to save your current configuration?n
Connection to host lost.
```

fallback

This command configures software fallback feature. The no command negates the enabling of the fallback feature.

**Syntax**

```
fallback (enable)
no fallback (enable)
```

- **enable** - Enables software fallback feature. Failure to boot with configured "use on boot" image allows booting with other image. No command disables the fallback feature.

**Default Setting**

Enabled

**Command Mode**

Global Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#no fallback enable
HPswitch(config)#
```
help

This command displays the interactive help system.

Syntax

help

Default Setting

N/A

Command Mode

Global

Example

HPswitch#help

CLI provides advanced help feature. When you need help, anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup until entering a '? ' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ? ') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show ve?').

hostname

This command sets the system’s network name. The no command negates this configuration.

Syntax

hostname (LINE)

no hostname

• LINE - The system’s network name.
Default Setting
Wireless Services

Command Mode
Global Configuration

Example

HPswitch#configure
HPswitch(config)#hostname EXHOSTNAME
ProCurve(wireless-services-B)(config)#

Related Commands
show hostname (page A-138)

interface
This command provides an interface selection to configure.

Syntax
interface (IFNAME | dnlink | tunnel | uplink | vlan)
  • IFNAME  vlan1 vlan4094, tunnel1 tunnel32, uplink / dnlink
  • dnlink  dnlink interface
  • tunnel  Tunnel interface
    – <132>  Tunnel Id
  • uplink  uplink interface
  • vlan    Vlan interface
    – <14094>  Vlan Id

Default Setting
N/A

Command Mode
Global

Example

HPswitch#configure
HPswitch(config)#interface vlan1
HPswitch(config-if)#

A-67
ip (global)

This command configures Internet Protocol (IP) parameters. The no command negates this configuration.

Syntax

ip (accesslist | defaultgateway | dhcp | dns | dnslookup | domain | http | local | nat | route | routing | securewebmanagement | telnet | webmanagement)

- accesslist  ACL Config
  - extended  Extended ACL
    + <100199>  IP extended access list
    + <20002699>  IP extended access list (expanded range)
    + WORD  Name of ACL
  - standard  Standard ACL
    + <199>  IP standard access list
    + <13001999>  IP standard access list (expanded range)
    + WORD  Name of ACL
- defaultgateway  Configure default gateway
  - A.B.C.D  IP gateway address
- dhcp  DHCP Server configuration
  - bootp  BOOTP specific configuration
    + ignore  Configure DHCP Server to ignore BOOTP requests
  - excludedaddress  Prevent DHCP Server from assigning certain addresses
    + A.B.C.D  Low IP Address
    - A.B.C.D  High IP Address
  - option  Define DHCP server option
    + WORD  Option name
      - <0254>  Option Code
        ++ ascii  Specify the option type as ascii
        ++ ip  Specify the option type as IP address
  - ping  Specify ping parameters used by DHCP Server
    + timeout  Specify ping timeout
      - <110>  Ping timeout in seconds
  - pool  Configure DHCP server address pool
    + WORD  Pool name
- dns  Add a Nameserver to the DNS
  - A.B.C.D  IP address of Nameserver to add
- dnslookup  Enable Domain Name Service (DNS)
• **domain**  Set default domain for DNS  
  – **WORD**  Domain string (e.g. company.com)

• **http**  Hyper Text Terminal Protocol (HTTP)  
  – **securetrustpoint**  Trustpoint to be used for secure connection  
    + **WORD**  Trustpoint Name

• **local**  IP address range assigned to VPN client using Modeconfig or IPSec with L2TP  
  – **pool**  specify address range  
    + **default**  default group tag  
      - **lowipaddress**  Lowest range for IP address  
        ++ **A.B.C.D**  Internet Protocol (IP)  
      - **highipaddress**  Highest range for IP address  
        ++ **A.B.C.D**  Internet Protocol (IP)

• **nat**  Network Address Translation (NAT)  
  – **inside**  Inside address translation  
    + **destination**  Destination address translation  
      - **static**  Specify static local>global mapping  
        ++ **A.B.C.D**  Inside local IP address (A.B.C.D)  
          -- **<165535>**  Inside local Port  
          +++ **tcp**  Transmission Control Protocol  
        ++ **A.B.C.D**  Inside global IP address (A.B.C.D)  
          -- **<165535>**  Inside global Port  
          +++ **udp**  User Datagram Protocol  
        ++ **A.B.C.D**  Inside global IP address (A.B.C.D)  
          -- **<165535>**  Inside global Port  
      + **source**  Source address translation  
        - **list**  Specify access list describing local addresses  
          ++ **WORD**  Access list name  
            -- **interface**  Select an Interface  
              +++ **IFNAME**  Interface Name  
                -- **overload**  Overload  
        - **static**  Specify static local>global mapping  
          ++ **A.B.C.D**  Inside local IP address (A.B.C.D)  
            -- **A.B.C.D**  Inside global IP address (A.B.C.D)
+++ <165535> Inside global Port
   outside Outside address translation
   + destination Destination address translation
   -- static Specify static local>global mapping
      ++ A.B.C.D Outside local IP address (A.B.C.D)
   -- <165535> Outside local Port
      +++ tcp Transmission Control Protocol
         --- A.B.C.D Outside global IP address (A.B.C.D)
            ++++ <165535> Outside global Port
      +++ udp User Datagram Protocol
         --- A.B.C.D Outside global IP address (A.B.C.D)
            ++++ <165535> Outside global Port
   -- A.B.C.D Outside global IP address (A.B.C.D)
      +++ <165535> Outside global Port
   + source Source address translation
   -- list Specify access list describing local addresses
      ++ WORD Access list name
   -- interface Select an Interface
      +++ IFNAME Interface Name
         overload Overload
   -- static Specify static local>global mapping
      ++ A.B.C.D Outside local IP address (A.B.C.D)
   -- A.B.C.D Outside global IP address (A.B.C.D)
      +++ <165535> Outside global Port
   • route Establish static routes
      -- A.B.C.D IP destination prefix
         + A.B.C.D IP destination prefix mask
            - A.B.C.D IP gateway address
      -- A.B.C.D/M IP destination prefix (e.g. 10.0.0.0/8)
         + A.B.C.D IP gateway address
   • routing Turn on IP routing
   • securewebmanagement Secured web server
   • telnet Telnet server
      -- port Listening port
         + <065535> Port number
   • webmanagement Web server
      -- localhost only serve requests from localhost
Default Setting
N/A

Command Mode
Global

Example

HPswitch#configure
HPswitch(config)#ip route 10.0.0.1/4 255.255.255.0
HPswitch(config)#ip routing
HPswitch(config)#ip web-management
HPswitch(config)#

Related Commands
show ip (page A-139)

licenses

This command configures licensing parameters.

Syntax
licenses (hardwareid | install | uninstall)
• hardwareid  Generate a hardware Id for license registration process.
  – radioports  Feature group
• install  Install the specified license key.
  – radioports  Feature group
    + WORD  License key: 44 byte char string encrypted with hardware id
• uninstall  Uninstall a set of licenses previously installed on the blade.
  – radioports  Feature Group
    + <010000>  Value of the license to be uninstalled (e.g. number of radio ports)

Default Setting
N/A

Command Mode
Global
Example

```
HPswitch# configure
HPswitch# licenses hardwareid radioports
The hardware Id for package radio-ports is
SG528WC011-H-EXAMPLE-8KJKPT6-T67XT6P-3GT8QJ9
HPswitch(config) #
```

Related Commands

show licenses (page A-143)

logging

This command modifies message logging facilities. The no command negates
the logging configuration.

Syntax

```
logging (aggregationtime | buffered | console | faility | host | monitor | on | syslog)
```

- **aggregationtime**  Set number of seconds for aggregating repeated
  messages
  - `<160>`  Aggregation time in seconds
- **buffered**  Set buffered logging level
  - `<07>`  Logging severity level
  - **alerts**  Immediate action needed (severity=1)
  - **critical**  Critical conditions (severity=2)
  - **debugging**  Debugging messages (severity=7)
  - **emergencies**  System is unusable (severity=0)
  - **errors**  Error conditions (severity=3)
  - **informational**  Informational messages (severity=6)
  - **notifications**  Normal but significant conditions (severity=5)
  - **warnings**  Warning conditions (severity=4)
- **console**  Set console logging level
  - `<07>`  Logging severity level
  - **alerts**  Immediate action needed (severity=1)
  - **critical**  Critical conditions (severity=2)
  - **debugging**  Debugging messages (severity=7)
  - **emergencies**  System is unusable (severity=0)
  - **errors**  Error conditions (severity=3)
  - **informational**  Informational messages (severity=6)
  - **notifications**  Normal but significant conditions (severity=5)
  - **warnings**  Warning conditions (severity=4)
• **facility** Syslog facility in which log messages are sent
  – **local0** Syslog facility local0
  – **local1** Syslog facility local1
  – **local2** Syslog facility local2
  – **local3** Syslog facility local3
  – **local4** Syslog facility local4
  – **local5** Syslog facility local5
  – **local6** Syslog facility local6
  – **local7** Syslog facility local7

• **host** Configure remote host to receive log messages
  – **A.B.C.D** Remote host’s IP address

• **monitor** Set terminal lines logging level
  – **<07>** Logging severity level
    – **alerts** Immediate action needed (severity=1)
    – **critical** Critical conditions (severity=2)
    – **debugging** Debugging messages (severity=7)
    – **emergencies** System is unusable (severity=0)
    – **errors** Error conditions (severity=3)
    – **informational** Informational messages (severity=6)
    – **notifications** Normal but significant conditions (severity=5)
    – **warnings** Warning conditions (severity=4)

• **on** Enable logging of system messages

• **syslog** Set syslog servers logging level
  – **<07>** Logging severity level
    – **alerts** Immediate action needed (severity=1)
    – **critical** Critical conditions (severity=2)
    – **debugging** Debugging messages (severity=7)
    – **emergencies** System is unusable (severity=0)
    – **errors** Error conditions (severity=3)
    – **informational** Informational messages (severity=6)
    – **notifications** Normal but significant conditions (severity=5)
    – **warnings** Warning conditions (severity=4)

**Default Setting**

N/A

**Command Mode**

Global

**Example**

```
HPswitch#logging aggregationtime <160>
HPswitch
```
logout

This command exits user from the CLI.

**Syntax**

```plaintext
logout
```

**Default Setting**

N/A

**Command Mode**

Global

**Example**

```
HPswitch#logout
HPswitch
```

mac

This command enables configuration of MAC access lists.

**Syntax**

```plaintext
mac (accesslist)
```

- **accesslist**  ACL Config
  - **extended**  MAC Extended ACL

  + **WORD**  Name of ACL. For specifying a number as a name it should be outside the range of 1199 and 13002699

**Default Setting**

N/A

**Command Mode**

Global

**Example**

```
HPswitch#mac accesslist extended WORD
HPswitch
```

**Related Commands**

- show logging (page A-143)
management

This command enables configuration of MAC access lists.

Syntax

management (secure)

• secure Limits local access to the switch (web/telnet/etc.) to the management interface.

Default Setting

N/A

Command Mode

Global

Example

HPswitch#management
HPswitch

no

This command enables user to negate a command or set its defaults.

Syntax

no

Default Setting

N/A

Command Mode

Global

Example

HPswitch#no ntp
HPswtch
ntp

This command enables user to configure NTP.

Syntax

\textit{ntp} [\texttt{accessgroup} | \texttt{authenticate} | \texttt{authenticationkey} | \texttt{autokey} | \texttt{broadcast} | \texttt{broadcastdelay} | \texttt{master} | \texttt{peer} | \texttt{server} | \texttt{trustedkey}]

- **accessgroup** Control NTP access
  - **peer** Provide full access
    - 199 Standard IP access list
    - 13001999 Standard IP access list (expanded range)
  - **queryonly** Allow only control queries
    - 199 Standard IP access list
    - 13001999 Standard IP access list (expanded range)
  - **serve** Provide server and query access
    - 199 Standard IP access list
    - 13001999 Standard IP access list (expanded range)
  - **serveonly** Provide only server access
    - 199 Standard IP access list
    - 13001999 Standard IP access list (expanded range)

- **authenticate** Authenticate time sources

- **authenticationkey** Authentication key for trusted time sources
  - 165534 Key number
  - **md5** MD5 authentication
    - \texttt{WORD} Authentication key

- **autokey** Enable NTP autokey authentication scheme
  - **clientonly** Switch will be a client to other trusted hosts in the autokey group
  - **host** Configure the switch as a trusted host

- **broadcast** Configure NTP broadcast service
  - **client** Listen to NTP broadcasts
  - **destination** Configure broadcast destination address
    - \texttt{WORD} Destination broadcast IP address
    - **key** Broadcast key
      - 165534 Key ID
    - **version** NTP version
      - 14 NTP Version number
      - **key** Broadcast key
      - 165534 Key ID

• **broadcastdelay**  Estimated roundtrip delay
  –  \(<19999999>\)  Roundtrip delay in microseconds

• **master**  Act as a NTP master clock
  –  \(<115>\)  Stratum number

• **peer**  Configure NTP peer
  –  **WORD**  Name/IP address of peer
    + **autokey**  Configure autokey peer authentication scheme
      - **prefer**  Prefer this peer when possible
      - **version**  Configure NTP version
    + **key**  Configure peer authentication key
      -  \(<165534>\)  Peer key number
        ++ **prefer**  Prefer this peer when possible
        ++ **version**  Configure NTP version
    + **prefer**  Prefer this peer when possible
    + **version**  Configure NTP version

• **server**  Configure NTP server
  –  **WORD**  IP address of peer
    + **autokey**  Configure autokey peer authentication scheme
      - **prefer**  Prefer this peer when possible
      - **version**  Configure NTP version
    + **key**  Configure peer authentication key
      -  \(<165534>\)  Peer key number
        ++ **prefer**  Prefer this peer when possible
        ++ **version**  Configure NTP version
    + **prefer**  Prefer this peer when possible
    + **version**  Configure NTP version

• **trustedkey**  Key numbers for trusted time sources
  –  \(<165534>\)  Key number

**Default Setting**

N/A

**Command Mode**

Global
password-encryption

This command encrypts passwords in configuration. The no command negates the encryption.

Syntax

password-encryption (secret)
no password-encryption

• secret - Encrypts passwords with secret phrase.
  – 2 - Type of encryption SHA256-AES256.
  +LINE - Passphrase for encryption.

Default Setting
Disabled

Command Mode
Global Configuration

Example

HPswitch#configure
HPswitch(config)#password-encryption secret 2 pass
HPswitch(config)#

Related Commands
show password-encryption (page A-146)

proxyarp

This command adds a proxy ARP entry in the ARP database.

Syntax

proxyarp (A.B.C.D)

• A.B.C.D - ARP Target IP address

Default Setting
N/A
**radius-server**

This command enables radius server mode.

**Syntax**

```
radius-server (host | key | local | transmit | timeout)
```

- **host** Specify a RADIUS server
  - `A.B.C.D` IP address of RADIUS server
  - `+authport` UDP port for RADIUS authentication server (default is 1812)
  - `<065536>` Port Number
  - `++ key` Perserver encryption key (overrides default)
    - `-- 0` Password is specified UNENCRYPTED
      - `+++ LINE` Text for this server’s key, upto 127 characters
    - `-- 2` Password is encrypted with passwordencryption secret
      - `+++ LINE` Text for this server’s key, upto 127 characters
    - `-- LINE` Text for this server’s key, upto 127 characters
  - `++ retransmit` Number of retries to active server (overrides default)
    - `<0100>` Number of retries to this server for a transaction
      - `+++ key` Perserver encryption key (overrides default)
        - `--- 0` Password is specified UNENCRYPTED
          - `++++ LINE` Text for this server’s key, upto 127 characters
        - `--- 2` Password is encrypted with passwordencryption secret
+++ LINE  Text for this server's key, upto 127 characters
--- LINE  Text for this server's key, upto 127 characters

++ timeout  Time to wait for this RADIUS server to reply (overrides default)
-- <11000>  Timeout value in seconds to wait for server to reply

+++ key  Perserver encryption key (overrides default)
--- 0  Password is specified UNENCRYPTED
+++ LINE  Text for this server's key, upto 127 characters
--- 2  Password is encrypted with passwordencryption secret
+++ LINE  Text for this server's key, upto 127 characters
--- LINE  Text for this server's key, upto 127 characters

++ retransmit  Number of retries to active server (overrides default)
-- <0100>  Number of retries to this server for a transaction

+++ key  Perserver encryption key (overrides default)
--- 0  Password is specified UNENCRYPTED
+++ LINE  Text for this server's key, upto 127 characters
--- 2  Password is encrypted with passwordencryption secret
+++ LINE  Text for this server's key, upto 127 characters
--- LINE  Text for this server's key, upto 127 characters

++ key  Perserver encryption key (overrides default)
-- 0  Password is specified UNENCRYPTED
+++ LINE  Text for this server's key, upto 127 characters
-- 2  Password is encrypted with passwordencryption secret
+++ LINE  Text for this server's key, upto 127 characters
-- LINE  Text for this server's key, upto 127 characters
++ retransmit  Number of retries to active server (overrides default)
-- <0100>  Number of retries to this server for a transaction
+++ key  Perserver encryption key (overrides default)
--- 0  Password is specified UNENCRYPTED
++++ LINE  Text for this server's key, upto 127 characters
--- 2  Password is encrypted with passwordencryption secret
++++ LINE  Text for this server's key, upto 127 characters
--- LINE  Text for this server's key, upto 127 characters
++ timeout  Time to wait for this RADIUS server to reply (overrides default)
-- <11000>  Timeout value in seconds to wait for server to reply
+++ key  Perserver encryption key (overrides default)
--- 0  Password is specified UNENCRYPTED
++++ LINE  Text for this server's key, upto 127 characters
--- 2  Password is encrypted with passwordencryption secret
++++ LINE  Text for this server's key, upto 127 characters
--- LINE  Text for this server's key, upto 127 characters
++ retransmit  Number of retries to active server (overrides default)
-- <0100>  Number of retries to this server for a transaction
+++ key  Perserver encryption key (overrides default)
--- 0  Password is specified UNENCRYPTED
++++ LINE  Text for this server's key, upto 127 characters
--- 2  Password is encrypted with passwordencryption secret

++++ LINE  Text for this server's key, upto 127 characters

--- LINE  Text for this server's key, upto 127 characters

• key  Encryption key shared with the radius servers
  – 0  Password is specified UNENCRYPTED
  + LINE  Text of shared key, upto 127 characters
  – 2  Password is encrypted with passwordencryption secret
  + LINE  Text of shared key, upto 127 characters
  – LINE  Text of shared key, upto 127 characters

• local  Configure local radius server parameters

• retransmit  Specify the number of retries to active server
  – <0100>  Number of retries for a transaction (default is 3)

• timeout  Time to wait for a RADIUS server to reply
  – <11000>  Wait time (default 5 seconds)

Default Setting
N/A

Command Mode
Global

Example

HPswitch#radius-server host A.B.C.D authport <065536> key 0
LINE
HPswitch

redundancy

This command enables user to configure redundancy group parameters. The no negates the configuration.

Syntax

redundancy | discoveryperiod | enable | groupid | handlestp | heartbeatperiod | holdperiod | interfaceip | manualrevert | memberip | mode

• discoveryperiod  Set the redundancy discovery interval.
  – <1060>  discovery time in secs (default is 30)

• enable  Enable redundancy protocol.
ProCurve Wireless Services zl Module Command Line Reference
GlobalCommands

• **groupid** Set the redundancy group id
  – `<165535>` Redundancy group Id

• **handlestp** Delay the redundancy protocol state machine exec, considering STP
  – **enable** Set handlestp to true

• **heartbeatperiod** Set the redundancy heartbeat interval.
  – `<1255>` heartbeat interval in secs (default is 5)

• **holdperiod** Set the redundancy hold interval.
  – `<10255>` hold interval in secs (default is 15)

• **interfaceip** Set redundancy interface IP address
  – `A.B.C.D` IP address of the wireless module

• **manualrevert** Revert standby to nonactive mode

• **memberip** Add member to this redundancy group
  – `A.B.C.D` IP address of the member

• **mode** set the redundancy mode
  – **active** mode can be active
  – **standby** mode can be standby

**Default Setting**

N/A

**Command Mode**

Global

**Example**

```
HPswitch#configure
HPswitch(config)#redundancy interfaceip 10.10.1.20
HPswitch(config)#redundancy memberip 10.10.1.21
HPswitch(config)#redundancy mode active
HPswitch(config)#redundancy holdperiod 20
HPswitch(config)#redundancy groupid 50
HPswitch(config)#redundancy handlestp enable
HPswitch(config)#redundancy discoveryperiod 10
HPswitch(config)#redundancy holdperiod 10
HPswitch(config)#
```

**Related Commands**

show redundancy (page A-148)
service

This command enables user to control the use of network services.

Syntax

service {dhcp | ftp | no | radius}

- dhcp  Enable the DHCP Server service
- ftp   Configure FTP Server
  - enable  Enable FTP Server
  - password  Configure FTP password
    + 0  Password is specified UNENCRYPTED
    - LINE  Password
    + 1  Password is encrypted with SHA1 algorithm
    - LINE  Password
    ++ LINE  Password
  - rootdir  Configure FTP root dir
    + DIR  Root dir of the FTP server
- no    Negate a command or set its defaults
  - ftp  Configure FTP Server
    + enable  Disable FTP Server
- radius  Enable radius server
  - restart  Restart the radius server with updated configuration

Default Setting

N/A

Command Mode

Global

Example

```
HPswitch# service dhcp
```

sflow

This command configures or unclaims an sflow sampling receiver.

Syntax

sflow (<13>)
• <13> Select one of three possible sFlow receiver tables
  – destination IP address of sFlow collector/management station
    + A.B.C.D IP address (e.g. 10.0.0.1)
      -- 80211toethernet Sampled interfaces will emulate Ethernet interfaces for sFlow collectors and management applications that don’t support the sFlow 802.11 extension
      -- <165535> UDP application port of sFlow collector/management station
      +++ 80211toethernet Sampled interfaces will emulate Ethernet interfaces for sFlow collectors and management applications that don’t support the sFlow 802.11 extension
  – polling Specify the radios for which packets are to be pollied
    + <11000> A single radio index
      -- 0 Disable polling
      -- <2065535> Specify the maximum interval (seconds) between polling of counters
    + RADIO A list (eg: 1,3,7) or range (eg: 37) of radio indices
      -- 0 Disable polling
      -- <2065535> Specify the maximum interval (seconds) between polling of counters
  – sampling Specify the radios for which packets are to be sampled
    + <11000> A single radio index
      -- 0 Disable sampling
      -- <5065535> Specify N, where 1/N is the number of packets sampled
    + RADIO A list (eg: 1,3,7) or range (eg: 37) of radio indices
      -- 0 Disable sampling
      -- <5065535> Specify N, where 1/N is the number of packets sampled

Default Setting
N/A

Command Mode
Global
Example

HPswitch#sflow <13> destination A.B.C.D 80211toethernet
HPswitch

show

This command shows running system information.

Syntax

display (access-list | aclstats | alarm-log | commands | crypto | debug | dhcp | file | flash | ftp | history | hostname | interfaces | ip | layer3-mobility | ldap | licenses | logging | mac | management | ntp | password-encryption | privilige | radius | redundancy-group | redundancy-history | redundancy-members | running-config | securitymgr | sflow | snmp | snmp-server | startup-config | terminal | time | timezone | upd-server | upgrade-status | users | version | vlans | wireless | wlan-acl)

- **access-list** Internet Protocol (IP)
  - <199> IP standard access list
  - <100199> IP extended access list
  - <13001999> IP standard access list (expanded range)
  - <20002699> IP extended access list (expanded range)
- **WORD** Name of ACL
- **radius** IDM/Radius Assigned
  + MAC Specify the user mac in AA-BB-CC-DD-EE-FF format
    - detail Details of all the IDM/Radius assigned attributes
- **aclstats** Show ACL Statistics information
  - **IFNAME** Interface Name
  - **vlan** Vlan Interface
  + <14094> Vlan Id
- **alarm-log** Display all alarms currently in the system
  - <165535> Display details for specific alarm id
  - acknowledged Display acknowledged alarms currently in the system
  - all Display all alarms currently in the system
  - count Display count of alarms currently in the system
  - new Display new alarms currently in the system
  - severitytolimit Display all alarms having specified or higher severity
    + critical Display all critical alarms
    + informational Display all informational or higher severity alarms
    + major Display all major or higher severity alarms
+ **normal**  Display all normal or higher severity alarms
+ **warning**  Display all warning or higher severity alarms

- **commands**  Show command lists
- **crypto**  encryption module
  - **ipssec**  Show IPSEC policy
  + **sa**  IPSec Security Association
  + **securityassociation**  securityassociation
    - **lifetime**  lifetime
  + **transformset**  transformset
    - **WORD**  transform set name or all transform sets
  - **isakmp**  Show ISAKMP
  + **policy**  policy
    - **<110000>**  priorityall isakmp policies
  + **sa**  All Crypto ISAKMP Security Association
  - **key**  Authentication key management
    + **mypubkey**  Show public keys associated with the switch
      - **rsa**  Show Rsa public keys
  - **map**  Crypto maps
    + **interface**  Crypto maps for an interface.
      - **WORD**  interface name
    + **tag**  Crypto maps with a given tag
      - **WORD**  crypto map name
  - **pki**  Public Key Infrastructure commands
    + **request**  Show certificate request
      - **WORD**  Trustpoint Name
    + **trustpoints**  Show trustpoints configured and configuration

- **debug**  Display debugging setting
- **dhcp**  DHCP Server Configuration
  - **config**  Display DHCP Server configuration
  - **status**  Display whether DHCP Server is running or not

- **file**  Display filesystem information
  - **information**  Display file information
    + **FILE**  Display information on FILE
  - **systems**  List filesystems

- **flash**  Display boot status.
- **ftp**  Display FTP Server configuration
- **history**  Display the session command history
• **hostname**  Display system's network name

• **interfaces**  Interface status and configuration
  – **IFNAME**  Interface name
  – **dnlink**  Dnlink Interface
  – **tunnel**  Tunnel Interface
    + **132**  Tunnel Id
  – **uplink**  Uplink Interface
  – **vlan**  Vlan Interface
    + **14094**  Vlan Id

• **ip**  Internet Protocol (IP)
  – **accessgroup**  Display ACLs attached to an interface
    + **IFNAME**  Interface name
    + **dnlink**  Ethernet Interface Id
    + **uplink**  Ethernet Interface
    + **vlan**  Vlan Interface
      - **14094**  Vlan Id
  – **access-list**  List IP access lists
  – **arp**  Address Resolution Protocol (ARP)
  – **ddns**  DDNS Configuration
    + **binding**  DNS Address bindings
  – **dhcp**  DHCP Server Configuration
    + **binding**  DHCP Address bindings
    + **pool**  DHCP Pools
      - **WORD**  DHCP pool name
  – **dhcpvendoroptions**  DHCP Option 43 parameters received from DHCP server
  – **dns**  DNS nameservers
  – **domain**  Default domain for DNS
  – **interface**  IP interface status and configuration
    + **IFNAME**  Interface name
    + **tunnel**  Tunnel Interface
      - **132**  Tunnel Id
    + **vlan**  Vlan Interface
      - **14094**  Vlan Id
  – **nat**  Network Address Translation (NAT)
    + **interfaces**  NAT Configuration on Interfaces
    + **translations**  NAT translations
      - **inside**  Inside
        ++ **destination**  Destination
++ source  Source
- outside  Outside
++ destination  Destination
++ source  Source
- verbose  NAT Translations in realtime
- route  IP routing table
  + A.B.C.D  Network in the IP routing table to display
  + A.B.C.D/M  IP prefix /, e.g., 35.0.0.0/8
  + detail  IP routing table in detail
- routing  IP routing status
- secure-web-management  Secured web server
- telnet  Telnet server
- webmanagement  Web server
• layer3-mobility  Display Mobility parameters
  - eventlog  Event Log
    + peer  Peer eventlogs
    + station  Mobileunit eventlogs
  - forwarding  Stations in the Forwarding Plane
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
  - global  Global Mobility parameters
  - peer  Mobility peers
    + A.B.C.D  IP address of Peer
    + detail  Detailed information display
  - station  Stations in the Mobility Database
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
    + detail  Detailed information display
  - statistics  Mobility statistics
    + AA-BB-CC-DD-EE-FF  MAC address of the Station
• ldap  LDAP server
  - configuration  LDAP server configuration parameters
    + primary  primary LDAP server
    + secondary  secondary LDAP server
• licenses  Installed licenses
  - uninstalled  uninstalled licenses
• logging  Show logging configuration and buffer
• mac  Media Access Control
  - accesslist  List MAC access lists
• management  Display L3 Managment Interface name
• ntp  Network time protocol
  – associations  NTP associations
    + detail  Show detail
  – status  NTP Status
• password-encryption  password encryption
  – status  Display password encryption status
• privilege  Show current privilege level
• radius  RADIUS configuration commands
  – configuration  radius server configuration parameters
  – eap  Eap parameters
    + configuration  Eap configuration
  – group  Radius group configuration
    + WORD  Existing radius group in the local radius database
  – nas  client information
    + A.B.C.D/M  client ip address / mask
  – proxy  proxy information
    + WORD  proxy realm name
  – raduser  Radius user information
    + WORD  Existing User name in the local radius database
  – trustpoint  Radius trustpoint configuration
  – config  Display configured redundancy group information.
• redundancy-group  Display redundancy group parameters
  – runtime  Display runtime redundancy group information.
• redundancy-history  Display state transition history of the wireless module.
• redundancy-members  Display redundancy group members in detail
  – A.B.C.D  IP address of member module
  – brief  Display members in brief
• running-config  Current Operating configuration
  – includefactory  Include Factory Defaults
• securitymgr  Securitymgr parameters
  – eventlogs  Display securitymgr event logs
• sflow  Display sFlow parameters
  – <16>  Select one of six possible sFlow receiver tables
    + destination  Displays information about the collector/management station to which the sampling/polling data is sent
    + sampling/polling  Displays information about sampling and polling
  – - <11000>  A single radio index
GlobalCommands

- **RADIO**  A list (eg: 1,3,7) or range (eg: 37) of radio indices
  - **agent**  Displays readonly agent information

- **snmp**  Display SNMP engine parameters
  - **user**  snmp user to show
    - **manager**  show manager info
    - **operator**  show operator info
    - **snmptrap**  show trap info

- **snmp-server**  Display SNMP engine parameters
  - **traps**  Display Trap enable flags
    - **wireless-statistics**  Display wirelessstats rate traps
      - **radio**  Display radio rate traps
      - **station**  Display station rate traps
      - **wireless-module**  Display wirelessmodule rate traps
      - **wlan**  Display wlan rate traps

- **startup-config**  Contents of startup configuration

- **terminal**  Display terminal configuration parameters

- **time**  Display system clock

- **timezone**  Display timezone

- **upd-server**  Display update server parameters.

- **upgrade-status**  Display last image upgrade status
  - **detail**  Last image upgrade log

- **users**  Display information about terminal lines

- **version**  Display software & hardware version
  - **verbose**  Display software & hardware details

- **vlans**  VLAN Information

- **wireless**  Wireless configuration commands
  - **ap-detection-config**  DetectedAP Configuration Parameters
  - **approve-daps**  Approved APs seen by radioport scans
  - **channel-power**  List of available channel and power levels for a radio
    + **11a**  radio is of type 802.11a
      - **indoor**  radio is placed indoor
      - **outdoor**  radio is placed outdoor
    + **11bg**  radio is of type 802.11bg
      - **indoor**  radio is placed indoor
      - **outdoor**  radio is placed outdoor
  - **config**  Wireless Configuration Parameters
  - **ids**  Intrusion detection parameters
+ filterlist  Display the list of currently filtered stations

- macauthlocal  list out the macauthlocal entries
+ <11000>  macauthlocal entry to display

- multicast-packet-limit  multicastpacketlimit

- phrase-to-key  display the WEP keys generated by a passphrase
+ wep128  display WEP128 keys
  - LINE  the passphrase (between 4 and 32 characters)
+ wep64  display WEP64 keys
  - LINE  the passphrase (between 4 and 32 characters)

- qos-mapping  Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags
+ wired-to-wireless  Mappings used when traffic is switched from wired to the wireless side
  + wireless-to-wired  Mappings used when traffic is switched from wireless to the wired side

- radio  Radio related commands
+ beacon-table  The RadiotoRadio beacon table
+ config  Radio configuration
  - <11000>  A single radio index
  - default11a  default 11a configuration template
  - default11bg  default 11bg configuration template
+ monitor-table  The RadiotoRadio monitoring table
+ statistics  Radio statistics
  - <11000>  A single radio index <11000>
    ++ detail  Detailed radio statistics
+ unadopted  List of unadopted radios

- radio-status  Status of all radios that are adopted or in the process of adoption
  + <11000>  A single radio index

- regulatory  Regulatory (allowed channel/power) information for a particular country
  + ae  United Arab Emirates
  + ar  Argentina
  + at  Austria
  + au  Australia
  + ba  Bosnia Herzegovina
  + be  Belgium
  + bg  Bulgaria
+ bh  Bahrain
+ bm  Bermuda
+ br  Brazil
+ bs  Bahamas
+ by  Belarus
+ ca  Canada
+ ch  Switzerland
+ cl  Chile
+ cn  China
+ co  Colombia
+ cr  Costa Rica
+ cy  Cyprus
+ cz  Czech Republic
+ de  Germany
+ dk  Denmark
+ do  Dominican Republic
+ ec  Ecuador
+ ee  Estonia
+ eg  Egypt
+ es  Spain
+ fi  Finland
+ fr  France
+ gb  United Kingdom
+ gr  Greece
+ gt  Guatemala
+ gu  Guam
+ hk  Hong Kong
+ hn  Honduras
+ hr  Croatia
+ ht  Haiti
+ hu  Hungary
+ id  Indonesia
+ ie  Ireland
+ il  Israel
+ in  India
+ is  Iceland
+ it  Italy
+ jo  Jordan
+ jp  Japan
+ kr  South Korea
+ kw  Kuwait
+ kz  Kazakhstan
+ li  Liechtenstein
+ lk  Sri Lanka
+ lt  Lithuania
+ lu  Luxembourg
+ lv  Latvia
+ ma  Morocco
+ mt  Malta
+ mx  Mexico
+ my  Malaysia
+ nl  Netherlands
+ no  Norway
+ nz  New Zealand
+ om  Oman
+ pe  Peru
+ ph  Philippines
+ pk  Pakistan
+ pl  Poland
+ pt  Portugal
+ qa  Qatar
+ ro  Romania
+ ru  Russia
+ sa  Saudi Arabia
+ se  Sweden
+ sg  Singapore
+ si  Slovenia
+ sk  Slovak Republic
+ th  Thailand
+ tr  Turkey
+ tw  Taiwan
+ ua  Ukraine
+ us  United States
+ uy  Uruguay
+ ve  Venezuela
+ vn  Vietnam
+ za  South Africa
– rp  Status of adopted radioport
  + <148>  The index of the radioport for detailed information
  + AA-BB-CC-DD-EE-FF  The MAC address of a radioport for detailed information
– rpimages  List of radioport images on the wireless module
– rpunadopted  List of unadopted radioport
– selfhealconfig  SelfHealing Configuration Parameters
  + <11000>  A single radio index
  + all  All Configured radios
– station  Details of associated stations
  + <14096>  Index of station
  + AA-BB-CC-DD-EE-FF  MAC address of station
+ radio  Show mobileunits associated to this radio
  - <11000>  A single radio index
+ statistics  station rf statistics
  - AA-BB-CC-DD-EE-FF  MAC address of station
    ++ detail  Detailed station statistics
+ wlan  Show mobileunits associated to this wlan
  - WLAN_RANGE  A wlan index <132>
– stationprobehistory  Display station probehistory
– unapprovedaps  Unapproved APs seen by radioport or station scans
– webauthconfig  Wlan webauth configuration
  + <132>  A wlan index <132>
– wiredwebauth  Wired web authentication
  + clients  Wired web authentication clients
  + config  Wired web authentication configuration parameters
– wirelessmodulestatistics  wirelessmodule statistics
  + detail  Detailed wirelessmodule statistics
– wlan  Wireless LAN related parameters
  + config  Wlan configuration
- `<132>` A wlan index `<132>`  
- `all` All wlans in configuration  
- `enabled` Only wlans that are currently enabled  

**statistics** WLAN statistics  
- `<132>` A wlan index `<132>`  
  + `detail` Detailed wlan statistics  

- **wlan-acl** WLAN based ACLs  
  - `<1-256>` Display ACLs attached to the specified WLAN id  
  - `all` Display ACLs attached to WLAN ports  

Default Setting  
N/A  

Command Mode  
Global  

Example  

```
HPswitch#show accesslist <199>
HPswitch
```

**snmp-server**  
This command modifies the snmp-server parameters. Use the `no` form to remove the specified snmp-server parameters.  

Syntax  
```
snmp-server (community | contact | enable | host | location | manager | user )  
no snmp-server  
```

- **community** - Sets community string and access privileges.  
  - `WORD` - SNMP community string. (private | public)  
    + `restricted` - Read-only access with this community string.  
    + `unrestricted` - Read-write access with this community string.  

- **contact** - Text for MIB object sysContact.  
  - `LINE` - Identification of the contact person for this managed node.  

- **enable** - Enables SNMP traps.  
  - `TRAPS` - Enable SNMP traps.  
    + `cluster` - Enable cluster traps.  
    + `miscellaneous` - Enable miscellaneous traps.
- **lowFsSpace** - Available file system space is lower than the limit.
- **processMaxRestartsReached** - Process has reached max restart.

**nsm** - Enable nsm traps.
- **dhcpIPChanged** - DHCP IP changed.

**snmp** - Enable SNMP traps.
- **authentication** - Enable authentication trap.
- **coldstart** - Enable coldStart trap.
- **linkdown** - Enable linkDown trap.
- **linkup** - Enable linkUp trap.

**upd-server** - Enable upd-server traps.
- **autoInstallInitiated** - Autoinstall request.
- **cfgCkSumMismatch** - Config checksum mismatch.
- **updSvrUnreachable** - Update server unreachable.

**wireless** - Enable wireless traps.
- **ap-detection** - Enable wireless AP detection traps.
  ++ **externalAPDetected** - External AP detected.
- **ids** - Enable wireless IDS traps.
  ++ **excessiveAuthAssociation** - Excessive association authentication.
  ++ **excessiveProbes** - Excessive probes.

**radio** - Enable wireless radio traps.
  ++ **adopted** - Radio adopted.
  ++ **detectedRadar** - Radio detected radar.
  ++ **unadopted** - Radio unadopted.

**self-healing** - Enable self healing traps.
  ++ **activated** - Self healing activated.

**station** - Enable wireless station traps.
  ++ **associated** - Wireless station associated.
  ++ **deniedAssociationAsPortCapacityReached** - Wireless station denied association due to port capacity reached.
  ++ **deniedAssociationOnCapability** - Wireless station denied association due to unsupported capability.
  ++ **deniedAssociationOnErr** - Wireless station denied association due to internal error.
+++deniedAssociationOnInvalidWPAWPA2IE - Wireless station denied association due to invalid/absent WPA/WPA2 IE
+++deniedAssociationOnRates - Wireless station denied association due to incompatible transmission rates.
+++deniedAssociationOnSSID - Wireless station denied association due to invalid SSID.
+++deniedAssociationOnShortPream - Wireless station denied association due to lack of short preamble support.
+++deniedAssociationOnSpectrum - Wireless station denied association due to lack of spectrum management capability.
+++deniedAuthentication - Wireless station denied 802.11 authentication.
+++disassociated - Wireless station disassociated.
+++radiusAuthFailed - Wireless station failed radius authentication.
+++tkipCounterMeasures - TKIP counter measures invoked.

+wireless-statistics - Enable wireless-stats rate traps.
- min-packets - Minimum packets for sending the trap.
  +++<1-65535> - Number of packets in the range <1-65535>.
The following three commands share the rate parameters.
- radio - Modify radio rate traps.
- station - Modify station rate traps.
- wlan - Modify wlan rate traps.
  +++avg-bit-speed-less-than - Average bit speed in Mbps is less than.
  +++avg-retry-greater-than - Average retry is greater than.
  +++avg-signal-less-than - Average signal in dBm is less than.
  +++gave-up-percent-greater-than - Percentage of pkts dropped is greater than.
  +++nu-percent-greater-than - Percentage of non-unicast pkts is greater than.
  +++num-stations-greater-than - Number of associated station is greater than.
  +++pktsps-greater-than - Packets per second is greater than.
  +++put-greater-than - Throughput in Mbps is greater than.
  +++undecrypt-percent-greater-than - Percentage of undecryptable pkts is greater than.
  ++num-stations-greater-than - Number of associated station is greater than.
  ++pktsps-greater-than - Packets per second is greater than.
  ++tput-greater-than - Throughput in Mbps is greater than.

- host - SNMP server host.
  – A.B.C.D - SNMP server host IP address.

- location - Text for MIB object sysLocation.

- manager - Enable SNMP manager.
  – all - Enable SNMP version v2 and v3.
  – v2 - Enable SNMP version v2.
  – v3 - Enable SNMP version v3.

- user - Defines a user who can access SNMP engine.
  – manager - Manager user.
    +v3 - User using v3 security model.
      - auth - Authentication parameters for the user.
        ++md5 - Use HMAC MD5 algorithm for authentication.
          - PASSWD - Authentication password for user.
      - encrypted - Specifying password as md5 digests.
        ++auth - Authentication parameters for the user.
          - md5 - Use HMAC MD5 algorithm for authentication
            +++PASSWD - Authentication password for user.
  – operator - Operator user.
    +v3 - User using v3 security model.
      - auth - Authentication parameters for the user.
        ++md5 - Use HMAC MD5 algorithm for authentication.
          - PASSWD - Authentication password for user.
      - encrypted - Specifying password as md5 digests.
        ++auth - Authentication parameters for the user.
          - md5 - Use HMAC MD5 algorithm for authentication.
            +++PASSWD - Authentication password for user.

Default Setting

SNMP v2: enabled
SNMP v2 community: private rw, public ro, trap ro
SNMP v3: enabled
Command Mode
Global Configuration

Example
HPswitch# configure
HPswitch(config)# snmp-server community private restricted
HPswitch(config)# snmp-server contact Paul
HPswitch(config)# snmp-server location 2F R19

Related Commands
show snmp (page A-154)

spanning-tree
This command enable spanning tree commands.

Syntax
spanning-tree (mst)
• mst - Multiple spanning tree.
  – configuration Configuration

Default Setting
Disabled

Command Mode
Global Configuration

Example
HPswitch# spanning-tree mst configuration
HPswitch(config-mst)#

time
This command configures time parameters.

Syntax
time
• HH:MM:SS - Current Time (in military format hours, minutes, and seconds).
timezone

This command configures timezone parameters. The no command negates this configuration.

Syntax

```
timezone (TIMEZONE)
no timezone
```

- **TIMEZONE** - File containing the timezone.
  
Enter <tab> to traverse through a list of files.

Default Setting

N/A

Command Mode

Global Configuration

Example

```
HPswitch# configure
HPswitch(config)# time 20:32:26
HPswitch(config)#
```

Related Commands

show timezone (page A-159)
upd-server

This command configures autoinstall update server parameters. The no command negates this configuration.

Syntax

updserver (cfgfileloc | clustercfgfile | forceCfgDownload | imgfileloc | ip | unreachable)

- **cfgfileloc**  Set config file location
  - **WORD**  Config file location
- **clustercfgfile**  Set cluster config file location
  - **WORD**  Config file location
- **forceCfgDownload**  Force the config update bypassing the checksum validation
- **imgfileloc**  Set Image file location
  - **WORD**  Path of the Image file on ftp/tftp server
    - **imgfilever**  Version of the image file
      - **WORD**  Version string
- **ip**  server ipaddress
  - **A.B.C.D**  ipaddress in A.B.C.D format
    + **protocol**  autoinstall server protocol
      - **ftp**  FTP protocol
        ++ **username**  server username
          -- **WORD**  username if applicable
        +++ **passwd**  server password
          --- **WORD**  password if applicable
      - **tftp**  TFTP protocol
- **unreachable**  Set update server reachability

Default Setting

N/A

Command Mode

Support

Example

```
HPswitch#configure
HPswitch(config)#updserver imgfileloc tftp imgfilever 2
HPswitch(config)#
```
Related Commands

show upd-server (page A-159)

username

This command enables user name authentication.

Syntax

username \( \text{WORD} \)

- \text{access} \ Set the user access mode
  - \text{console} \ Only allowed from console
  - \text{web} \ Only allowed from applet (webUI)
- \text{password} \ Specify the password for the user
  - \text{0} \ Password is specified UNENCRYPTED
    - \text{ LINE} \ User password (plaintext password length should be between 8 and 32 characters)
  - \text{1} \ Password is encrypted with SHA1 algorithm
    - \text{ LINE} \ User password (plaintext password length should be between 8 and 32 characters)
  - \text{LINE} \ User password (plaintext password length should be between 8 and 32 characters)
- \text{privilege} \ Set user access privilege
  - \text{helpdesk} \ Helpdesk (troubleshooting) access
  - \text{monitor} \ Monitor (readonly) access
  - \text{nwadmin} \ Network (wired & wireless) admin access
  - \text{superuser} \ Superuser (root) access
  - \text{sysadmin} \ System (general system configuration) admin access
  - \text{webadmin} \ Web auth (hotspot) user admin access

Default Setting

N/A

Command Mode

Global
Example

HPswitch#username WORD access console
HPswitch

wireless

This command accesses the wireless context. This section does not detail the commands in the wireless context, refer to the Wireless Context Command Section.

Syntax

wireless

Default Setting

N/A

Command Mode

Global Configuration

Example

HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#

wlan-acl

This command enable spanning tree commands.

Syntax

wlan-acl <1-256>
  • <1-256> - WLAN index.

Default Setting

Disabled

Command Mode

Global Configuration
Interface Commands

These commands are used to configure the Interface Context commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] description</td>
<td>(Negates) Interface specific description.</td>
<td>A-105</td>
</tr>
<tr>
<td>end</td>
<td>Detailed in Global Command Section.</td>
<td>A-64</td>
</tr>
<tr>
<td>exit</td>
<td>Detailed in Manager Command Section.</td>
<td>A-8</td>
</tr>
<tr>
<td>help</td>
<td>Detailed in Manager Command Section.</td>
<td>A-23</td>
</tr>
<tr>
<td>[no] ip</td>
<td>(Negates) Sets the IP address of the interface.</td>
<td>A-106</td>
</tr>
<tr>
<td>logout</td>
<td>Detailed in Manager Command Section.</td>
<td>A-23</td>
</tr>
<tr>
<td>management</td>
<td>Sets current interface as Management Interface.</td>
<td>A-107</td>
</tr>
<tr>
<td>[no] mtu</td>
<td>(Negates) Sets mtu value for vlan interface.</td>
<td>A-107</td>
</tr>
<tr>
<td>show</td>
<td>Detailed in Show Command Section.</td>
<td>A-128</td>
</tr>
<tr>
<td>support</td>
<td>Detailed in Support Command Section.</td>
<td>A-185</td>
</tr>
</tbody>
</table>

**description (interface)**

This command configures a description for the interface. The no command negates this configuration.

**Syntax**

```
description (LINE ) 
no description
```

- **LINE** - Characters describing this interface.

**Default Setting**

N/A
**Command Mode**

Interface Configuration

**Example**

```bash
HPswitch# configure
HPswitch(config)# interface vlan1
HPswitch(config-if)# description EXAMDES
HPswitch(config-if)#
```

**Related Commands**

show interfaces (page A-138)

**ip (interface)**

This command configures ip parameters of the interface. The no command negates this configuration.

**Syntax**

```
ip (address)
no ip address
```

- **address** - Configures an internet protocol address of an interface.
  - `A.B.C.D/M` - IP address (e.g. 10.0.0.1/8).
  - `dhcp` - Use DHCP Client to obtain IP address for this interface.

**Default Setting**

unassigned (DHCP)

**Command Mode**

Interface Configuration

**Example**

```bash
HPswitch# configure
HPswitch(config)# interface vlan1
HPswitch(config-if)# ip 10.0.0.1/4
HPswitch(config-if)#
```

**Related Commands**

show ip interface (page A-139)
management

This command configures the selected interface as the management interface.

**Syntax**

```plaintext
management
```

**Default Setting**

N/A

**Command Mode**

Interface Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#interface vlan1
HPswitch(config-if)#management
```

**Related Commands**

- `show management` (page A-144)

**mtu**

This command sets the mtu value for the vlan interface.

**Syntax**

```plaintext
mtu (<512-1500>)
```

- `<512-1500>` - MTU in bytes.

**Default Setting**

N/A

**Command Mode**

Interface Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#interface vlan1
HPswitch(config-if)#mtu 600
```

A-107
## Wireless Commands

These commands are used to configure the Wireless Context commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] advanced-config</td>
<td>(Negates) Enables advanced configuration.</td>
<td>A-110</td>
</tr>
<tr>
<td>[no] ap-detection</td>
<td>(Negates) Configures neighboring access point detection.</td>
<td>A-110</td>
</tr>
<tr>
<td>[no] dot11-shared-key-auth</td>
<td>(Negates) Enables support for 802.11 shared key authentication.</td>
<td>A-112</td>
</tr>
<tr>
<td>end</td>
<td>Detailed in Global Command Section.</td>
<td>A-64</td>
</tr>
<tr>
<td>exit</td>
<td>Detailed in Manager Command Section.</td>
<td>A-8</td>
</tr>
<tr>
<td>help</td>
<td>Detailed in Manager Command Section</td>
<td>A-23</td>
</tr>
<tr>
<td>ids</td>
<td>Intrusion detection configuration commands.</td>
<td>A-112</td>
</tr>
<tr>
<td>logout</td>
<td>Detailed in Manager Command Section</td>
<td>A-23</td>
</tr>
<tr>
<td>[no] mac-auth-local</td>
<td>(Negates) Establishes local mac authentication list.</td>
<td>A-113</td>
</tr>
<tr>
<td>[no] proxy-arp</td>
<td>(Negates) Responds to ARP requests from the RON to WLAN on behalf of stations.</td>
<td>A-114</td>
</tr>
<tr>
<td>show</td>
<td>Detailed in Show Command Section</td>
<td>A-128</td>
</tr>
<tr>
<td>support</td>
<td>Detailed in Support Command Section</td>
<td>A-185</td>
</tr>
<tr>
<td>[no] wlan</td>
<td>(Negates) WLAN configuration commands.</td>
<td>A-120</td>
</tr>
<tr>
<td>[no] wlan-prioritization</td>
<td>(Negates) Use wlan priority weights to determine packet queueing order.</td>
<td>A-127</td>
</tr>
</tbody>
</table>
adopt-unconf-radio

This command adopts a radio even if its not yet configured. The default templates are used for configuration. The no command negates this configuration.

Syntax

```
adopt-unconf-radio (enable)

no adopt-unconf-radio enable

• enable - Enables the adoption of unconfigured radios.
```

Default Setting

N/A

Command Mode

Wireless Configuration

Example

```
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#adopt-unconf-radio enable
HPswitch(config-wireless)#
```

adoption-pref-id

This command configures a preference identifier for this wireless module. All radios configured with this preference identifier are more likely to be adopted by this blade. The no command negates this configuration.

Syntax

```
adoption-pref-id

no adoption-pref-id

• <1-65535> - Assign the ID.
```

Default Setting

N/A

Command Mode

Wireless Configuration
Example

```
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#adoption-pref-id 600
HPswitch(config-wireless)#
```

**advanced-config**

This command allows advanced configuration of wlan settings. The no command negates this configuration.

**Syntax**

```
advanced-config
no advanced-config
```

• **enable** - Enables support for the advanced configuration.

**Default Setting**

Disabled

**Command Mode**

Wireless Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#advanced-config enable
HPswitch(config-wireless)#
```

**Related Commands**

show running-config (page A-151)

**ap-detection**

This command configures the periodic detection of nearby access points. The no command disables ap-detection.

**Syntax**

```
ap-detection (approved | enable | max-aps | timeout )
no ap-detection
```

• **approved** - Configures the approved detection list.
- **add** - Add an entry to the approved AP list.
  +<1-200> - Index where this approved entry will be added: <1-200>.

- **MAC** - MAC address in AA-BB-CC-DD-EE-FF format.
  ++**LINE** - A string of up to 32 characters.
  ++**any** - Any SSID.

- **any** - Any MAC address.
  ++**LINE** - A string of up to 32 characters.
  ++**any** - Any SSID.

- **enable** - Allow radio-ports to look for APs.

- **max-aps** - The maximum amount of entries unapproved-seen and approved-seen can show.
  - <1-1000> - Number of entries between 1 and 1000.

- **timeout** - The amount of seconds a AP will remain in the list after it is no longer seen.
  - <1-65535> - Number of seconds between 1 and 65535.

**Default Setting**

Disabled

**Command Mode**

Wireless Configuration

**Example**

```
HPswitch# configure
HPswitch(config)# wireless
HPswitch(config-wireless)# ap-detection approved add 2 any any
HPswitch(config-wireless)# ap-detection enable
HPswitch(config-wireless)# ap-detection timeout 65
HPswitch(config-wireless)# ap-detection max-aps 200
HPswitch(config-wireless)#
```

**Related Commands**

show wireless ap-detection-config (page A-164)
dot11-shared-key-auth

This command enables support for 802.11 shared key authentication. The no command negates the support.

NOTE

Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accommodate wireless stations that are unable to carry out Open-System authentication.

Syntax

```plaintext
dot11-shared-key-auth (enable)
no dot11-shared-key-auth

• enable - Enables support for shared key authentication.
```

Default Setting

N/A

Command Mode

Wireless Configuration

Example

```plaintext
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#dot11-shared-key-auth enable
```

ids

This command configures the Intrusion Detection configuration commands. The no command negates the configuration.

Syntax

```plaintext
ids (excessive-associations | excessive-probes | filter-ageout)
no ids

• excessive-associations - Monitors the number of association requests from stations.
  – <0-65535> - Maximum number of association requests per second.

• excessive-probes - Monitors the number of probe requests from stations.
  – <0-65535> - Maximum number of association requests per second.
```
• **filter-ageout** - Set the number of seconds to filter a station that
  set off IDS.
  – `<0-65535>` - Time in seconds.

**Default Setting**

N/A

**Command Mode**

Wireless Configuration

**Example**

```
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#ids excessive-associations 500
HPswitch(config-wireless)#ids excessive-probes 400
HPswitch(config-wireless)#ids filter ageout 40
HPswitch(config-wireless)#
```

**Related Commands**

show wireless ids (page A-168)

**mac-auth-local**

This command configures the local MAC authentication list. The no command
disables the configuration.

**Syntax**

```
mac-auth-local
no mac-auth-local
```

• `<1-1000>` - MAC Auth local entry.
  – **allow** - Allow stations that match this rule to associate.
    - **MAC** - Starting MAC address in AA-BB-CC-DD-EE-FF format.
    - **MAC** - Ending MAC address in AA-BB-CC-DD-EE-FF format.
    - **+WORD** - A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices.
  – **deny** - Deny stations that match this rule to associate.
    - **MAC** - Starting MAC address in AA-BB-CC-DD-EE-FF format.
    - **MAC** - Ending MAC address in AA-BB-CC-DD-EE-FF format.
    - **+WORD** - A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices.

**Default Setting**

Disabled
proxy-arp

This command responds to ARP requests from the RON to WLAN on behalf of stations. The no command disables the support for the proxy-arp response.

**Syntax**

```plaintext
proxy-arp (enable)
no proxy-arp enable
```

- **enable**: Enables support for proxy arp.

**Default Setting**

N/A

**Command Mode**

Wireless Configuration

**Example**

```plaintext
HPswitch(config)#proxy-arp enable
HPswitch(config)#
```
radio

This command configures the radio parameters. The no command negates the radio parameter configuration.

**Note**

To configure many of the radio parameters, you must first configure the country code. See country code.

**Syntax**

```
radio ( <1-1000> | RADIO | add | all-11a | all-11bg | configure-8021X | default-11a | default-11bg )
no radio
```

- `<1-1000>` - A single radio index.
- `RADIO` - A list (eg: 1,3,7) or range (eg: 3-7) of radio indices.
- `all-11a` - All 11a radios currently in configuration.
- `all-11bg` - All 11bg radios currently in configuration.
- `default-11a` - Default 11a configuration template.
- `default-11bg` - Default 11bg configuration template.

The radio commands share the following parameters:

- `adoption-pref-id` - A preference identifier for this radio port. The radio port is more likely to be adopted by a wireless module that is its preferred wireless module.
  + `<1-65535>` - The ID.
- `antenna-mode` - Antenna diversity mode.
  + `diversity` - Full Diversity (both antennas).
  + `primary` - Primary Antenna only.
  + `secondary` - Secondary Antenna only.
- `beacon-interval` - Beacon interval in K-uSec.
  + `<50-200>` - Beacon interval in milliSeconds.
- `bss` - Map wireless LANs to radio BSSIDs.
  + `<1-4>` - The BSS where wireless LANs will be mapped.
  - `WLAN` - A list (eg: 1,3,7) or range (eg: 3-7) of WLAN indices.
    When a BSS is also specified, the first WLAN will be used as the primary WLAN. When the auto option is used, the system will automatically assign the first four WLANs as primaries on their respective BSS.
  + `auto` - Automatic assignment of BSS. The user selects wireless LANs, and the system assigns them to a BSS automatically.
- **WLAN** - A list (eg: 1,3,7) or range (eg: 3-7) of WLAN indices. When a BSS is also specified, the first WLAN will be used as the primary WLAN. When the auto option is used, the system will automatically assign the first four WLANs as primaries on their respective BSS.

  - **channel-power** - Location, channel and transmit power level.
  + **indoor** - Indoor location.
  + **outdoor** - Outdoor location.

The indoor and outdoor parameters share these parameters:

- **<1-200>** - Channel number.
  ++ **<4-20>** - Power in dBm.
- **acs** - Auto channel selection (radio will scan for the least congested channel at startup or reconfiguration).
  ++ **<4-20>** - Power in dBm.
- **random** - Random channel selection.
  ++ **<4-20>** - Power in dBm.

- **copy-config-from** - Copies the configuration from a previously configured radio.
  + **<1-1000>** - A single radio index.
  + **default-11a** - Default 11a configuration template.
  + **default-11bg** - Default 11bg configuration template.
- **detector** - Dedicate this radio as a detector. No stations can associate to a detector.
- **dtim-period** - DTIM period (number of beacons between successive DTIMs).
  + **<1-50>** - DTIM period.
- **max-stations** - Maximum number of stations allowed to associate.
  + **<1-64>** - Number of stations.
- **reset** - Resets a radio (this will only reset the specified radio, not the complete radio-port).
- **reset-rp** - Resets the parent rp (this will reset all radios on that radio-port).
- **rts-threshold** - RTS threshold.
  + **<100-2346>** - RTS threshold in bytes.
- **run-acs** - Runs auto-channel-selection on a radio. The radio should already have been configured for ACS.
- **self-heal-offset** - Configure the self-healing offset for regulatory.
  + **<0-65535>** - The self-heal offset in dB.
- **short-preamble** - Short preamble.
- **speed** - Configures the basic and supported data rates / speed.
Wireless Commands

+ {1,2,5,6,9,11,12,18,24,36,48,54} - Mbps.

– + {basic1,basic2,basic5,5,basic6,basic9,basic11,basic12,basic18,basic24,basic36,basic48,basic54} - Mbps.

+ default - Factory default rates based on radio-type.

+ range - All rates enabled, the lowest one set to basic.

+ throughput - All rates basic (note: only g clients allowed on 11bg.

– wmm - 802.11e / Wireless MultiMedia parameters.

+ background - Background traffic [DSCP: 0x08, 0x10] [802.1d: 1, 2]

+ best effort - Best effort traffic [DSCP: 0x00, 0x18] [802.1d: 0, 3]

+ video - Video Traffic [DSCP: 0x20, 0x28] [802.1d: 4, 5]

+ voice - Voice Traffic [DSCP: 0x30, 0x38] [802.1d: 6, 7]

The background, best effort, voice, and video share these parameters:

- aifsn - Arbitration Inter Frame Spacing Number: the wait time in milliseconds between data frames is derived using AIFSN and the slot-time.

  +<1-15> - The Arbitration Inter Frame Spacing Number.

- burst - Transmit-opportunity: an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium.

  +<0-65535> - The transmit-opportunity in 32 microSecond units.

- cw - Contention Window parameters: wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window.

  +<0-15> - cwMin: The minimum contention window. The actual value used is \((2^{cwMin} - 1)\).

  -<0-15> - cwMax: The maximum contention window. The actual value used is \((2^{cwMax} - 1)\).

- add - Adds a new radio.

  – <1-1000> - Index where this radio is to be added.

  +<MAC> - Mac address in AA-BB-CC-DD-EE-FF format.

  -11a - 802.11a type radio.

  -11bg - 802.11bg type radio.

- configure-8021X - Configures 802.1X username and password onto all currently adopted radio-ports.

  – username - Specify the 802.1X username the radio-port must use.
+**WORD** - 802.1X username.

-**password** - Specify the 802.1X password the radio-port must use.

++**WORD** - 802.1X password.

**Default Setting**

Disabled

**Command Mode**

Wireless Configuration

**Examples**

```
HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#radio 1 adoption-pref-id 5

HPswitch(config-wireless)#radio 1 antenna-mode diversity

HPswitch(config-wireless)#radio 1 beacon-interval 50

HPswitch(config-wireless)#radio 1 channel-power indoor acs 10

Regulatory parameter values depend on country of operation and radio type. Refer to documentation for more regulatory information.

HPswitch(config-wireless)#radio 2 copy config-from default-11a

HPswitch(config-wireless)#radio 1 max-stations 64

HPswitch(config-wireless)#radio 1 wmm background cw 3 5

HPswitch(config-wireless)#radio add 5 A1-B2-C3-D4-E5-F6 11bg

HPswitch(config-wireless)#radio configure-8021X username manager password simple
```

**Related Commands**

show wireless radio statistics (page A-171)
self-heal

This command configures the self-healing commands. The no command negates the configuration.

Syntax

self-heal (interference-avoidance| neighbor-recovery)
no self-heal

- **interference-avoidance** - Interference Avoidance configuration.
  - **enable** - Enables/disables interference avoidance.
  - **hold-time** - The number of seconds to disable interference avoidance after a detection. This prevents a radio from changing channels continuously.
    + **<0-65535>** - A number of seconds between 0-65535.
  - **retries** - The average number retries to cause a radio to re-run auto channel selection.
    + **Number** - A decimal number between 0.0 and 15.0.

- **neighbor-recovery** - Neighbor recovery configuration commands.
  - **action** - Radios self-healing action when neighbors are detected down.
    + **both** - Raise the power to max and open all rates.
    + **none** - Do nothing.
    + **open-rates** - Open all rates.
    + **raise-power** - Raise the power to max.
  - **enable** - Monitor radio-ports and attempt to increase coverage on failure.
  - **neighbors** - Add radios as neighbors.
    + **<1-1000>** - A single radio index.
    - **<1-1000>** - A single radio index.
  - **run-neighbor-detect** - Disassociate all stations, clear current neighbors and run neighbor detection.

Default Setting

N/A

Command Mode

Wireless Configuration
ProCurve Wireless Services zl Module Command Line Reference

Wireless Commands

Example

HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#self-heal interference-avoidance enable
HPswitch(config-wireless)#self-heal neighbor-recovery enable
HPswitch(config-wireless)#self-heal neighbor-recovery neighbors 5 5
HPswitch(config-wireless)#self-heal neighbor-recovery run-neighbor-detect
HPswitch(config-wireless)#

Related Commands

show wireless self-heal-config (page A-178)

wlan

This command configures the wireless LAN parameters. The no command negates the WLAN parameter configuration.

Syntax

wlan (<1-32> | WLAN )
no wlan

• <1-1000> - A single WLAN index.
• WLAN - A list (eg: 1,3,7) or range (eg: 3-7) of WLAN indices.

The radio (<1-1000> | WLAN ) commands share the following parameters:

- authentication-type - The authentication type of this WLAN.
  +eap - EAP authentication (802.1X).
  +none - None / pre-shared keys.
  +web-auth - Web based authentication (Note: encryption-type will be changed to none).
- closed-system - Hides the SSID in beacons, and doesn't respond to probes for broadcast ESS on this WLAN.
- description - The description of this WLAN.
  +LINE - A string of up to 20 characters.
- dot11i - Configures IEEE 802.11i (TKIP/AES) parameters.
  +key - Configures the key (PMK).
    -0 - Password is specified UNENCRYPTED.
    ++WORD - The 256 bit (64 hex characters) long key.
-2 - Password is encrypted with password-encryption secret.
++WORD - The 256 bit (64 hex characters) long key.
-WORD - The 256 bit (64 hex characters) long key.
+key-rotation - Controls the periodic update of the broadcast keys of all associated stations.
-enable - Enables key rotation.
+key-rotation-interval - Configures the broadcast key rotation interval.
   <60-86400> - The key rotation interval in seconds.
+oo-pmk-caching - Enables the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X).
+phrase - Configures the passphrase.
   - 0 - Password is specified UNENCRYPTED.
   ++LINE - A passphrase between 8 and 63 characters long.
   - 2 - Password is encrypted with password-encryption secret.
   ++LINE - A passphrase between 8 and 63 characters long.
   - LINE - A passphrase between 8 and 63 characters long.
+pmk-caching - Enables the use of cached pairwise master keys (fast roaming with eap/802.1X).
   - enable - Enables specified wireless LAN(s).
   - encryption-type - Enables specified wireless LAN(s).
   +aes - AES Counter Mode CBC-MAC Protocol (CCMP).
   +none - No encryption.
   +tkip - Temporal Key Integrity Protocol (TKIP).
   +tkip-aes - Enables both TKIP and AES on this WLAN.
   +wep128 - Wired Equivalence Privacy (WEP) with 128 bit keys.
   +wep64 - Wired Equivalence Privacy (WEP) with 64 bit keys.

Note

A configuration where two WLANs are mapped to the same VLAN, and one of them is configured with no encryption and the other with WEP, is insecure. It can lead to a compromise of the WEP key.

   - inactivity-timeout - Inactivity timeout in seconds. If a frame is not received from a station for this amount of time, the station is disassociated.
   +<60-86400> - Inactivity timeout in seconds.
   - inter-station-blocking - Prevents station to station traffic on this WLAN.
   - qos - Quality of Service commands.
**+mcast1** - The Egress prioritization multicast mask.
- **MAC** - MAC address in AA-BB-CC-DD-EE-FF format.

**+mcast2** - MAC address in AA-BB-CC-DD-EE-FF format.
- **MAC** - MAC address in AA-BB-CC-DD-EE-FF format.

**+prioritize-voice** - Prioritize voice frames over general data frames (applies non-WMM station).

**+svp** - Support for Spectralink Voice Prioritization.
- **enable** - Enable Spectralink Voice Prioritization support on this WLAN.

**+weight** - The egress weight (relative priority to other WLANs) of this WLAN.
- **<1-10>** - A weight <1-10>.

**+wmm** - 802.11e / Wireless MultiMedia parameters.
- **8021p** - Use 802.1p frame priority (field in the VLAN tag) to determine packet priority.

- **background** - Background traffic [DSCP: 0x08, 0x10] [802.1d: 1, 2]

- **best effort** - Best effort traffic [DSCP: 0x00, 0x18] [802.1d: 0, 3]

- **dscp** - Use DSCP (Differentiated Services Code Point) bits in the IP header to determine packet priority.

- **enable** - Enables 802.11e (Wireless MultiMedia) support on this WLAN.

- **video** - Video Traffic [DSCP: 0x20, 0x28] [802.1d: 4, 5]

- **voice** - Voice Traffic [DSCP: 0x30, 0x38] [802.1d: 6, 7]

The background, best effort, voice, and video share these parameters:

++ **aifsn** - Arbitration Inter Frame Spacing Number: the wait time in milliseconds between data frames is derived using AIFSN and the slot-time.
- **<1-15>** - The Arbitration Inter Frame Spacing Number.

++ **burst** - Transmit-opportunity: an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium.
- **<0-65535>** - The transmit-opportunity in 32 microSecond units.
++cw - Contention Window parameters: wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window.

- - <0-15> - cwMin: The minimum contention window. The actual value used is \(2^{cwMin} - 1\).
  + + + <0-15> - cwMax: The maximum contention window. The actual value used is \(2^{cwMax} - 1\).

++txop-limit - Transmit-opportunity: an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium.

- - <0-65535> - The transmit-opportunity in 32 microSecond units.

– radius - Modify Radius/802.1X related parameters.

+reauth - Enables periodic reauthentication of all associated stations.

-<30-65535> - Reauthentication period in seconds.

+server - Modifies Radius/802.1X server parameters.

-primary - Primary radius server.

-secondary - Primary radius server.

The primary and secondary commands share these parameters:

++A.B.C.D - Radius server IP address.

- - auth-port - Radius server authentication port (default:1812).
  + + + <024-65535> - Radius server authentication port (default:1812).

++radius-key - Radius server shared secret, up to 127 characters.

- - 0 - Password is specified UNENCRYPTED.
  + + + LINE - Radius server shared secret, up to 127 characters.

- - 2 - Password is encrypted with password-encryption secret.
  + + + LINE - Radius server shared secret, up to 127 characters.

- - - LINE - Radius server shared secret, up to 127 characters.
timeout - Time the wireless module waits for a response from the radius server before retrying.
- <1-60> - Timeout in seconds.
  ++retransmit- Number of retries before the wireless module will give up and disassociate the station.
  - - <1-10> - Retry count.
station - Modifies Radius/802.1X supplicant related parameters.
+timeout - Time the wireless module waits for a response from the radius server before retrying.
- <1-60> - Timeout in seconds.
  ++retransmit- Number of retries before the wireless module will give up and disassociate the station.
  - - <1-10> - Retry count.
SSID - The SSID of this WLAN.
+WORD - A string of up to 32 characters.
vlan - The VLAN assignment of this WLAN.
+<1-4094> - A VLAN identifier <1-4094>.
web-auth - Modify web-auth related parameters.
+allow-list - Modify web-auth white list parameters. Users who have not yet authenticated will be allowed access to these IP addresses.
  - <1-10> - Allow-list Rule index (1-10).
  ++A.B.C.D - Allow-list IP address.
radius - Modify web-auth radius server parameters. The parameter extensions are the same as previous listed under “radius - Modify Radius/802.1X related parameters.” on page A-123.
+webpage - Modify web-auth page parameters.
  -external - Modify web-auth External page.
  -internal - Modify web-auth Internal page.

The external and internal commands share these parameters:
  ++failure - Users are redirected to this webpage if they fail authentication.
  ++login - Users are prompted for their username and password on this webpage.
  ++welcome - Users are redirected to this webpage after they authenticate successfully.

The failure/login/welcome parameters share these parameters:
- **description** - Text that is displayed as the main body (normal font, middle of page) of the webpage.
- **footer** - Text that is displayed at the footer (smaller font, bottom section) of the webpage.
- **header** - Text that is displayed as a header (large font, top section) of the webpage.
- **main-logo** - Main image (large size) that will be served up by the local webpage. Appears between the header and description on the webpage.
- **small-logo** - Small image (thumbnail size) that will be served up by the local webpage. Appears near the footer on the webpage.
- **title** - Text that will be the title of the webpage.

**webpage-location** - The location of the web pages to be used for authentication. These pages can either be hosted on the wireless module or on an external web server.

- **external** - Use login/welcome/failure Web pages on an external server.
- **internal** - Use login/welcome/failure Web pages configured on the wireless module.

- **wep128** - Configure WEP128 parameters.
- **wep64** - Configure WEP64 parameters.

The wep128 and wep64 commands share these parameters:

**key** - Configures pre-shared hex keys.

- **<1-4>** - Key index being configured.
  
  **++ascii** - Keys as ascii characters (5 characters for wep64, 13 for wep128).
  
  **++hex** - Keys as ascii characters (5 characters for wep64, 13 for wep128).

The hex and ascii commands share these parameters:

- **-0** - Password is specified UNENCRYPTED.
  
  **+++WORD** - Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128).
  
  **-2** - Password is encrypted with password-encryption secret.
  
  **+++WORD** - Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128).
  
  **-WORD** - Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128).
+phrase - Specify a passphrase from which the keys are to be derived.
+LINE - The passphrase between 4 and 32 characters long.
+web-default-key - Configures the transmit key index.
+<1-4>- The key index to be used for transmission from AP to MU.

Default Setting
Disabled

Command Mode
Wireless Configuration

Examples

HPswitch#configure
HPswitch(config)#wireless
HPswitch(config-wireless)#wlan 1 enable
HPswitch(config-wireless)#wlan 1 ssid SAM
HPswitch(config-wireless)#wlan 1 encryption-type wep128
HPswitch(config-wireless)#wlan 1 authentication-type eap
HPswitch(config-wireless)#wlan 1 closed-system
HPswitch(config-wireless)#wlan 1 qossvp enable
HPswitch(config-wireless)#wlan 1 inter-station-blocking
HPswitch(config-wireless)#wlan 1 wep128 web-default-key 4
HPswitch(config-wireless)

Related Commands
show wireless wlan statistics (page A-183)
wlan-prioritization

This command uses WLAN priority weights to determine packet queueing order. The no command disables this support.

**Syntax**

```
wlan-prioritization (enable)
```

```no wlan-prioritization enable```

- **enable** - Enables prioritization across wireless LANs.

**Default Setting**

N/A

**Command Mode**

Wireless Configuration

**Example**

```
HPswitch# configure
HPswitch(config)# wireless
HPswitch(config-wireless)# wlan-prioritization enable
HPswitch(config-wireless)#
```

**Related Commands**

- show wireless wlan statistics (page A-183)
Show Commands

These commands are common commands used to display configured parameters in all contexts.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td>Displays IP access lists.</td>
<td>A-130</td>
</tr>
<tr>
<td>show aclstats</td>
<td>Displays ACL statistics.</td>
<td>A-130</td>
</tr>
<tr>
<td>show alarm-log</td>
<td>Displays list of alarms occurring since boot.</td>
<td>A-131</td>
</tr>
<tr>
<td>show commands</td>
<td>Shows command lists.</td>
<td>A-132</td>
</tr>
<tr>
<td>show crypto</td>
<td>Displays encryption related commands.</td>
<td>A-133</td>
</tr>
<tr>
<td>show debug</td>
<td>Displays debugging setting.</td>
<td>A-134</td>
</tr>
<tr>
<td>show dhcp</td>
<td>Displays DHCP server information.</td>
<td>A-135</td>
</tr>
<tr>
<td>show file</td>
<td>Displays file system information.</td>
<td>A-135</td>
</tr>
<tr>
<td>show flash</td>
<td>Displays boot status.</td>
<td>A-136</td>
</tr>
<tr>
<td>show ftp</td>
<td>Displays FTP server configuration.</td>
<td>A-137</td>
</tr>
<tr>
<td>show history</td>
<td>Displays the session command history.</td>
<td>A-137</td>
</tr>
<tr>
<td>show hostname</td>
<td>Displays the hostname.</td>
<td>A-138</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Shows interfaces status and configuration.</td>
<td>A-138</td>
</tr>
<tr>
<td>show ip</td>
<td>Shows ip parameters.</td>
<td>A-139</td>
</tr>
<tr>
<td>show layer3mobility</td>
<td>Displays license information.</td>
<td>A-141</td>
</tr>
<tr>
<td>show ldap</td>
<td>Displays LDAP server configuration.</td>
<td>A-142</td>
</tr>
<tr>
<td>show licenses</td>
<td>Displays license information.</td>
<td>A-143</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays message logging facilities.</td>
<td>A-143</td>
</tr>
<tr>
<td>show mac</td>
<td>Displays media access control list.</td>
<td>A-144</td>
</tr>
<tr>
<td>show management</td>
<td>Displays L3 Management Interface name.</td>
<td>A-144</td>
</tr>
<tr>
<td>show ntp</td>
<td>Displays network time protocol</td>
<td>A-145</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>show password-encryption</td>
<td>Displays password encryption.</td>
<td>A-151</td>
</tr>
<tr>
<td>show privilege</td>
<td>Displays current privileges.</td>
<td>A-146</td>
</tr>
<tr>
<td>show proxy-arpdb</td>
<td>Displays proxyARP entries in ARP database.</td>
<td>A-147</td>
</tr>
<tr>
<td>show radius</td>
<td>Displays RADIUS configuration information.</td>
<td>A-147</td>
</tr>
<tr>
<td>show redundancy-group</td>
<td>Displays redundancy group parameters.</td>
<td>A-151</td>
</tr>
<tr>
<td>show redundancy-history</td>
<td>Displays state transition history of the wireless module.</td>
<td>A-151</td>
</tr>
<tr>
<td>show redundancy-members</td>
<td>Displays redundancy member parameters.</td>
<td>A-151</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays current operating configuration.</td>
<td>A-151</td>
</tr>
<tr>
<td>show security-mgr</td>
<td>Displays securitymgr parameters.</td>
<td>A-153</td>
</tr>
<tr>
<td>show sflow</td>
<td>Displays Sflow configuration.</td>
<td>A-153</td>
</tr>
<tr>
<td>show snmp</td>
<td>Displays snmp engine parameters.</td>
<td>A-154</td>
</tr>
<tr>
<td>show snmp-server</td>
<td>Displays snmp server information.</td>
<td>A-156</td>
</tr>
<tr>
<td>show sntp</td>
<td>Displays sntp configuration.</td>
<td>A-156</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays contents of startup configuration.</td>
<td>A-157</td>
</tr>
<tr>
<td>show terminal</td>
<td>Displays terminal configuration parameters.</td>
<td>A-158</td>
</tr>
<tr>
<td>show time</td>
<td>Displays system clock.</td>
<td>A-158</td>
</tr>
<tr>
<td>show timezone</td>
<td>Displays time zone.</td>
<td>A-159</td>
</tr>
<tr>
<td>show upd-server</td>
<td>Displays server information.</td>
<td>A-159</td>
</tr>
<tr>
<td>show upgrade-status</td>
<td>Displays status of the last image upgrade.</td>
<td>A-160</td>
</tr>
<tr>
<td>show users</td>
<td>Displays information about terminal lines.</td>
<td>A-162</td>
</tr>
<tr>
<td>show version</td>
<td>Displays software &amp; hardware version.</td>
<td>A-161</td>
</tr>
<tr>
<td>show vlans</td>
<td>Displays VLAN information.</td>
<td>A-163</td>
</tr>
<tr>
<td>show wireless</td>
<td>Displays wireless configuration commands.</td>
<td>A-164</td>
</tr>
<tr>
<td>show wireless unapproved-apps</td>
<td>Displays wireless configuration commands.</td>
<td>A-164</td>
</tr>
</tbody>
</table>
Show Commands (All Contexts)

This section details the show commands displayed in all available contexts.

**show access-list**

This command displays IP access lists.

**Syntax**

```
show access-list (<199> | <100199> | <13001999> | <20002699> | WORD | radius)
```

- `<199>` IP standard access list
- `<100199>` IP extended access list
- `<13001999>` IP standard access list (expanded range)
- `<20002699>` IP extended access list (expanded range)
- `WORD` Name of ACL
- `radius` IDM/Radius Assigned
  - `+ MAC` Specify the user mac in AA-BB-CC-DD-EE-FF format
  - `- detail` Details of all the IDM/Radius assigned attributes

**Default Setting**

N/A

**Command Mode**

Manager

**Example**

```
HPswitch# show access-list
```

```
HPswitch#
```

**show aclstats**

This command displays ACL statistics.

**Syntax**

```
show aclstats (IFNAME)
```

- `IFNAME` Interface Name

```
+ vlan Vlan Interface
```

- `<14094>` Vlan Id
show alarm-log

This command displays all alarms since the last boot.

Syntax

```
show alarm-log [<1-65535> | acknowledged | all | count | new | severitytolimit]
```

- `<165535>`  Display details for specific alarm id
- `acknowledged`  Display acknowledged alarms currently in the system
- `all`  Display all alarms currently in the system
- `count`  Display count of alarms currently in the system
- `new`  Display new alarms currently in the system
- `severitytolimit`  Display all alarms having specified or higher severity
  - `+ critical`  Display all critical alarms
  - `+ informational`  Display all informational or higher severity alarms
  - `+ major`  Display all major or higher severity alarms
  - `+ normal`  Display all normal or higher severity alarms
  - `+ warning`  Display all warning or higher severity alarms

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch# show aclstats
HPswitch#
```

show alarm-log

This command displays all alarms since the last boot.

Syntax

```
show alarm-log [<1-65535> | acknowledged | all | count | new | severitytolimit]
```

- `<165535>`  Display details for specific alarm id
- `acknowledged`  Display acknowledged alarms currently in the system
- `all`  Display all alarms currently in the system
- `count`  Display count of alarms currently in the system
- `new`  Display new alarms currently in the system
- `severitytolimit`  Display all alarms having specified or higher severity
  - `+ critical`  Display all critical alarms
  - `+ informational`  Display all informational or higher severity alarms
  - `+ major`  Display all major or higher severity alarms
  - `+ normal`  Display all normal or higher severity alarms
  - `+ warning`  Display all warning or higher severity alarms

Default Setting

N/A

Command Mode

All
Example

HPswitch#show alarm-log
No Alarms in the alarm log
HPswitch#

show commands

This command displays command lists.

Syntax

show commands

Default Setting

N/A

Command Mode

Manager
Example

```bash
HPswitch#show commands
  acknowledge alarm-log (all|<1-65535>)
  acknowledge alarm-log (all|<1-65535>)
  cd (DIR)
  cd (DIR)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear arp (IFNAME)
  clear arp (IFNAME)
  clear logging
  clear wireless-statistics
  configure (terminal)
  configure (terminal)
  copy (FILE|URL) (FILE|URL)
  copy (FILE|URL) (FILE|URL)
  copy (FILE|URL) (FILE|URL)
  copy (FILE|URL) (FILE|URL)
  debug all
  debug cc (|err|warn|info|all)
  debug cc (|err|warn|info|all)
  debug cc (|err|warn|info|all)
-- MORE --, next page: Space, next line: Enter, quit:
Control-C
HPswitch#
```

show crypto

This command displays encryption related commands.

Syntax

```
show crypto (ipsec | isakmp | key | map | pki)
  -- ipsec  Show IPSEC policy
    + sa   IPSec Security Association
    + securityassociation  securityassociation
      - lifetime  lifetime
    + transformset  transformset
      - WORD  transform set name or all transform sets
  -- isakmp  Show ISAKMP
    + policy  policy
      - <110000>  priorityall isakmp policies
```
ProCurve Wireless Services zl Module Command Line Reference
Show Commands (All Contexts)

+ sa  All Crypto ISAKMP Security Association
    - key  Authentication key management
+ mypubkey  Show public keys associated with the switch
    - rsa  Show Rsa public keys
- map  Crypto maps
    + interface  Crypto maps for an interface.
        - WORD  interface name
    + tag  Crypto maps with a given tag
        - WORD  crypto map name
- pki  Public Key Infrastructure commands
    + request  Show certificate request
        - WORD  Trustpoint Name
+ trustpoints  Show trustpoints configured and configuration

Default Setting
N/A

Command Mode
Manager

Example

HPswitch# show crypto pki request
Self-Signed Certificate
Status : Available
Country : US
City : Palo Alto
Organization : Hewlett Packard, Inc.
Issuer : Wireless Services
Validity Date :
    start date : Nov 3 12:15:27 2005 GMT
    end date : Feb 1 12:15:27 2006 GMT
HPswitch#

show debug

This command displays debugging setting.

Syntax

    show debug
Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show debug
debugging is off
HPswitch#

show dhcp

This command displays DHCP server information.

Syntax
show dhcp (config | status)

- config Display DHCP Server configuration
- status Display whether DHCP Server is running or not

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show dhcp status
DHCP Server is Not Running
HPswitch#

show file

This command displays filesystem information.

Syntax
show file (information | systems)

- information Display file information
- + FILE Display information on FILE
- systems List filesystems
Default Setting

N/A

Command Mode

Manager

Example

HPswitch# show file information TESTFILE
flash:TESTFILE:
    type is text file
HPswitch# show file systems
File Systems:
   Size(b)     Free(b)     Type  Prefix
    -           -   opaque  system:
   4058112     2691072    flash  nvram:
   5057536     2764800    flash  flash:
    -           -  network  tftp:
    -           -  network  ftp:
    -           -  network  scp:

show flash

This command displays flash information.

Syntax

show flash

Default Setting

N/A

Command Mode

Manager
Example

show ftp
This command displays ftp server configuration.

Syntax

    show ftp

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show ftp
FTP Server: Disabled
User Name: anonymous or ftpuser
Password: ********
Root dir: flash:/HPswitch#

show history
This command displays session command history.

Syntax

    show history

Default Setting
N/A
Command Mode
Manager

Example

HPswitch#show history
1 show hostname
2 show history
HPswitch#

show hostname
This command displays the network name of the system.

Syntax
show hostname

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show hostname
Configured hostname : Wireless Services
HPswitch#

show interfaces
This command displays interface status and configuration.

Syntax
show interfaces (IFNAME | dblink | tunnel | uplink | vlan)
- IFNAME Interface name
- dblink Dlink Interface
- tunnel Tunnel Interface
  + <132> Tunnel Id
- uplink Uplink Interface
- vlan Vlan Interface
  + <14094> Vlan Id

A-138
Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show interfaces dnlink
Interface dnlink
Hardware Type Ethernet, Interface Mode Layer 2, address is 00-01-e6-f5-86-fc
index=2, metric=1, mtu=1500, (PAL-IF) <UP,BROADCAST,RUNNING,MULTICAST>
Speed: Admin Auto, Operational 1G, Maximum 1G
Duplex: Admin Auto, Operational Full
input packets 1372779, bytes 457008862, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 1372758, bytes 117174000, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0

HPswitch#

show ip
This command displays ip status and configuration.

Syntax

show ip [accessgroup | accesslist | arp | dns | dhcp | dhcpvendoroptions | dns | domain | interface | nat | route | routing | securewebmanagement | telnet | webmanagement]
  - accessgroup  Display ACLs attached to an interface
    + IFNAME  Interface name
    + dlink  Ethernet Interface Id
    + uplink  Ethernet Interface
    + vlan  Vlan Interface
      - <14094>  Vlan Id
  - accesslist  List IP access lists
  - arp  Address Resolution Protocol (ARP)
  - ddns  DDNS Configuration
    + binding  DNS Address bindings
  - dhcp  DHCP Server Configuration
    + binding  DHCP Address bindings
    + pool  DHCP Pools
      - WORD  DHCP pool name

A-139
– **dhcpvendoroptions**  DHCP Option 43 parameters received from DHCP server
– **dns**  DNS nameservers
– **domain**  Default domain for DNS
– **interface**  IP interface status and configuration
  + **IFNAME**  Interface name
  + **tunnel**  Tunnel Interface
    - `<132>`  Tunnel Id
  + **vlan**  Vlan Interface
    - `<14094>`  Vlan Id
– **nat**  Network Address Translation (NAT)
  + **interfaces**  NAT Configuration on Interfaces
  + **translations**  NAT translations
    - **inside**  Inside
      ++ **destination**  Destination
      ++ **source**  Source
    - **outside**  Outside
      ++ **destination**  Destination
      ++ **source**  Source
  + **verbose**  NAT Translations in realtime
– **route**  IP routing table
  + **A.B.C.D**  Network in the IP routing table to display
  + **A.B.C.D/M**  IP prefix /, e.g., 35.0.0.0/8
  + **detail**  IP routing table in detail
– **routing**  IP routing status
– **securewebmanagement**  Secured web server
– **telnet**  Telnet server
– **webmanagement**  Web server

**Default Setting**

N/A

**Command Mode**

Manager
Examples

HPswitch# show ip arp
IP Address     MAC Address          Interface  Type
192.168.15.1   00-14-bf-bf-72-30    vlan1      dynamic

HPswitch# show ip dns
68.87.76.178    dynamic
68.87.66.196    dynamic

HPswitch# show ip domain
IP dns-lookup : Enable
Domain Name   : hsd1.ca.comcast.net.

HPswitch# show ip interface vlan1
Interface             IP-Address            Status                Protocol
vlan1                 192.168.15.104(DHCP)   up                    up

HPswitch# show ip route
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
* - candidate default
Gateway of last resort is 192.168.15.1 to network 0.0.0.0
D* 0.0.0.0/0 [0/0] via 192.168.15.1, vlan1
C 192.168.15.0/24 is directly connected, vlan1

show layer3-mobility

This command displays Mobility parameters.

Syntax

show layer3-mobility (eventlog | forwarding | global | peer | station | statistics)
  - event-log  Event Log
  + peer         Peer eventlogs
  + station      Mobile unit event logs
  - forwarding   Stations in the Forwarding Plane
                 + AA-BB-CC-DD-EE-FF  MAC address of the Station
  - global       Global Mobility parameters
  - peer          Mobility peers
+ A.B.C.D  IP address of Peer
  + detail  Detailed information display
  – station  Stations in the Mobility Database
  + AA-BB-CC-DD-EE-FF  MAC address of the Station
  + detail  Detailed information display
  – statistics  Mobility statistics
  + AA-BB-CC-DD-EE-FF  MAC address of the Station

Default Setting
N/A

Command Mode
Manager

Example

HPswitch# show layer3-mobility event-log station
HPswitch#

show ldap

This command displays the ldap server configuration.

Syntax

  show ldap (configuration)
  – configuration  LDAP server configuration parameters
     + primary  primary LDAP server
     + secondary  secondary LDAP server

Default Setting
N/A

Command Mode
Manager

Example

HPswitch# show ldap configuration primary
primary LDAP server is not configured
HPswitch#
show licenses

This command displays installed licenses.

Syntax

    show licenses (uninstalled)

        •  **uninstalled** - Display uninstalled licenses.

Default Setting

    N/A

Command Mode

    Manager

Example

```plaintext
HPswitch# show licenses
Index  Feature Group     Value  Installed License Key (encoded)
-----  ----------------  -----  -------------------------------
0      radio-ports          12  ********************

HPswitch# show licenses uninstalled
No uninstalled licenses are present.

HPswitch#
```

show logging

This command displays logging configuration and buffer.

Syntax

    show logging

Default Setting

    N/A

Command Mode

    Manager
Example

HPswitch#show logging

Syslog logging: enabled
  Aggregation time: disabled
  Console logging: level debugging
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: disabled
Log Buffer (0 bytes):

HPswitch#

- **passwordencryption**  password encryption
  - **status**  Display passwordencryption status

show mac

This command displays the media access control list.

**Syntax**

```
show mac (accesslist)
  - accesslist  List MAC access lists
```

**Default Setting**

N/A

**Command Mode**

Manager

**Example**

HPswitch#show mac accesslist
Mgmt Interface: vlan1
HPswitch#

show management

This command displays L3 management interface name.

**Syntax**

```
show management
```
Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show management
Mgmt Interface: vlan1
HPswitch#

show ntp

This command displays network time protocol.

Syntax

show ntp (associations | status)
  – associations  NTP associations
  + detail      Show detail
  – status      NTP Status

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show ntp status
Mgmt Interface: vlan1
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 20
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
HPswitch#show ntp associations
address    ref clock    st when poll reach delay
offset    disp
  * master (synced), # master (unsynced), + selected, -
candidate, ~ configured
show password-encryption

This command displays password encryption parameters.

Syntax

show password-encryption (status)

• status - Displays password-encryption status.

Default Setting

N/A

Command Mode

Manager

Example

HPswitch#show password-encryption status
Password encryption is disabled
HPswitch#

show privilege

This command shows current privilege level.

Syntax

show privilege

Default Setting

N/A

Command Mode

Manager

Example

HPswitch#show privilege
Password encryption is disabled
HPswitch#
show proxy-arpdb

This command display proxyARP entries in ARP database.

Syntax
show proxy-arpdb

Default Setting
N/A

Command Mode
Manager

Example
HPswitch#show proxy-arpdb
HPswitch#

show radius

This command displays RADIUS configuration information.

Syntax
show radius
    configuration  radius server configuration parameters
    eap  Eap parameters
        + configuration  Eap configuration
    group  Radius group configuration
        + WORD  Existing radius group in the local radius database
    nas  client information
        + A.B.C.D/M  client ip address / mask
    proxy  proxy information
        + WORD  proxy realm name
    raduser  Radius user information
        + WORD  Existing User name in the local radius database
    trustpoint  Radius trustpoint configuration
    config  Display configured redundancy group information.

Default Setting
N/A
Command Mode
Manager

Example

HPswitch#show radius configuration
Radius Server Configuration
---------------------------
    Server Status : enabled
    Data Source   : local
HPswitch#

- redundancygroup Display redundancy group parameters
  - runtime Display runtime redundancy group information.
- redundancyhistory Display state transition history of the wireless module.
- redundancymembers Display redundancy group members in detail
  - A.B.C.D IP address of member module
  - brief Display members in brief

show redundancy-group

This command displays redundancy group parameters.

Syntax
  show redundancy-group (runtime)
  - runtime - Displays runtime redundancy group information.

Default Setting
N/A

Command Mode
Manager
**Examples:** These examples display runtime and group information.

```
HPswitch#show redundancy-group runtime
Redundancy Group Runtime Information
Redundancy Protocol Version : 1.0
Redundancy Group Authorization Level : 0
Radio Ports Adopted by Group : Not Applicable
Radio Ports Adopted by this Module : Not Applicable
Redundancy State : Disabled
Established Peer(s) Count : Not Applicable
Redundancy Group Connectivity status : Not Applicable

HPswitch#show redundancy-group
Redundancy Group Configuration Detail
Redundancy Feature : Disabled
Redundancy group ID : 50
Redundancy Mode : Active
Redundancy Interface IP : 10.10.1.20
Number of configured peer(s) : 1
Heartbeat-period : 5 Seconds
Hold-period : 20 Seconds
Discovery-period : 10 Seconds
Handle STP : Enabled
Module Authorization Level : 36

Redundancy Group Runtime Information
Redundancy Protocol Version : 1.0
Redundancy Group Authorization Level : 0
Radio Ports Adopted by Group : Not Applicable
Radio Ports Adopted by this Module : Not Applicable
Redundancy State : Disabled
Established Peer(s) Count : Not Applicable
Redundancy Group Connectivity status : Not Applicable

HPswitch#
```

**show redundancy-history**

This command displays state transition history of the wireless module.

**Syntax**

```
show redundancy-history
```

**Default Setting**

N/A
Command Mode

Manager

Example

HPswitch#show redundancy-history
State Transition History
Time                        Event Triggered       State
-------------------------------------------
Apr 25 07:42:30 2006        Redundancy Disabled   Disabled
HPswitch#

show redundancy-members

This command displays redundancy group parameters.

Syntax

show redundancy-members (A.B.C.D | brief)
- A.B.C.D  IP address of member module
- brief    Display members in brief

Default Setting

N/A

Command Mode

Manager

Example

HPswitch#show redundancy-members brief
Member ID (Self) : 0.0.0.0
Member State : Not Applicable
HPswitch#
show running-config

This command displays current operating configuration.

Syntax

    show running-config (include-factory)
    • include-factory - Include the factory defaults.

Default Setting

    N/A

Command Mode

    Manager
Example

HPswitch#show running-config
! configuration of ProCurveWLANModule Wireless Services version WS.01.03 on Tue6
! version 1.0
! no country-code
redundancy group-id 50
redundancy interface-ip 10.10.1.20
redundancy holdtime-period 20
redundancy discovery-period 10
redundancy handle-stp enable
redundancy member-ip 10.10.1.21
ip web-management
snmp-server manager v2
snmp-server manager v3
snmp-server user manager v3 encrypted auth md5 0x709f649df8ba589f178416c291fcba0
snmp-server user operator v3 encrypted auth md5 0x777da3446d4dcea9e722cfaa520021
wireless
interface vlan1
  ip address 192.168.1.5/21
!
end
HPswitch#show running-config include-factory
! configuration of ProCurveWLANModule Wireless Services version WS.01.03 on Tue6
! version 1.0
! no service password-encryption
no support prompt crash-info
no support set command-history
no support set reboot-history
no support set upgrade-history
hostname "Wireless Services"
ip dns-lookup
support pm max-sys-restarts 2
no support support pm sys-restart
support diag period 1000
support diag enable
no country-code
no snmp-server enable traps wireless-statistics min-packets
no snmp-server enable traps wireless-statistics wlan pktsps-greater-than
-- MORE --, next page: Space, next line: Enter, quit: Control-C
show securitymgr

This command displays securitymgr event logs.

Syntax

    show securitymgr (event-logs)

- event-logs Displays securitymgr event log.

Default Setting

N/A

Command Mode

Manager

Example

HPswitch#show securitymgr event-logs

Event Logs

========================

1> Tue Jan 23 2007 17:30:07: CORRUPT_PACKET: source vlan1: udp: Src 15.29.37.16
2> Tue Jan 23 2007 17:29:45: CORRUPT_PACKET: source vlan1: udp: Src 15.29.37.16
5> Tue Jan 23 2007 17:19:44: CORRUPT_PACKET: source vlan1: udp: Src 15.29.37.16
7> Tue Jan 23 2007 17:15:06: CORRUPT_PACKET: source vlan1: udp: Src 15.29.37.16

-- MORE --, next page: Space, next line: Enter, quit: Control-C
HPswitch#
+ sampling-polling  Displays information about sampling and polling
  - <11000>  A single radio index
  - RADIO  A list (eg: 1,3,7) or range (eg: 37) of radio indices
  - agent  Displays read-only agent information.

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#show sflow agent
#Version       : 1.3;HP;WS.02.01.24258R
Agent Address : 15.255.124.152
HPswitch

show snmp

This command displays snmp engine parameters.

Syntax

show snmp (user)
  •  snmp  Display SNMP engine parameters
     –  user  Displays snmp user details
       + manager  Display snmp manager details.
       + operator  Displays snmp operator details.
       + snmp-trap  Displays snmp trap details.

Default Setting
N/A

Command Mode
Manager
Examples

HPswitch#show snmp user

<table>
<thead>
<tr>
<th>userName</th>
<th>access</th>
<th>engineId</th>
<th>Auth</th>
<th>Priv</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager</td>
<td>rw</td>
<td>0000000c000000007f000001</td>
<td>MD5</td>
<td>DES</td>
</tr>
<tr>
<td>operator</td>
<td>ro</td>
<td>0000000c000000007f000001</td>
<td>MD5</td>
<td>DES</td>
</tr>
</tbody>
</table>

HPswitch#show snmp-server traps

---

Global enable flag for Traps
-----------------------------
N

Enable flag status for Individual Traps
----------------------------------------

<table>
<thead>
<tr>
<th>Module Type</th>
<th>Trap Type</th>
<th>Enabled?[Y/N]</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>coldstart</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>linkdown</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>linkup</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>authentication</td>
<td>N</td>
</tr>
<tr>
<td>upd-server</td>
<td>autoInstallInitiated</td>
<td>N</td>
</tr>
<tr>
<td>upd-server</td>
<td>cfgCkSumMismatch</td>
<td>N</td>
</tr>
<tr>
<td>upd-server</td>
<td>updSvrUnreachable</td>
<td>N</td>
</tr>
<tr>
<td>nsm</td>
<td>dhcpIPChanged</td>
<td>N</td>
</tr>
<tr>
<td>cluster</td>
<td>memberUp</td>
<td>N</td>
</tr>
<tr>
<td>cluster</td>
<td>memberDown</td>
<td>N</td>
</tr>
<tr>
<td>cluster</td>
<td>memberMisConfigured</td>
<td>N</td>
</tr>
<tr>
<td>cluster</td>
<td>adoptionExceeded</td>
<td>N</td>
</tr>
<tr>
<td>cluster</td>
<td>licenseChanged</td>
<td>N</td>
</tr>
<tr>
<td>misc</td>
<td>lowFsSpace</td>
<td>N</td>
</tr>
<tr>
<td>misc</td>
<td>processMaxRestartsReached</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>associated</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>disassociated</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnCapability</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnShortPream</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnSpectrum</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnErr</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnSSID</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnRates</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnInvalidWPAWPA2IE</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationAsPortCapacityReached</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>tkipCounterMeasures</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAuthentication</td>
<td>N</td>
</tr>
</tbody>
</table>

HPswitch#
show snmp-server

This command displays SNMP server information.

Syntax

```
snmp-server (traps)
  - traps  Displays trap-enable flags.
  + wireless-statistics  Display wireless-stats rate traps
    - radio  Display radio rate traps
    - station  Display station rate traps
    - wireless-module  Display wireless-module rate traps
    - wlan  Display wlan rate traps
```

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#show snmp-server
Location:
Contact:
SysName: Wireless Services

SNMP v2: enabled
public  ro, private  rw

SNMP v3: enabled

SNMP host:
  trap receiver:10.30.0.242:162 version v3
  trap receiver:10.30.0.43:162 version v3
HPswitch#
```

show sntp

This command displays simple NTP configuration.

Syntax

```
show sntp
```
Show Commands (All Contexts)

Default Setting
N/A

Command Mode
Manager

Example

HPswitch# show sntp
Simple NTP is Disabled
Simple NTP Servers:
No Simple NTP servers are configured
HPswitch#

show startup-config

This command displays contents of startup configuration.

Syntax

show startup-config

Default Setting
N/A

Command Mode
Manager

Example

HPswitch# show startup-config
! factory default configuration
! prompt to include indication of crash files
support prompt crash-info
! vlan 1 gets an IP address via DHCP
interface vlan1
  ip address dhcp
! web and snmp are enabled to allow the management java applet to function ip
web-management
snmp-server manager v2
snmp-server manager v3
snmp-server user manager v3 encrypted auth md5
0x709f649df8ba589f178416c291fcba0
snmp-server user operator v3 encrypted auth md5
0x777da3446d4dcea9e722cfaa520021
! HPswitch#
show terminal

This command displays terminal configuration parameters.

Syntax

show terminal

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#show terminal
Terminal Type: vt100
Length: 24 Width: 80
HPswitch#
```

show time

This command displays the system clock.

Syntax

show time

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch#show time
Feb 21 16:56:46 2006
HPswitch#
```
show timezone

This command displays the timezone.

Syntax
  show timezone

Default Setting
  N/A

Command Mode
  Manager

Example

HPswitch#show timezone
Timezone is Etc/UTC
HPswitch#

show upd-server

This command displays update server parameters.

Syntax
  show upd-server

Default Setting
  N/A

Command Mode
  Manager
Example

HPswitch#show upd-server
Terminal Type: vt100
Length: 24   Width: 80
ProCurve(wireless-services-A)#*show time
Feb 21 16:56:46 2006
ProCurve(wireless-services-A)#*show timezone
Timezone is Etc/UTC
ProCurve(wireless-services-A)#*show upd-server
Unreachable : FALSE
Address      : 0.0.0.0
Protocol     : ftp
Username     :
Password     :
Img File Loc :
Img File Ver :
Cfg File Loc :
HPswitch#

show upgrade-status

This command displays the status of the last image upgrade.

Syntax

    show upgrade-status (detail)

-   detail - Display last image upgrade log.

Default Setting

N/A

Command Mode

Manager
Example

```
HPswitch#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Nov 22 15:18:17 2005
HPswitch#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Nov 22 15:18:17 2005
```

----------------------------------------
var2 is 13 percent full
/tmp is 35 percent full
Free Memory 187880 kB
FWU invoked via Linux shell
Update Params: tftp://10.30.0.91///ProCurveWLANModule-WS.01.XX.0551Swami.img
R5
Using /usr/bin/copy_file tftp://10.30.0.91///ProCurveWLANModule-WS.01.XX.0551Se
Reading image file header
Removing other partition
Added WS.01.XX.0551Swami *
Making file system
Extracting files
Version of firmware update file is WS.01.XX.0551Swami
Versions match, renaming my ver to WS.01.XX.0551Swami-
Creating LILO files
Running LILO
Added WS.01.XX.0551Swami- *
Added WS.01.XX.0551Swami
```

show version

This command displays the software and hardware version.

Syntax

```
show version (verbose)
```

- **verbose** - Display software and hardware details.

Default Setting

N/A

Command Mode

Manager
Example

HPswitch#show version
ProCurveWLANModule version WS.01.XX.0551Swami
Copyright (c) 2005 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 0 days, 2 hours 37 minutes
CPU is AMD Athlon(tm) Processor
256112 kB of on-board RAM
ide device hda disk model TOSHIBA THNCF256MBA capacity 500736 blocks, cache 2
HPswitch#show version verbose
ProCurveWLANModule version WS.01.XX.0551Swami
Copyright (c) 2005 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 0 days, 2 hours 42 minutes
CPU is AMD Athlon(tm) Processor
PCI bus 0 device 17 function 0
  ISA bridge
  VIA Technologies, Inc.
  VT8235 ISA Bridge (rev 0).
PCI bus 0 device 17 function 1
  IDE interface
  VIA Technologies, Inc.
  VT82C586A/B/VT82C686/A/B/VT823x/A/C PIPC Bus Master IDE (rev 6).
PCI bus 1 device 0 function 0
  PIC
  VIA Technologies, Inc.
  VPX/VPX2 I/O APIC Interrupt Controller (rev 3).
PCI bus 2 device 8 function 0
  Ethernet controller
  Intel Corporation
  82546BB Gigabit Ethernet Controller (rev 1).
-- MORE --, next page: Space, next line: Enter, quit: Control-C

show users

This command displays information about terminal lines.

Syntax

show users

Default Setting

N/A
Command Mode

Manager

Example

HPswitch# **show users**
<table>
<thead>
<tr>
<th>Line</th>
<th>PID</th>
<th>User</th>
<th>Uptime</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>130</td>
<td>vty</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>07:26:26</td>
<td></td>
</tr>
</tbody>
</table>

HPswitch#

---

**show vlans**

This command displays vlan information.

**Syntax**

```
show vlans
```

**Default Setting**

N/A

**Command Mode**

Manager

Example

HPswitch# **show vlans**

Downlink:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2100</td>
<td>VLAN2100</td>
<td>ADP,C1-C24</td>
</tr>
</tbody>
</table>

Uplink:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>AUP,B1-B4,C1-C24,D1-D24</td>
</tr>
</tbody>
</table>

HPswitch#
Show Commands (Wireless)

This section details the show commands pertaining to the wireless parameters.

show wireless ap-detection-config

This command displays detected radio port configuration parameters.

Syntax

```plaintext
show wireless ap-detection-config
```

Default Setting

N/A

Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

```plaintext
HPswitch(config-wireless)#show wireless ap-detection-config
timeout                  : 300
max-detected-aps         : 100
configured approved-aps  :
Index | Bss Mac         | Ssid
-------------------------------------------------------
HPswitch(config-wireless)#
```

show wireless approved-aps

This command displays approved applications as seen by radio port scanning.

Syntax

```plaintext
show wireless approved-aps
```

Default Setting

N/A
Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

HPswitch(config-wireless)#show wireless approved-aps
0 Approved APs found

<table>
<thead>
<tr>
<th>Bss Mac</th>
<th>Rpt Rd</th>
<th>Ch</th>
<th>Last Seen</th>
<th>Ssid</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-14-C2-B3-01-70</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>SSID 1</td>
</tr>
</tbody>
</table>

HPswitch(config-wireless)#

show wireless channel-power

This command displays available channel and power levels for a radio.

Syntax

show wireless channel-power (11a|11bg)

+ 11a radio is of type 802.11a
   - indoor radio is placed indoor
   - outdoor radio is placed outdoor
+ 11bg radio is of type 802.11bg
   - indoor radio is placed indoor
   - outdoor radio is placed outdoor

Default Setting

N/A

Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context
show wireless config

This command displays wireless configuration parameters.

Syntax

show wireless config

Default Setting

N/A

Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context
Example

HPswitch(config-wireless)#show wireless config
    country-code : us
    adoption-pref-id : 1
    proxy-arp : disabled
    wlan-prioritization : disabled
    adopt-unconf-radio : enabled
    dot11-shared-key-auth: disabled
    ap-detection : enabled
    advanced-config : disabled

HPswitch(config-wireless)#

show wireless country-code-list

This command displays a list of supported country names and two letter ISO 3166 codes.

Syntax

    show wireless country-code list
        + Output modifiers
        + Output redirection
        + Output redirection appending

Default Setting

    N/A

Command Mode

    Manager Configuration Context
    Global Configuration Context
    Interface Configuration Context
    Wireless Configuration Context

Example

HPswitch(config-wireless)#show wireless country-code list

HPswitch(config-wireless)##
show wireless ids

This command displays intrusion detection parameters.

Syntax

```
show wireless ids [filter-list]
+ filter-list  Displays the list of currently filtered stations.
```

Default Setting

N/A

Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

```
HPswitch(config-wireless)# show wireless ids
filter-agetout        : 60 seconds
excessive-probes      : disabled
excessive-associations: disabled

HPswitch(config-wireless) #
```

show wireless mac-auth-local

This command displays the mac-auth-local entries.

Syntax

```
show wireless mac-auth-local (<1100>)
+ <11000>  macauthlocal entry to display
```

Default Setting

N/A
**Command Mode**

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

**Example**

```
HPswitch(config-wireless)#show wireless mac-auth-local
[need output]
HPswitch(config-wireless)#
```

**show wireless multicast-packet-limit**

This command displays multicast-packet limit.

**Syntax**

```
show wireless multicast-packet-limit
```

**Default Setting**

N/A

**Command Mode**

Wireless Configuration Context

**Example**

```
HPswitch(config-wireless)#show wireless multicast-packet-limit
vlan # multicast-packet-limit (packets/sec)
all vlans 0 ]
HPswitch(config-wireless)#
```
show wireless phrase-to-key

This command displays the WEP keys generated by a passphrase.

Syntax

show wireless phrase-to-key (wep128 | wep64)

- **wep128** - Displays WEP128 keys.
  - **WORD** - Passphrase between 4 and 32 characters.
- **wep64** - Displays WEP64 keys.
  - **WORD** - Passphrase between 4 and 32 characters.

Default Setting

N/A

Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

HPswitch(config-wireless)#show wireless phrase-to-key wep128 help
1) d7aad741102ccc216ed1b59322
2) 2cdd3865719e93719d5a2a87c6
3) 984590afb106774126f8c0b583
4) 792ef65147269f968cc23c204

HPswitch(config-wireless)#

show wireless qos-mapping

This command displays the Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags.

Syntax

show wireless qos-mapping (wired-to-wireless | wireless-to-wired)

- **wired-to-wireless** - Mappings used when traffic is switched from wired to the wireless side.
- **wireless-to-wired** - Mappings used when traffic is switched from wireless to the wired side.
Default Setting
N/A

Command Mode
Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

```
HPswitch(config-wireless)# show wireless qos-mapping wired-to-wireless
DSCP value : WMM Access Category
  0  1  2  3  4  5  6  7 24 25 26 27 28 29 30 31 : best-effort
  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 : background
 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 : video
 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 : voice
802.1p tag : WMM Access Category
  0  3 : best-effort
  1  2 : background
  4  5 : video
  6  7 : voice
HPswitch(config-wireless)#
```

```
show wireless radio
This command displays the radio configuration.

Syntax
show wireless radio (beacon-table | config | monitor-table | statistics | unadopted )
  + beacon-table The RadiotoRadio beacon table
  + config   Radio configuration
     - <11000> A single radio index
     - default-11a default 11a configuration template
     - default-11bg default 11bg configuration template
  + monitor-table The RadiotoRadio monitoring table
  + statistics Radio statistics
     - <11000> A single radio index <11000>
        ++ detail Detailed radio statistics
```
**ProCurve Wireless Services zl Module Command Line Reference**

**Show Commands (Wireless)**

- **unadopted**  List of unadopted radios
- **rp**  Status of an adopted radio port.
- **+ <148>**  The index of the radioport for detailed information
- **+ AA-BB-CC-DD-EE-FF**  The MAC address of a radioport for detailed information

**Default Setting**

N/A

**Command Mode**

- Manager Configuration Context
- Global Configuration Context
- Interface Configuration Context
- Wireless Configuration Context

**Example**

```
HPswitch(config-wireless)#show wireless radio-config
index  description  radio port mac   type   wlans-mapped
1   RADIO1       00-14-C2-A0-1B-3E  11bg
2   RADIO2       00-14-C2-A0-1B-3E  11a
3   RADIO3       00-14-C2-A0-0B-EC  11bg
4   RADIO4       00-14-C2-A0-0B-EC  11a
def-11a DEFAULT-11A   FF-FF-FF-FF-FF-FF  11a
def-11b DEFAULT-11B   FF-FF-FF-FF-FF-FF  11b
def-11bg DEFAULT-11G   FF-FF-FF-FF-FF-FF  11bg
HPswitch(config-wireless)#
```

**show wireless radio-status**

This command displays the status of all radios that are adopted or in the process of adoption.

**Syntax**

`show wireless radio-status (<1-1000>)`

- **+ <11000>**  A single radio index

**Default Setting**

N/A
Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

```
HPswitch#show wireless radio-status
#  Radio Port MAC     Start BSS        Radio  State     Channel  Pwr
1]  00-14-C2-A0-1B-3E 00-14-C2-A0-8F-A4  11bg   normal    1 (rnd)  20
2]  00-14-C2-A0-1B-3E 00-14-C2-A0-CP-F0  11a    normal    48 (rnd)  17
3]  00-14-C2-A0-0B-EC 00-14-C2-A0-4E-EC  11bg   normal    11 (rnd)  20
4]  00-14-C2-A0-0B-EC 00-14-C2-A0-CP-34  11a    normal    40 (rnd)  17
```

show wireless regulatory

This command displays regulatory (allowed channel/power) information for a particular country.

Syntax

```
show wireless regulatory <country-codes>
```

+ ae United Arab Emirates
+ ar Argentina
+ at Austria
+ au Australia
+ ba Bosnia Herzegovina
+ be Belgium
+ bg Bulgaria
+ bh Bahrain
+ bm Bermuda
+ br Brazil
+ bs Bahamas
+ by Belarus
+ ca Canada
+ ch Switzerland
+ cl Chile
+ cn China
+ co  Colombia
+ cr  Costa Rica
+ cy  Cyprus
+ cz  Czech Republic
+ de  Germany
+ dk  Denmark
+ do  Dominican Republic
+ ec  Ecuador
+ ee  Estonia
+ eg  Egypt
+ es  Spain
+ fi  Finland
+ fr  France
+ gb  United Kingdom
+ gr  Greece
+ gt  Guatemala
+ gu  Guam
+ hk  Hong Kong
+ hn  Honduras
+ hr  Croatia
+ ht  Haiti
+ hu  Hungary
+ id  Indonesia
+ ie  Ireland
+ il  Israel
+ in  India
+ is  Iceland
+ it  Italy
+ jo  Jordan
+ jp  Japan
+ kr  South Korea
+ kw  Kuwait
+ kz  Kazakhstan
+ li  Liechtenstein
+ lk  Sri Lanka
<table>
<thead>
<tr>
<th>Code</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>lt</td>
<td>Lithuania</td>
</tr>
<tr>
<td>lu</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>lv</td>
<td>Latvia</td>
</tr>
<tr>
<td>ma</td>
<td>Morocco</td>
</tr>
<tr>
<td>mt</td>
<td>Malta</td>
</tr>
<tr>
<td>mx</td>
<td>Mexico</td>
</tr>
<tr>
<td>my</td>
<td>Malaysia</td>
</tr>
<tr>
<td>nl</td>
<td>Netherlands</td>
</tr>
<tr>
<td>no</td>
<td>Norway</td>
</tr>
<tr>
<td>nz</td>
<td>New Zealand</td>
</tr>
<tr>
<td>om</td>
<td>Oman</td>
</tr>
<tr>
<td>pe</td>
<td>Peru</td>
</tr>
<tr>
<td>ph</td>
<td>Philippines</td>
</tr>
<tr>
<td>pk</td>
<td>Pakistan</td>
</tr>
<tr>
<td>pl</td>
<td>Poland</td>
</tr>
<tr>
<td>pt</td>
<td>Portugal</td>
</tr>
<tr>
<td>qa</td>
<td>Qatar</td>
</tr>
<tr>
<td>ro</td>
<td>Romania</td>
</tr>
<tr>
<td>ru</td>
<td>Russia</td>
</tr>
<tr>
<td>sa</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>se</td>
<td>Sweden</td>
</tr>
<tr>
<td>sg</td>
<td>Singapore</td>
</tr>
<tr>
<td>si</td>
<td>Slovenia</td>
</tr>
<tr>
<td>sk</td>
<td>Slovak Republic</td>
</tr>
<tr>
<td>th</td>
<td>Thailand</td>
</tr>
<tr>
<td>tr</td>
<td>Turkey</td>
</tr>
<tr>
<td>tw</td>
<td>Taiwan</td>
</tr>
<tr>
<td>ua</td>
<td>Ukraine</td>
</tr>
<tr>
<td>us</td>
<td>United States</td>
</tr>
<tr>
<td>uy</td>
<td>Uruguay</td>
</tr>
<tr>
<td>ve</td>
<td>Venezuela</td>
</tr>
<tr>
<td>vn</td>
<td>Vietnam</td>
</tr>
<tr>
<td>za</td>
<td>South Africa</td>
</tr>
</tbody>
</table>

**Default Setting**

N/A
Command Mode
Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example
HPswitch(config-wireless)#show wireless regulatory us
802.11a Outdoor
Channels : 52 56 60 64 149 153 157 161 165
Power(dBm): 20 20 20 20 20 20 20 20 20

802.11a Indoor
Channels : 36 40 44 48 52 56 60 64 149 153 157 161 165
Power(dBm): 17 17 17 17 20 20 20 20 20 20 20 20 20

802.11bg Outdoor
Channels : 1 2 3 4 5 6 7 8 9 10 11
Power(dBm): 20 20 20 20 20 20 20 20 20 20 20 20 20

802.11bg Indoor
Channels : 1 2 3 4 5 6 7 8 9 10 11
Power(dBm): 20 20 20 20 20 20 20 20 20 20 20 20 20

HPswitch(config-wireless)#

show wireless rp

This command displays the status of an adopted radio port.

Syntax
show wireless rp (<148> | AA-BB-CC-DD-EE-FF)
+ <148> The index of the radioport for detailed information
+ AA-BB-CC-DD-EE-FF The MAC address of a radioport for detailed information

Default Setting
N/A
**Command Mode**
Manager Configuration Context  
Global Configuration Context  
Interface Configuration Context  
Wireless Configuration Context

**Example**

```markdown
HPswitch(config-wireless)#show wireless rp  
Number of radio-ports adopted : 2  
Available licenses : 34  
Clustering enabled : N  
Clustering mode : active

<table>
<thead>
<tr>
<th>#</th>
<th>Mac</th>
<th>Radios [indices]</th>
<th>Model Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-14-C2-A0-1B-3E</td>
<td>2 [ 1 2 ]</td>
<td>ProCurve Radio Port 230</td>
</tr>
<tr>
<td>2</td>
<td>00-14-C2-A0-0B-EC</td>
<td>2 [ 3 4 ]</td>
<td>ProCurve Radio Port 220</td>
</tr>
</tbody>
</table>
```

HPswitch(config-wireless)#

**show wireless rp-images**

This command displays the radio-port images on the wireless module.

**Syntax**

```markdown
show wireless rp-images
```

**Default Setting**

N/A

**Command Mode**
Manager Configuration Context  
Global Configuration Context  
Interface Configuration Context  
Wireless Configuration Context
**Example**

```
HPswitch(config-wireless)#show wireless rp-images
Idx   Image-File           Version       Release Date    Size (bytes)
 1     ProCurve-200-Series 00.02-27 [00] 04 Feb 2006     293320
HPswitch(config-wireless)#
```

**show wireless rp-unadopted**

This command displays a list of unadopted radio-port.

**Syntax**

```
show wireless rp-unadopted
```

**Default Setting**

N/A

**Command Mode**

- Manager Configuration Context
- Global Configuration Context
- Interface Configuration Context
- Wireless Configuration Context

**Example**

```
HPswitch(config-wireless)#show wireless rp-unadopted
Idx   radio-port Mac   Last Seen       radio-port Model
 1]   00-14-c2-b3-01-70 9 seconds ago  ProCurve-200-Series
HPswitch(config-wireless)#
```

**show wireless self-heal-config**

This command displays the self-healing configuration parameters.

**Syntax**

```
show wireless self-heal-config (<1-1100> | all)
```

- `<1-1000>` - single radio index.
- `all` - all configured radios.
Default Setting
N/A

Command Mode
Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

HPswitch(config-wireless)# show wireless self-heal-config
interference-avoidance : disabled
retries : 14.0
hold-time : 3600 seconds
neighbor-recovery : disabled

HPswitch(config-wireless)#

show wireless station

This command displays the details of associated stations.

Syntax

text

show wireless station (<14096> | AA-BB-CC-DD-EE-FF | radio | statistics | wlan)

+ <14096>  Index of station
+ AA-BB-CC-DD-EE-FF  MAC address of station
+ radio  Show mobileunits associated to this radio
- <11000>  A single radio index
+ statistics  station rf statistics
- AA-BB-CC-DD-EE-FF  MAC address of station
++ detail  Detailed station statistics
+ wlan  Show mobile units associated to this wlan
- WLAN_RANGE  A wlan index <132>

Default Setting
N/A
Show Commands (Wireless)

Command Mode
Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

HPswitch(config-wireless)#show wireless station
Number of stations associated: 0
HPswitch(config-wireless)#

show wireless unapproved-aps

This command displays the unapproved APs seen by radio-port scans.

Syntax
show wireless unapproved-aps

Default Setting
N/A

Command Mode
Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context
Example

HPswitch(config-wireless)#show wireless unapproved-aps
Detected 32 unapproved APs (from 32 AP scan reports)

<table>
<thead>
<tr>
<th>Bss Mac</th>
<th>Rpt Rd</th>
<th>Ch</th>
<th>dBm</th>
<th>Last Seen</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-14-C2-A5-2C-F0</td>
<td>1</td>
<td>6</td>
<td>-46</td>
<td>0 secs</td>
<td>J1</td>
</tr>
<tr>
<td>00-14-C2-B3-01-70</td>
<td>1</td>
<td>6</td>
<td>-40</td>
<td>0 secs</td>
<td>SSID 1</td>
</tr>
<tr>
<td>00-30-AB-28-7F-11</td>
<td>1</td>
<td>6</td>
<td>-49</td>
<td>0 secs</td>
<td>wireless-g</td>
</tr>
</tbody>
</table>

HPswitch(config-wireless)#

show wireless web-auth-config

This command displays the WLAN web-auth configuration.

Syntax

show wireless web-auth-config (<1-32>)

– <1-32> - A WLAN index.

Default Setting

N/A

Command Mode

- Manager Configuration Context
- Global Configuration Context
- Interface Configuration Context
- Wireless Configuration Context
Example

HPswitch(config-wireless)#show wireless web-auth-config
WLAN: 1 status: disabled description: ssid: SSID 1
     Page-Location: internal
     Radius Server Parameters:
         primary server:
             IP address: 0.0.0.0 authentication-port: 1812 radius-key:
         secondary server:
             IP address: 0.0.0.0 authentication-port: 1812 radius-key:
     Retries: 3 Timeout: 5
     Internal Pages
         Page-type: login
         Title: Login Page
         Header: Network Login
         Description: Please enter your username and password
         Footer: Contact the network administrator if you do not have an account
     Image URL main:
     Image URL small:
-- MORE --, next page: Space, next line: Enter, quit: Control-C

show wireless wireless-module-statistics
This command displays the wireless module statistics.

Syntax

    show wireless wireless-module-statistics (detail)
        – detail - detailed wireless-module statistics.

Default Setting

    N/A

Command Mode

    Manager Configuration Context
    Global Configuration Context
    Interface Configuration Context
    Wireless Configuration Context
Example

HPswitch(config-wireless)#show wireless wireless-module-statistics
stations Associated :  0     Radios adopted :  4

------ Traffic ----------------------------------------------

<table>
<thead>
<tr>
<th>Total</th>
<th>Rx</th>
<th>Tx</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>30s</td>
<td>1hr</td>
</tr>
<tr>
<td>Pkts per sec:</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Throughput:</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Avg bit speed:</td>
<td>0.00</td>
<td>0.00 Mbps</td>
</tr>
<tr>
<td>% Non-unicast pkts:</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

------ RF Status-----------------------------------------------

<table>
<thead>
<tr>
<th></th>
<th>30s</th>
<th>1hr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg station signal:</td>
<td>0.00</td>
<td>0.00 dBm</td>
</tr>
<tr>
<td>Avg station noise:</td>
<td>0.00</td>
<td>0.00 dBm</td>
</tr>
<tr>
<td>Avg station SNR(dB):</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

show wireless wlan

This command displays the WLAN configuration.

Syntax

show wireless wlan (config | statistics)
+ config  Wlan configuration
  - <132>  A wlan index <132>
  - all    All wlans in configuration
  - enabled Only wlans that are currently enabled
+ statistics  WLAN statistics
  - <132>  A wlan index <132>
  ++ detail Detailed wlan statistics

Default Setting

N/A
Command Mode

Manager Configuration Context
Global Configuration Context
Interface Configuration Context
Wireless Configuration Context

Example

HPswitch(config-wireless)#show wireless wlan config

<table>
<thead>
<tr>
<th>#</th>
<th>enabled</th>
<th>ssid</th>
<th>authentication</th>
<th>encryption</th>
<th>vlan/tunnel</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N</td>
<td>SSID 1</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>N</td>
<td>SSID 2</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>N</td>
<td>SSID 3</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>N</td>
<td>SSID 4</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>N</td>
<td>SSID 5</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>N</td>
<td>SSID 6</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>N</td>
<td>SSID 7</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>N</td>
<td>SSID 8</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>N</td>
<td>SSID 9</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>N</td>
<td>SSID 10</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>N</td>
<td>SSID 11</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>N</td>
<td>SSID 12</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>N</td>
<td>SSID 13</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>N</td>
<td>SSID 14</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>N</td>
<td>SSID 15</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>N</td>
<td>SSID 16</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>N</td>
<td>SSID 17</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>N</td>
<td>SSID 18</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>N</td>
<td>SSID 19</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>N</td>
<td>SSID 20</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>N</td>
<td>SSID 21</td>
<td>none</td>
<td>none</td>
<td>vlan 1</td>
<td></td>
</tr>
</tbody>
</table>

HPswitch(config-wireless)#show wireless wlan statistics
Support Commands

These commands are common commands used for advanced support duties in all contexts.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>support clear (all</td>
<td>cores</td>
<td>dumps</td>
</tr>
<tr>
<td>support copy tech-support URL</td>
<td>Displays resets the functions.</td>
<td>A-187</td>
</tr>
<tr>
<td>[no] support diag (enable</td>
<td>period)</td>
<td>(Negate) Configures diagnostics.</td>
</tr>
<tr>
<td>[no] support diag shell</td>
<td>(Negate) Provides diagnostic shell access.</td>
<td>A-188</td>
</tr>
<tr>
<td>[no] support pm (max-sys-restarts</td>
<td>sys-restart)</td>
<td>(Negate) Displays information about processes controlled by Process Monitor.</td>
</tr>
<tr>
<td>support save-cli</td>
<td>Saves CLI tree for all modes in HTML format.</td>
<td>A-192</td>
</tr>
<tr>
<td>[no] support set (command-history</td>
<td>reboot-history</td>
<td>upgrade-history )</td>
</tr>
<tr>
<td>support show (chassis</td>
<td>cli</td>
<td>command-history</td>
</tr>
</tbody>
</table>

See Support Commands (Wireless)
# Support Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no]support wireless dump-core</td>
<td>Creates a core file of the ccsvr process.</td>
<td>A-196</td>
</tr>
<tr>
<td>[no] support wireless dump-scale</td>
<td>Creates a ccsvr.dump file in nvram with internal state information.</td>
<td>A-196</td>
</tr>
<tr>
<td>[no]support wireless rate-scale</td>
<td>Enables wireless rate scaling (default)</td>
<td>A-197</td>
</tr>
<tr>
<td>support wireless request-rp-log</td>
<td>This command requests a radio port log.</td>
<td>A-197</td>
</tr>
</tbody>
</table>
Support Commands (All Contexts)

This section details the support commands available to all contexts.

support clear

This command resets the functions.

Syntax

```
support clear (all | clitree | cores | dumps | panics | pm )
```

- **all** - Removes all core, dump, panic, and pm files.
- **clitree** - Removes clitree.html
- **cores** - Removes all core files.
- **dumps** - Removes all dump files.
- **panics** - Removes all kernel panic files.
- **pm** - Process Monitor
  - **statistics** - Heartbeat counters and restarts.
  - **system-restart-count** - Number of times that PM restarted the system.

Default Setting

N/A

Command Mode

Manager

Example

```
HPswitch# support clear cores
HPswitch#
```

support copy

This command copies from one file to another.

Syntax

```
support copy tech-support URL
```

- **tech-support** - Copy extensive system information useful to technical support for troubleshooting a problem.
  - **URL** - URL to which to copy.
Support Commands (All Contexts)

URLs:
- tftp://<hostname or IP>/path/file
- ftp://<user>:<passwd>@<hostname or IP>/path/file
- scp://<user>@<hostname or IP>/path/file

Default Setting
N/A

Command Mode
Manager

Example

```
HPswitch# support copy tech-support tftp://192.168.1.10/testfile
HPswitch#
```

**support diag**

This command configures diagnostics. The no command negates the diagnostics.

**Syntax**

```
support diag (enable | limit | period | watchdog )
```
- **enable** - Enable in-service diagnostics.
- **limit** - Set diagnostic period.
  - **buffer** - Buffer usage warning limit.
    + \(<128>\) - 128k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<16>\) - 16k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<1>\) - 1k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<256>\) - 256k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<2>\) - 2k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<32>\) - 32k byte buffer limit.
    - \(<0-65535>\) - buffer usage warning limit.
    + \(<4>\) - 4k byte buffer limit.
```
- `<0-65535>` - buffer usage warning limit.
+ `<512>` - 512k byte buffer limit.
- `<0-65535>` - buffer usage warning limit.
+ `<64>` - 64k byte buffer limit.
- `<0-65535>` - buffer usage warning limit.
+ `<8>` - 8k byte buffer limit.
- `<0-65535>` - buffer usage warning limit.
- `fan` - Fan speed limit.
+ `<1>` - Fan number
- `low` - Low speed limit.
  ++ `<1000-15000>` - Limit value.
- `filesys` - File system freespace limit.
- `inodes` - File system inodes limit.
- `load` - Aggregate processorload.
- `maxFDs` - Maximum number of file descriptors.
- `pkbuffers` - Packet buffer head cache.
+ `<0-65535>` - Limit.
- `procRAM` - Percent RAM used by a processor.
+ `WORD` - Limit from 0.0-100.
- `ram` - Percent free RAM.
+ `WORD` - Limit from 0.0-100.
- `rotechache` - IP route cache usage.
+ `<0-65535>` - Limit.
- `temperature` - Temperature limit.
+ `<1-8>` - Temperature sensor number.
  - `Critical` - Critical temperature limit.
  ++ `WORD` - 0.0-250
  - `High` - High temperature limit.
  ++ `WORD` - 0.0-250
  - `Low` - Low temperature limit.
  ++ `WORD` - 0.0-250

- `period` - Set diagnostic period.
  – `<100-30000>` - Diagnostics period, default is 1000 miliseconds.
- `watchdog` - Enable the watchdog.

**Default Setting**

Diagnostic Period: 1000
**Command Mode**

Manager

**Example**

```
HPswitch#support diag enable
HPswitch#
```

**support diag-shell**

This command provides diagnostic shell access. The no command negates the shell access.

**Syntax**

```
support diag-shell
```

**Default Setting**

N/A

**Command Mode**

Manager

**Example**

```
HPswitch#support diag-shell
Diagnostic shell started for testing
diag >
```

**support encrypt**

This command encrypts password or key.

**Syntax**

```
support encrypt
```

- **secret** - Encrypt password/keys with a secret phrase.
  - 2 - Type of encryption.
  + **Word** - Passphrase for encryption.
  - **plaintext** - Plaintext password or key.
  ++ **LINE** - Plaintext to be encrypted with given secret.
Default Setting
N/A

Command Mode
Manager

Example

HPswitch#support encrypt secret 2 Word plaintest LINE
HPswitch#

support pm

This command supports the process monitor. The no command negates the process configuration.

Syntax

support pm (max-sys-restarts | sys-restart)

- **max-sys-restarts** - Maximum number of times PM will restart the system because of failure.
  - <1-5> - Number of system restarts.
- **sys-restart** - Enable PM to restart the system when a process fails.

Default Setting
N/A

Command Mode
Manager

Example

HPswitch#support pm sys-restart
HPswitch#

support prompt

This command enables the crash-info prompt. The no command negates the enabling of the crash-info prompt.

Syntax

support prompt (crash-info)

- **crash-info** - Enables crash-info prompt.
Default Setting
N/A

Command Mode
Manager

Example

HPswitch#support prompt crash-info
HPswitch#

**support save-cli**

This command saves cli tree for all modes in HTML format.

**Syntax**

    support save-cli

**Default Setting**
N/A

**Command Mode**
Manager

**Example**

HPswitch#support save-cli
CLI command tree is saved as clitree.html.
This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
HPswitch#

**support set**

This command sets service parameters.

**Syntax**

    support set (command-history | reboot-history | upgrade-history)

- command-history - Set size of command history. Default: 200.
  - <10-300> - History size.
- reboot-history - Set size of reboot history. Default: 50.
  - <10-100> - History size.
• upgrade-history - Set size of upgrade history. Default: 50.
  – <10-100> - History size.

Default Setting
command-history (200), reboot-history (50), and upgrade-history (50)

Command Mode
Manager

Example

HPswitch#support set command-history 100
HPswitch#

support show

This command shows running system information.

Syntax

support show (autoinstall-status | chassis | cli | command-history | cpu | crash-info | diag | info | last-passwd | pm | process | reboot-history | rp | sessions | startup-log | temperature | upgrade-history | wireless)

• autoinstall-status - Auto-install status.
• chassis - Chassis Details.
• cli - Shows CLI tree of current mode.
• command-history - Displays command (except show commands) history.
• cpu - Display system load.
• crash-info - Displays information about core, panic and AP dump files.
  – PANIC_FILENAME - Show contents of specified kernel panic file.
• diag - Diagnostics.
  – hardware - Shows the system hardware configuration.
  – limits - Shows limit values.
  – period - Shows the period (ms) for the in service diagnostics.
  – stats - Shows the current diagnostics statistics.
  – top - Shows top processes.
  – watchdog - Shows watchdog status.
• info - Shows snapshot of available support information.
• last-passwd - Displays last password used to enter shell.
• memory - Shows memory statistics.
ProCurve Wireless Services zl Module Command Line Reference
Support Commands (All Contexts)

- **pm** - Process Monitor.
  - **history** - States changes for a process, the time they happened and the events that triggered them.
  + **WORD** - Process name.
  + **all** - All processes.
- **process** - Displays process activity in real time.
- **reboot-history** - Shows reboot history.
- **rp** - Radio-port serviceability parameters.
  - **adopt-history** - Radio-port adopt-history.
  + **XX-XX-XX-XX-XX-XX** - Radio-port MAC.
- **startup-log** - Shows startup log.
- **temperature** - Displays CPU temperature.
- **upgrade-history** - Shows upgrade history
- **wireless** - Shows wireless parameters.
  - **rp** - Radio port serviceability parameters
  + **history** - Radio port history.

**Command Mode**

N/A

**Command Mode**

Manager

**Examples**

```
HPswitch#support show command-history
Configured size of command history is 100
Date & Time User Location Command
======================================================================
Feb 27 15:17:24 2006 0 vty 130 support set command-history 100
Feb 27 15:08:47 2006 0 vty 131 wireless
Feb 27 15:08:47 2006 0 vty 131 config t
Feb 27 15:08:47 2006 0 vty 131 interface eth0
Feb 27 15:08:47 2006 0 vty 131 config t
Feb 27 15:08:47 2006 0 vty 131 config t
Feb 27 15:02:25 2006 0 vty 130 support rp force-dump
Feb 27 14:59:01 2006 0 vty 130 support prompt crash-info
Feb 27 14:55:02 2006 0 vty 130 support pm sys-restart
Feb 27 14:37:54 2006 0 vty 131 support diag enable
```
A-195

ProCurve Wireless Services zl Module Command Line Reference
Support Commands (All Contexts)

HPswitch# support show info
4.0M out of 4.0M available for logs.
6.7M out of 8.2M available for history.
3.5M out of 4.8M available for crashinfo.
List of Files:
/var/log/messages.log 0   Feb 27 09:09
/var/log/startup.log  11.2k Feb 27 09:09
/var2/history/command.history 834    Feb 27 15:17
/var2/history/reboot.history 3.4k   Feb 27 09:09
/var2/history/upgrade.history 1.6k   Nov 22 15:18
Please export these files or delete them for more space.

HPswitch# support show rp adopt-history
<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Timestamp</th>
<th>Event</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-14-C2-A0-0B-05</td>
<td>Oct 19 10:19:22 2005</td>
<td>adoption</td>
<td>NULL</td>
</tr>
<tr>
<td>00-14-C2-A0-0B-05</td>
<td>Nov 22 17:38:20 2005</td>
<td>adoption</td>
<td>NULL</td>
</tr>
<tr>
<td>00-14-C2-A0-0B-05</td>
<td>Nov 22 15:26:18 2005</td>
<td>adoption</td>
<td>NULL</td>
</tr>
<tr>
<td>00-14-C2-A0-0B-05</td>
<td>Nov 22 08:49:42 2005</td>
<td>adoption</td>
<td>NULL</td>
</tr>
<tr>
<td>00-14-C2-A0-0B-05</td>
<td>Nov 22 08:08:51 2005</td>
<td>adoption</td>
<td>NULL</td>
</tr>
</tbody>
</table>

HPswitch# support show temperature
Value of temperature in degree C : 36

HPswitch# support show upgrade-history
Configured size of upgrade history is 50

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Old Version</th>
<th>New Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 22 15:17:32 2005</td>
<td>WS.01.XX.0551Swami~</td>
<td>WS.01.XX.0551Swami</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 21 13:09:25 2005</td>
<td>WS.01.XX.0551n</td>
<td>WS.01.XX.0551Swami</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 21 13:09:05 2005</td>
<td>WS.01.XX.0551n</td>
<td>WS.01.XX.0551n</td>
<td>Unable to get update file.</td>
</tr>
<tr>
<td>Nov 18 11:30:22 2005</td>
<td>WS.01.XX.0548n~</td>
<td>WS.01.XX.0551n</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 17 15:27:19 2005</td>
<td>WS.01.XX.0548n~</td>
<td>WS.01.XX.0548n~</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 17 15:17:28 2005</td>
<td>WS.01.XX.0548n~</td>
<td>WS.01.XX.0548n</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 15 16:43:22 2005</td>
<td>WS.01.XX.0548n~</td>
<td>WS.01.XX.0548n~</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 15 15:31:05 2005</td>
<td>WS.01.XX.0526n</td>
<td>WS.01.XX.0548n</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 15 15:26:06 2005</td>
<td>WS.01.XX.0526n</td>
<td>WS.01.XX.0526n</td>
<td>Unable to get update file.</td>
</tr>
<tr>
<td>Nov 02 17:15:16 2005</td>
<td>WS.01.XX.0526jim</td>
<td>WS.01.XX.0526n</td>
<td>Successful</td>
</tr>
<tr>
<td>Nov 02 12:16:54 2005</td>
<td>WS.01.XX.0526n</td>
<td>WS.01.XX.0526jim</td>
<td>Successful</td>
</tr>
<tr>
<td>Oct 31 10:42:48 2005</td>
<td>WS.01.XX.0505j</td>
<td>WS.01.XX.0526n</td>
<td>Successful</td>
</tr>
<tr>
<td>Oct 31 09:58:44 2005</td>
<td>WS.01.XX.0505j</td>
<td>WS.01.XX.0505j</td>
<td>Bad file, image header</td>
</tr>
</tbody>
</table>

-- MORE --, next page: Space, next line: Enter, quit: Control-C
Support Commands (Wireless)

This section details the support commands available for the Wireless parameters.

support wireless dump-core

This command creates a core file of the ccsrvr process.

Syntax

support wireless dump-core

Default Setting

Enabled

Command Mode

Manager

Example

HPswitch(config-wireless)#support wireless dump-core
HPswitch(config-wireless)##

support wireless dump-state

This command creates a ccsrvr.dump file in nvram with internal state information.

Syntax

support wireless dump-state

Default Setting

Enabled

Command Mode

Manager

Example

HPswitch(config-wireless)#support wireless dump-state
HPswitch(config-wireless)##
support wireless rate-scale

This command enables wireless rate scaling. The no command negates the configuration of the wireless parameters.

Syntax

```
support wireless rate-scale
no support wireless rate-scale
```

- rate-scale - Enable wireless rate scaling (default).

Default Setting

Enabled

Command Mode

Manager

Example

```
HPswitch(config-wireless)#support wireless rate-scale
HPswitch(config-wireless)#
```

support wireless request-rp-log

This command requests a radio port log.

Syntax

```
support wireless request-rp-log (<1-48>)
```

- `<1-48>` - RP index.
  - file - output to file
  - log - output to syslog

Default Setting

Enabled

Command Mode

Manager

Example

```
HPswitch(config-wireless)#support wireless request-rp-log (<1-48>)
file
HPswitch(config-wireless)#
```
Appendix B

The Apache Software License, Version 1.1

Copyright (C) 1999 The Apache Software Foundation. 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 Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "log4j" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

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 THE APACHE SOFTWARE FOUNDATION 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 software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.
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
---------------

Copyright (c) 1998-2005 The OpenSSL Project. 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. 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
EXRESSED 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 rouines 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.]

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1996, 1998-2000 The Regents of the University of California
All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE 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.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----
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.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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 the name of the Sun Microsystems, Inc. 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 THE COPYRIGHT HOLDERS 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.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc
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 the name of Sparta, Inc 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 THE COPYRIGHT HOLDERS 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.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. 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 the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their 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 THE COPYRIGHT HOLDERS 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
Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl>
Copyright (c) 1993 Branko Lankester <branko@hacktic.nl>
Copyright (c) 1993 Ulrich Pegelow <pegelow@moorea.uni-muenster.de>
Copyright (c) 1995, 1996 Michael Elizabeth Chastain <mec@duracef.shout.net>
Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com>
Copyright (c) 1998-2001 Wichert Akkerman <wakkerma@deephackmode.org>
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 of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

$Id: COPYRIGHT,v 1.3 2002/03/31 18:43:00 wichert Exp $
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 names of the authors and copyright holders may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "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 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.

License: BSD

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 names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Linux LOader (LILO) program code, documentation, and auxiliary programs are
Copyright 1999-2004 John Coffman.
All rights reserved.

License
-------

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 the names of the author(s) nor the names of other contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

Disclaimer
----------

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 THE AUTHORS 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.

(Note: The above license is copied from the BSD license at:
   http://www.opensource.org/licenses/bsd-license.html,
   substituting the appropriate references in the template.)

Copyright (c) 1998-2003,2004 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, distribute with modifications, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

(c) Copyright 2003-2005 Matt Messier and John Viega
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 the name of the primary nor the names of the 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 THE COPYRIGHT OWNER 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.
thttpd.c - tiny/turbo/throttling HTTP server

Copyright 1995, 1998, 1999, 2000, 2001 by Jef Poskanzer <jef@mail.acme.com>. 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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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 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.
This software is provided "AS IS", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly        Mark Adler
jloup@gzip.org          madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)    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".

      [Tatu continues]
      However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most
restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY
-------------

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.

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.

2) The 32-bit CRC compensation attack detector in deattack.c was
Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>
<http://www.core-sdi.com>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

    Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "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 AUTHORS 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.
5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

The Regents of the University of California. 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. Neither the name of the University 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 REGENTS 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 THE REGENTS 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.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42):
<phk@login.dknet.dk> wrote this file. As long as you retain this
notice you can do whatever you want with this stuff. If we meet
some day, and you think this stuff is worth it, you can buy me a
beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995
This code is based on code written by Patrick Powell
(papowell@astart.com) It may be used for any purpose as long as this
notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)
Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller
Theo de Raadt
Damien Miller
Eric P. Allman
The Regents of the University of California

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. Neither the name of the University 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 REGENTS 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 THE REGENTS 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.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.
Todd C. Miller

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, 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.
Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

$OpenBSD: LICENCE,v 1.19 2004/08/30 09:18:08 markus Exp $

This file is automatically generated from html/copyright.html

Copyright Notice
jpg "Clone me," says Dolly sheepishly
Last update: 15:44 UTC Tuesday, July 15, 2003

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.
The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. [1] Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
2. [2] Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
4. [5] Michael Barone <michael.barone@lmco.com> GPSVME fixes
5. [6] Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
6. [7] Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8] Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
8. [9] Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10] Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSP clock driver, Trimble PARSE support
10. [11] Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
11. [12] Steve Clift <clift@ml.csiro.au> OMEGA clock driver
12. [13] Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
15. [16] Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
16. [17] Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
17. [18] John Hay <jhay@lcomtek.csir.co.za> IPv6 support and testing
18. [19] Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
19. [20] Mike Iglesias <iglesias@uci.edu> DEC Alpha port
20. [21] Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
21. [22] Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
22. [23] Hans Lambermont  <Hans.Lambermont@nl.origin-it.com> or
23. [24] <H.Lambermont@chello.nl> ntpsweep
23. [25] Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
24. [26] Frank Kardel <Frank.Kardel@informatik.uni-erlangen.de> PARS <GENERIC> driver (14 reference clocks), STREAMS modules for PARS, support scripts, syslog cleanup
25. [28] William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
26. [29] Dave Katz <dkatz@cisco.com> RS/6000 AIX port
27. [30] Craig Leres <leres@ee.1bl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
28. [31] George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
29. [32] Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
30. [33] Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
31. [34] Danny Mayer <mayer@ntp.org> Network I/O, Windows Port, Code Maintenance
33. [36] Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
34. [37] Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
35. [38] Tom Moore <tmoore@flevel.daytonoh.nrc.com> i386 svr4 port
36. [39] Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
37. [40] Derek Mulcahy <derek@toybox.demon.co.uk> and [41] Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
38. [42] Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
39. [43] Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
40. [44] Wilfredo Schez <wsanchez@apple.com> added support for NetInfo
41. [45] Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
42. [46] Jack Saaportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
43. [47] Ray Schnitzler <schnitz@unipress.com> Unixware1 port
44. [48] Michael Shields <shields@tembel.org> USNO clock driver
45. [49] Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
46. [50] Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
47. [51] Kenneth Stone <ken@sdd.hp.com> HP-UX port
48. [52] Ajit Thyagarajan <ajit@ee.udel.edu> IP multicast/anycast support
49. [53] Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp> TRAK clock driver
50. [54] Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
51. [55] Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

References
-----------

1. mailto:%20mark_andrews@isc.org
2. mailto:%20altmeier@atsoft.de
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, 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.

Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
<info@isc.org>
http://www.isc.org/

This package, the EXT2 filesystem utilities, are made available under the GNU Public License.

However, I request that if the version string in the file version.h contains the string "pre-", or "WIP" that this version of e2fsprogs be distributed in source form only. Please feel free to give a copy of the e2fsck binary to help a friend recover his or her filesystem, as the need arises. However, "pre" or "WIP" indicates that this release is under development, and available for ALPHA testing. So for your protection as much as mine, I'd prefer that it not appear in a some distribution --- especially not a CD-ROM distribution!

The most recent officially distributed version can be found at http://e2fsprogs.sourceforge.net. If you need to make a distribution, that's the one you should use. If there is some reason why you'd like a more recent version that is still in ALPHA testing for your distribution, please contact me (tytso@mit.edu), and we will very likely be able to work out something that will work for all concerned. The release schedules for this package are flexible, if you give me enough lead time.

Theodore Ts'o
15-Mar-2003
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 proprietary. To prevent this, we have made it clear that anyprogram will
individually obtain patent licenses, in effect making the
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) <year> <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) year 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 1989
Ty 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.
GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 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.

[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

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 Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it. You can use it for
your libraries, 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 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 a program 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.

Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library. If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
version, 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 companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free this as regards changes in header files, but we have achieved it as regards libraries that are incorporated in them. (We have not seen how to achieve changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

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, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.
GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library 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 offer warranty 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 compile 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) 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.

   c) 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.

   d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

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 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.

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
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 to 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 Library 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 Library 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
Library General Public License for more details.

You should have received a copy of the GNU Library 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 1990
Ty Coon, President of Vice

This file contains the copying permission notices for various files in the GNU C Library distribution that have copyright owners other than the Free Software Foundation. These notices all require that a copy of the notice be included in the accompanying documentation and be distributed with binary distributions of the code, so be sure to include this file along with any binary distributions derived from the GNU C Library.

All code incorporated from 4.4 BSD is distributed under the following license:

    Copyright (C) 1991 Regents of the University of California.
    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. [This condition was removed.]
4. Neither the name of the University 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 REGENTS 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 THE REGENTS 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 DNS resolver code, taken from BIND 4.9.5, is copyrighted both by
UC Berkeley and by Digital Equipment Corporation. The DEC portions are under the following license:

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, 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.

The Sun RPC support (from rpcsrc-4.0) is covered by the following license:

Copyright (C) 1984, Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED "AS IS" WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

The following CMU license covers some of the support code for Mach, derived from Mach 3.0:

Mach Operating System
Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Carnegie Mellon requests users of this software to return to

Software Distribution Coordinator
School of Computer Science
Carnegie Mellon University
Pittsburgh PA 15213-3890

or Software.Distribution@CS.CMU.EDU any improvements or extensions that they make and grant Carnegie Mellon the rights to redistribute these changes.

The file if_ppp.h is under the following CMU 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. Neither the name of the University 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 CARNEGIE MELLON UNIVERSITY 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 THE UNIVERSITY 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 following license covers the files from Intel's "Highly Optimized Mathematical Functions for Itanium" collection:

Intel License Agreement
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.

* The name of Intel Corporation may not 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.

The files inet/getnameinfo.c and sysdeps/posix/getaddrinfo.c are copyright (C) by Craig Metz and are distributed under the following license:

The Inner Net License, Version 2.00

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of the all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. [The copyright holder has authorized the removal of this clause.]
5. Neither the name(s) of the author(s) 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 its authors 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 the authors 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.

If these license terms cause you a real problem, contact the author.

This source code has been made available to you by IBM on an AS-IS basis. Anyone receiving this source is licensed under IBM copyrights to use it in any way he or she deems fit, including copying it, modifying it, compiling it, and redistributing it either with or without modifications. No license under IBM patents or patent applications is to be implied by the copyright license.

Any user of this software should understand that IBM cannot provide technical support for this software and will not be responsible for any consequences resulting from the use of this software.

Any person who transfers this source code or any derivative work must include the IBM copyright notice, this paragraph, and the preceding two paragraphs in the transferred software.

Copyright (c) 2001, Dr Brian Gladman, Worcester, UK. All rights reserved.

License terms
-----------

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.
ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

Copyright (c) 2004 Linus Torvalds <torvalds@osdl.org>
Copyright (c) 2004 Red Hat, Inc., James Morris <jmorris@redhat.com>

DISCLAIMER
-------

This software is provided "AS IS" with no explicit or implied warranties in respect of its properties including, but not limited to, correctness and fitness for purpose.

Issue Date: 29/07/2002
sFlow License

LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE REPRODUCING OR IN ANY WAY UTILIZING THE sFlow(R) SOFTWARE ("SOFTWARE") AND/OR ANY ACCOMPANYING DOCUMENTATION ("DOCUMENTATION") AND/OR THE RELATED SPECIFICATIONS ("SPECIFICATIONS"). YOUR REPRODUCTION OR USE OF THE SOFTWARE AND/OR THE DOCUMENTATION AND/OR THE SPECIFICATIONS CONSTITUTES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU MAY NOT REPRODUCE OR IN ANY WAY UTILIZE THE SOFTWARE OR THE DOCUMENTATION OR THE SPECIFICATIONS.

1. Definitions.

"Documentation" means the user manuals, training materials, and operating materials, if any, InMon provides to Licensee under this Agreement.

"InMon" means InMon Corporation, its affiliates and subsidiaries.

"Intellectual Property Rights" means any trade secrets, patents, including without limitation any patents covering the Software, copyrights, know-how, moral rights and similar rights of any type under the laws of any governmental authority, domestic or foreign, including all applications and registrations relating to any of the foregoing.

"Licensee Hardware" means all computers, routers, or other equipment owned or controlled by or on behalf of Licensee.

"Products" means any and all software applications, computers, routers, or other equipment manufactured by or on behalf of Licensee for the purpose of resale or lease to any other third party, or otherwise made available by Licensee free of charge.

"Software" means the sFlow(R) software programs, in source or binary code format, that Licensee licenses from InMon under this Agreement and any bug fixes or error corrections which InMon may provide to Licensee.

"Specifications" means the published specifications provided or otherwise made available by

"Trademark" means InMon's "sFlow(R)" trademark.

2. License Grant.

2.1 Software, Documentation and Specifications License Grant. InMon hereby grants to Licensee, under all of InMon's Intellectual Property Rights therein, a perpetual (subject to InMon's termination rights under Section 7 below), nonexclusive, royalty-free, worldwide, transferable, sublicensable license, to:

(i) use and reproduce the Software, the Documentation, and the Specifications;
(ii) modify the Software; (iii) implement the Specifications in the Products;
(iv) install the Software, or software in which the Specifications have been
implemented, on Licensee Hardware and Products, and (v) distribute any Products that include the Software, the Documentation, or software in which the Specifications have been implemented.

2.2 Trademark License. InMon hereby grants to Licensee a perpetual (subject to InMon’s termination rights under Section 7 below), nonexclusive, royalty-free, worldwide, transferable, sublicensable license to use the Trademark on or in connection with the Software, the Documentation, the Specifications and any software that implements the Specifications.

2.3 Restrictions. Licensee agrees that it will not use the Software in a way inconsistent with the license granted in Section 2.1. Further, Licensee agrees that, in exercising its rights under the license granted to it in this Agreement, Licensee will:

(i) strictly adhere to and fully comply with the Specifications; (ii) use the Trademark, and no other mark, to identify the Software, the Documentation, the Specifications and any Products that implement the Specifications; (iii) place, in a font or graphic design designated by InMon, the phrase "sFlow(R)" on any technical documentation, sales/marketing materials, catalogs, or other such materials relating to products it manufactures or markets which it has configured to be compatible with the Software or otherwise implement the Specifications; (iv) in connection with any Products shipped to or sold in other countries that include the Software or any software that implements the Specifications, comply with the patent and trademark laws and practice of such other country; and (v) not alter or impair any acknowledgment of copyright or trademark rights of InMon that may appear in or on the Software, the Documentation or the Specifications. In the event InMon determines that Licensee is not complying with its obligations under clauses (i)-(v) above, InMon shall notify Licensee of such non-compliance, and if Licensee fails to correct such non-compliance within three (3) months, InMon may immediately terminate this Agreement as provided under paragraph 7 below and pursue any and all actions and remedies as it deems necessary, including, but not limited to breach of contract.

3. Ownership. Except for the license expressly granted in Section 2, Inmon hereby retains all right, title, and interest in and to the Trademark and all its Intellectual Property Rights in the Software, the Documentation and the Specifications. Licensee obtains no rights hereunder in the Trademark, Software, Documentation or Specifications by implication, estoppel or otherwise. Licensee acknowledges that the Trademark, Software, Documentation and Specifications are being licensed and not sold under this Agreement, and that this Agreement does not transfer title in the Trademark, Software, Documentation or Specifications, or any copy thereof, to Licensee.

4. Support. Inmon shall have no obligation under this Agreement to (a) supply maintenance or support, bug fixes or error corrections to the Licensed Software, (b) supply future versions of the Licensed Software or (c) provide Licensed Software development tools to Licensee.

5. Warranty. INMON HEREBY DISCLAIMS ALL WARRANTIES, EITHER EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE TRADEMARK, THE SOFTWARE, THE DOCUMENTATION, THE SPECIFICATIONS. OR OTHERWISE, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS.
6. Limitation of Liability. IN NO EVENT SHALL INMON OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, INDIRECT OR EXEMPLARY DAMAGES WHATSOEVER, WHETHER RELATED TO OR ARISING OUT OF THIS AGREEMENT, THE TRADEMARK, THE SOFTWARE, THE DOCUMENTATION, THE SPECIFICATIONS, OR OTHERWISE, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES OR FOR ANY CLAIM OR DEMAND AGAINST LICENSEE BY ANY OTHER PARTY, OR OTHER PECUNIARY LOSS, EVEN IF INMON HAS BEEN ADVISED OF OR KNOWS OF THE POSSIBILITY OF SUCH DAMAGES.

7. Term and Termination. The term of this Agreement will begin on the Effective Date, which shall be deemed to be the date of delivery of the Software and/or Documentation and/or specifications to Licensee, and shall continue indefinitely unless and until terminated by Licensee's giving written notice of termination to InMon, or by InMon pursuant to InMon's termination rights as set forth in Section 2.3 above. Upon any termination of this Agreement, Licensee shall cease exercising its license rights under this Agreement, including the right to distribute Products that incorporate the Software or Documentation or that implement the Specifications. The rights and obligations contained in Sections 1, 3, 5, 6, 7, and 8 shall survive any termination of this Agreement.


8.1 Assignment. This Agreement shall be binding upon and inure to the benefit of the parties hereto and their permitted successors and permitted assigns. InMon will have the right to assign this Agreement without notice to Licensee. Licensee may assign or transfer (whether by merger, operation of law or in any other manner) any of its rights or delegate any of its obligations hereunder without the prior written consent of InMon, provided the assignee assumes in writing all of Licensee's obligations hereunder.

8.2 Notices. All notices permitted or required under this Agreement shall be in writing and shall be delivered in person or mailed by first class, registered or certified mail, postage prepaid, to the address of the party specified in this Agreement or such other address as either party may specify in writing. Such notice shall be deemed to have been given upon receipt.

8.3 Non-Waiver. No term or provision hereof shall be deemed waived, and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent or waiver, whether express or implied, shall not constitute a consent or waiver of, or excuse for any separate, different or subsequent breach.

8.4 Independent Contractor. The parties' relationship shall be solely that of independent contractors, and nothing contained in this Agreement shall be construed to make either party an agent, partner, representative or principal of the other for any purpose.

8.5 Choice of Law and Forum. This Agreement shall be governed by and construed under the laws of the State of California, without giving effect to such state's conflict of laws principles. The parties hereby submit to the personal jurisdiction of, and agree that any legal proceeding with respect to or arising under this Agreement shall be brought in, the United States District Court for
the Northern District of California or the state courts of the State of California for the County of San Francisco.

8.6 U.S. Government Licenses. The Software and Documentation are considered a "commercial item" as that term is defined at 48 C.F.R 2.101, or "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R 12.212 of the Federal Acquisition Regulations and its successors, and 48 C.F.R. 227.7202 of the DoD FAR Supplement and its successors.

8.7 Severability. If any provision of this Agreement is held to be unenforceable under applicable law, then such provision shall be excluded from this Agreement and the balance of this Agreement shall be interpreted as if such provision were so excluded and shall be enforceable in accordance with its terms. The court in its discretion may substitute for the excluded provision an enforceable provision which in economic substance reasonably approximates the excluded provision.

8.8 Compliance With Law. Licensee shall comply with all applicable laws and regulations (including privacy laws and regulations) having application to or governing its use and/or operation of the Software and agrees to indemnify and hold InMon harmless from and against any claims, damages, losses or obligations suffered or incurred by InMon arising from its failure to so comply.

8.9 Entire Agreement; Amendment. This Agreement constitutes the final, complete and entire agreement between the parties with respect to the subject matter hereof, and supersedes any previous proposals, negotiations, agreements, or arrangements, whether verbal or written, made between the parties with respect to such subject matter. This Agreement shall control over any additional or conflicting terms in any of Licensee's purchase orders or other business forms. This Agreement may only be amended or modified by mutual agreement of authorized representatives of the parties in writing.

InMon Corp.
580 California Street, 5th Floor, San Francisco, CA 94104
Phone: (415) 283-3260
URL: www.inmon.com
Email: info@inmon.com
Index

Numerics

5400zl Series
See wireless services-enabled switch

802.11
frame types … 1-56
management frames … 1-56
overview … 1-54
802.11 replay attack … 12-58
802.11a
defined … 1-54
radio adoption defaults for … 3-9
802.11b
defined … 1-55
radio adoption defaults for … 3-9
802.11g
802.11g only … 3-16
defined … 1-55
radio adoption defaults for … 3-9
802.11h … 1-55
802.1X … 1-25
client on radio port … 1-68, 1-74, 2-78
configuring on a WLAN … 4-34
dynamic VLANs with … 4-87
pre-authentication for … 9-3
RADIUS server settings … 4-42
station settings … 4-35
8200zl Series
See wireless services-enabled switch

A
access category
setting for WLAN manually … 4-111
WMM and … 4-92
accounting
overview … 4-68
RADIUS … 11-37
See also RADIUS accounting
syslog, for WLAN … 4-69
ACL
applying to interface … 7-26
applying to physical port … 7-26
configuration steps … 7-10
creating and choosing type … 7-10
dynamic or user-based … 1-36, 4-88
extended IP
defined … 7-3
destination IP filter … 7-22
ICMP filter … 7-19
protocol filter … 7-19
source address filter … 7-22
TCP/UDP port filter … 7-21
filters
overview … 7-5
MAC extended
defined … 7-4
encapsulated protocol filter … 7-25
priority filter … 7-25
VLAN ID filter … 7-25
MAC standard (filter)
allow list … 12-76
applying to a WLAN … 12-78
configuring … 12-76
defined … 7-4
deny list … 12-76
NAT
standard ACL for … 8-22
operation
physical port required … 7-26
types … 7-7
overview … 7-2
precedence
defined … 7-5
setting in extended IP … 7-18
setting in MAC extended … 7-24
setting in standard IP … 7-15
viewing in detailed statistics … 7-31
routing required for … 7-26
rules
creating … 7-13
creating for extended IP … 7-17
creating for MAC extended … 7-23
creating for standard IP … 7-14
overview … 7-4
standard IP
defined … 7-3
source address filter … 7-16
stateful … 7-2
strategies for creating … 7-8
types … 1-40, 7-3
viewing statistics … 7-29
action ID … 7-30
details … 7-30
protocol ID … 7-30
times used … 7-30

ACS
See auto-channel select

active mode
for redundancy group … 1-78, 10-4

address resolution table … 6-17

adoption
automatic versus manual … 2-70
failure, reasons for … 1-78

Layer 2
auto-provisioning … 2-58
connecting RP to infrastructure switch … 2-59
connecting RP to wireless services-enabled switch … 2-58
network requirements for … 2-58

Layer 3
compared to Layer 2 … 2-57
customizing RPs’ DNS request … 2-68
default DNS request … 2-64
DHCP option 189 … 2-65
DNS lookup … 2-67
network requirements for … 2-62
RP requirements for … 2-63
verifying … 2-69
messages RPs send … 1-68
overview … 2-57

preference ID
configuring for module … 10-28
certifying for specific radio … 3-33
configuring in radio adoption defaults … 3-19
defined … 2-76
radio pre-configured … 1-67, 3-30
redundancy group and … 10-5
unadopting a radio … 3-40
viewing adopted RPs … 12-37
viewing unadopted RPs … 12-38

advanced mode configuration
configuring a specific radio … 4-18
configuring radio adoption defaults … 4-15, 4-16
considerations … 4-11
enabling … 4-13
normal mode with … 4-22
overview … 4-11
primary WLAN … 4-18, 4-20
reasons for using … 4-12
reverting to normal mode … 4-23

AIFS
defined … 4-92
radio … 4-108
station … 4-104

alarms
acknowledging … 12-74
deleting … 12-73
exporting … 12-74
managing log … 12-71
SNMP traps required for … 2-109, 12-71
viewing details … 12-73

 Allow list
local MAC authentication … 12-76
Web-Auth
certifying … 4-41, 5-29
defined … 5-8
necessary addresses … 5-9

answer broadcast ESS option … 4-66

antenna
effect on coverage … 3-45
external, lowering transmit power … 3-14
internal … 1-53
mode … 3-18, 3-33

AP detection
allowing unapproved APs … 12-53
approved list … 12-54
dedicated detector, configuring … 3-29, 12-40
detector mode … 1-63
enabling … 12-40
lists of detected APs … 12-46
overview … 12-39
single-channel detector, configuring … 3-30, 12-40
single-channel versus dedicated detector … 12-41
triggering SNMP trap … 12-55
unapproved list … 12-51
unseen AP timeout … 12-43
unseen AP timeout … 12-43

arbitration interframe spacing number
See AIFSN

association flood attack … 12-58
attack checking … 1-38

authentication
802.1X … 1-25, 4-34
encryption options with … 4-48
local MAC … 4-34, 12-75
MAC standard ACL … 1-40
open-key … 4-49
options for WLAN ... 1-24
RADIUS MAC ... 1-28, 4-43
See also 802.1X
See also MAC authentication
See also Web-Auth
shared-key ... 4-75
Web-Auth ... 1-26, 4-39, 5-2
authentication failure attack ... 12-58
auto-channel select
    configuring for specific radio ... 3-32
    configuring in radio adoption defaults ... 3-13
running ... 3-37, 3-41
auto-provisioning ... 1-8, 2-58

B
basic rate settings
    802.11g only ... 3-16
    defined ... 3-16
    specifying for specific radio ... 3-32
    specifying in radio adoption defaults ... 3-16
basic service set ... 1-56
basic service set identifier
    See BSSID
beacon
    DTIM in ... 3-23
    information in ... 1-61
    setting interval for radio adoption defaults ... 3-23
    setting interval for specific radio ... 3-33
    SSID in ... 1-62, 4-9
        selecting ... 4-18, 4-20
bind DN and password ... 11-22
broadcast key ... 4-56, 4-57, 4-60
BSS ... 1-56
BSSID
    defined ... 1-58
    generated from base radio MAC ... 3-30
    radio ports, on ... 1-60
    WLANs assigned to ... 3-34

certificate
    CA-signed, uploading to module ... 2-181
    defined ... 1-45, 2-166
    deleting ... 2-184
    keys
        deleting ... 2-184
        public/private keys
            creating manually ... 2-191
            creating with Certificates Wizard ... 2-177
            defined ... 2-166
            deleting ... 2-184
            passphrase for ... 2-196
            transferring ... 2-193
        request
            creating ... 2-175
            saving ... 2-180
            specifying LDAP values for ... 2-178
        revocation list
            uploading ... 2-187
        self-signed
            creating ... 2-172
            specifying LDAP values for ... 2-174
            uses ... 2-166
        certificate revocation list, uploading ... 2-187
    Certificates Wizard
        accessing ... 2-170
        CA-signed certificate, uploading ... 2-181
        certificate request, creating ... 2-175
        deleting operations ... 2-184, 13-3
        public/private key, creating ... 2-173
        self-signed certificate, creating ... 2-172
    CGI commands
        Web-Auth pages on external server ... 5-37, 5-38
        Web-Auth pages on internal server,
            advanced ... 5-37, 5-38
    channel
        auto-channel select
            for radio adoption defaults ... 3-13
            for specific radio ... 3-32
            manually selecting ... 3-32
        CLI ... 2-21
            redundancy group configuration mode
                context ... 10-9
                saving changes in ... 2-23
                using ... 2-23
                wireless-services context ... 2-22
                write memory ... 2-23
    closed system
        defined ... 1-61
        enabling on WLAN ... 4-65
        primary WLAN and ... 1-62
    command line interface
        See CLI
configuration files
  deleting … 2-97
  managing … 2-86
  startup-config, returning to factory defaults … 2-98
  transferring … 2-89
  viewing … 2-87
contention window
  See CW Max
  See CW Min
counter polling
  defined … 13-3
  interval … 13-16
  manually activating … 13-14
country code … 2-136, 3-4
CRL
  uploading … 2-187
CW Max
  defined … 4-92
  radio … 4-108
  station … 4-104
CW Min
  defined … 4-92
  radio … 4-108
  station … 4-104
D
decryption attack … 12-58
default gateway
  single active … 2-8
  specifying in the CLI … 2-7
delivery traffic indication message
  See DTIM period
destination NAT
  configuring … 8-33
  overview and uses … 8-9
DFS … 1-55
DHCP
  extended option
    See extended DHCP option
DHCP exclusions … 6-32
DHCP pool
  associating with an interface … 6-27
  boot file … 6-28
  dynamic DNS for … 6-41
  host pool
    client ID for … 6-31
    creating … 6-28
    defined … 6-24
    lease time … 6-27
    NetBIOS node type … 6-28
    network pool
      creating … 6-24
      defined … 6-23
      servers … 6-27
DHCP relay
  configuring … 6-45
  gateway interface … 6-45, 6-47
  overrides server … 6-45
  overview … 6-45
  relayed interface … 6-45, 6-47
DHCP requests
  allowing in ACL … 7-1
  relaying to external server … 6-45
DHCP server
  dynamic IP address for module … 2-7
  internal
    BOOTP with … 6-35
    enabling … 6-33
    excluding addresses … 6-32
    extended options … 6-37
    host pools … 6-28
    network pools … 6-24
    overview … 6-22
    ping interval … 6-35
    pools … 6-23
    requirements for enabling on VLAN … 6-23
    See also DHCP pool
    See also extended DHCP option
    viewing leases … 6-43
    Web-Auth and … 5-3
DHCP services … 1-24
digital certificate
  See certificate
disassociation flood attack … 12-58
DNS
  dynamic … 6-41
    client update … 6-43
    server update … 6-43
    overview … 6-19
    servers
      adding … 6-19
      deleting … 6-21
domain name system
  See DNS
domain proxy RADIUS server
  settings for … 11-30
  specifying … 11-28
downlink port … 1-7, 1-8
DTIM period
  defined … 3-23
  different value for each BSSID … 3-34
  specifying for specific radio … 3-34
  specifying in radio adoption defaults … 3-24
dynamic DNS … 6-41
  client update … 6-43
  server update … 6-43
Dynamic Frequency Selection … 1-55
Dynamic Host Configuration Protocol
  See DHCP pool
  See DHCP relay
  See DHCP requests … 6-22
  See DHCP server … 6-22
dynamic index (radio) … 1-67, 3-30
dynamic NAT
  configuring … 8-26
  overview and uses … 8-5
dynamic VLAN assignment
  authentication required … 4-87
  considerations for … 4-87
  enabling … 4-87
  local group policies, in … 1-35, 11-26
  prohibited … 4-32

e
EAP … 1-25
EAP start frame attack … 12-58
encryption
  passwords and roaming … 2-106
  passwords in config … 2-105
  See also WEP
  See also WPA/WPA2
WLAN
  configuring … 4-47
  options for … 1-32
  error reporting … 2-109
ESS … 1-58
extended DHCP option
  adding to pool … 6-39
  defining … 6-37
  excluded codes … 6-38
  excluded names … 6-38
  overview … 6-37
extended IP ACL
  defined … 7-3
  destination IP filter … 7-22
  ICMP filter … 7-19
  protocol filter … 7-19
  source address filter … 7-22
  TCP/UDP port filter … 7-21
extended service set identifier … 1-58
external antenna
  mode for … 3-18
  self healing offset and … 3-24

f
failover
  standby mode … 1-78
fast Layer 2 roaming
  enabling … 4-58, 9-12
  overview … 9-3
  pre-authentication … 9-3
files
  browsing file systems … 2-34, 2-95
  configuration … 2-86
  software image … 2-82
  transferring … 2-89
  Web-Auth pages … 5-8
filter
  for local MAC authentication
    applying to a WLAN … 12-78
    combined with other authentication … 1-29
    configuring … 12-76
    defined … 12-75
    Web browser screen … 2-16
    creating … 2-17
    disabling … 2-21
    hiding … 2-21
firewall … 1-38
flash memory
  browsing … 2-34, 2-95
  logo files in … 5-33
  Web-Auth pages in … 5-8
flow sampling
  defined … 13-2
  manually activating … 13-11
  rate … 13-13
  sample size … 13-14
  See also sFlow

FTP server
  external
downloading files from … 2-89
  saving files to … 2-93
  internal … 2-32

G
  group
    internal RADIUS … 11-12
    See also RADIUS database
  group attribute … 11-24
  group filter … 11-23
  group membership attribute … 11-24

H
  hardware ID … 2-128
  help, online … 2-14
  hidden stations
    defined … 3-21
    setting RTS threshold for
      radio adoption defaults … 3-22
      specific radio … 3-33
  high availability
    See redundancy group
  hostname
    definition … 6-19
  HTTPS
    access … 2-24
    certificate … 1-46, 2-166

I
  Identity Driven Manager (IDM) … 1-35, 4-88
  inactivity timeout … 4-67
  index type (radio) … 1-67, 3-30
  indoors radio
    specifying for specific radio … 3-32
    specifying in radio adoption defaults … 3-12
  infrastructure mode … 1-57

interface
  DHCP pool … 6-27
  DHCP relay … 6-45
  DHCP relay (gateway) … 6-45
  VLAN … 6-3
  WLAN mapped to … 4-30
  interference avoidance
    auto-channel select (ACS) with … 12-100
    average retries threshold … 12-100
    overview … 12-100
  interframe spacing number
    See AIFS
  inter-station blocking … 4-63
  IP address
    address resolution table … 6-17
    compared to hostname … 6-19
    dynamic, for module … 2-7
    management in module … 6-3
    maximum on module … 1-17
    static, for module … 2-6, 2-7
    VLAN … 1-17
      assigning … 6-5
      editing … 6-7
      viewing … 6-7, 6-10
  IP routing
    capabilities requiring … 6-12
    enabling … 6-12

K
  key
    certificate, for
      See public/private keys
    license … 2-128
    multicast … 4-56
    static WEP … 4-51
    WPA/WPA2-PSK … 4-59

L
  Layer 2 adoption
    auto-provisioning … 2-58
    connecting RP to infrastructure switch … 2-59
    connecting RP to wireless services-enabled
      switch … 2-58
    network requirements for … 2-58
    of radio ports … 1-68
Layer 3 adoption
- compared to Layer 2 ... 2-57
- customizing RPs’ DNS request ... 2-68
- default DNS request ... 2-64
- DHCP option 189 ... 2-65
- DNS lookup ... 2-67
- network requirements for ... 2-62
- of radio ports ... 1-68
- RP requirements for ... 2-63
- verifying ... 2-69
Layer 3 device
- module as a ... 6-3
Layer 3 mobility
- configuration steps ... 9-15
- dynamic VLANs with ... 9-15
- enabling ... 9-20
- enabling on a WLAN ... 9-18
- IDM location domain with ... 9-7
- IP address, for local module ... 9-16
- monitoring stations ... 9-26, 12-10
- overview ... 9-6
- peers ... 9-19
- messages to and from ... 9-23
- monitoring ... 9-22
- tunneling with ... 9-7
- when required ... 9-5
LDAP server
- binding RADIUS server to ... 11-22
- bind DN and password ... 11-22
- group attribute ... 11-24
- group filter ... 11-23
- group membership attribute ... 11-24
- password attribute ... 11-23
- steps ... 11-20
- user login filter ... 11-22
- specifying as RADIUS data source ... 11-9
license key ... 2-128
licenses, radio port
- installing ... 2-127, 2-128
- maximum ... 2-122
- overview ... 1-50, 2-122
- uninstalling ... 2-127, 2-132
LLDP
- configuring RP’s name ... 3-41
- RPs’ messages ... 1-68
logging
- alarms ... 12-71
- events ... 12-63
- events versus alarms ... 12-64
- forwarding to server ... 12-65
- overview ... 12-63
- See also alarms
- severity ... 12-63
- to buffer (local file) ... 12-64
- to console ... 12-64
- transferring local file ... 12-69
- viewing local file ... 12-66
logo
- copying to internal flash ... 5-33
- failed page, on ... 5-23
- login page, on ... 5-16, 5-17
- welcome page, on ... 5-20
M
MAC address
- address resolution table ... 6-17
- RP Ethernet ... 12-37
- RP radio ... 3-30
- station’s ... 12-5
MAC authentication
- local ... 12-75
- MAC standard ACL ... 1-40
- overview ... 1-28
RADIUS
- configuring ... 4-43
- defined ... 4-34
- format ... 4-47
- protocol ... 4-46
- server for ... 11-36
- server settings ... 4-46
management interfaces
- CLI ... 2-21
- options ... 2-5
- SNMP applications ... 2-5
- Web browser interface ... 2-5
management VLAN
- secure ... 2-9, 2-29
- specifying ... 2-8
manager user
- changing password ... 2-35
- logging in as ... 2-11
- SNMP v3 and ... 2-25
marking traffic … 7-7
extended IP ACL … 7-19
MAC extended ACL … 7-24
overview … 7-7
physical port required … 7-26
standard IP ACL … 7-16
module statistics
button … 12-27
screen … 12-34
multicast address … 4-113
multicast key … 4-56
My ProCurve Web Portal
registering on … 2-127

N
NAT
applying to an interface … 8-24
collection steps … 8-24
defining interface for … 8-24
destination
configuring … 8-33
uses … 8-9
dynamic
ACL for … 8-22, 8-28
configuring … 8-26
overloaded interface … 8-28
port address translation … 8-8
uses … 8-5
global address
defined … 8-4, 8-12
specifying for destination … 8-36
specifying for source … 8-32
interface type
defining a VLAN’s … 8-24
dynamic NAT, for … 8-28
inside versus outside … 8-3
static NAT, for … 8-31, 8-35
local address
defined … 8-4, 8-12
specifying for destination … 8-36
specifying for source … 8-31
overview … 1-43, 8-3
planning the configuration … 8-15
port forwarding … 8-10
local port … 8-36
protocol … 8-36
port translation … 8-37
source
configuring dynamic … 8-26
configuring static … 8-30
static
configuring, destination … 8-33
configuring, source … 8-30
defined … 8-8
types … 1-43
uses for … 1-44
viewing sessions … 8-38
neighbor recovery … 12-89
automatically detecting neighbors … 12-94
enabling … 12-90
failure of radio … 12-89
manually specifying neighbors … 12-92
monitoring neighbors … 12-89
self healing action
opening data rates … 12-95
raising transmit power … 12-95
self healing offset … 3-24, 12-98
Network Address Translation
See NAT
normal mode configuration
enabling more than four WLANs … 4-7
overview … 4-4
NTP
See secure NTP

O
online help … 2-14
open-key authentication … 4-49
operator user
changing password … 2-35
SNMP v3 and … 2-26
opportunistic key caching
defined … 9-3
enabling … 4-58, 9-14
outdoors radio
specifying for specific radio … 3-32
specifying in radio adoption defaults … 3-12

P
packet sampling … 13-2
See also flow sampling
See also sFlow
Index – 9

password
  changing manager or operator … 2-35
  encryption
    in config … 2-105
    roaming and … 2-106
See also key
  Web browser interface … 2-11
password attribute … 11-23
PKI … 1-45
PMK caching
  defined … 9-3
  enabling … 4-58, 9-14
  required for pre-authentication … 9-14
PoE … 1-75
port address translation … 8-8
  See also NAT … 8-8
port authentication … 1-74
power over Ethernet … 1-75
power save
  DTIM period … 3-23, 3-34
  viewing station support for … 12-5
pre-authentication
  enabling … 4-58, 9-14
  overview … 9-3
  PMK caching required for … 9-14
precedence
  ACLs, for … 7-5, 7-15
primary WLAN … 4-9, 4-20
proxy ARP … 4-75
public/private keys
  creating manually … 2-191
  creating with Certificates Wizard … 2-177
  passphrase for … 2-196
  transferring … 2-193

Q
QoS
  classifying WLAN traffic … 4-111
  mapping value to access category … 4-108
  marking traffic for a value … 7-7
    extended IP ACL … 7-19
    MAC extended ACL … 7-24
    physical port required … 7-26
    standard IP ACL … 7-16
  mechanisms supported by the module … 4-90
  overview … 1-46, 4-89
See also WMM
  QoS mapping … 4-108

R
radio
  adoption default configuration … 1-65, 3-8
  advanced properties … 3-17
  antenna mode … 3-18
  beacon interval … 3-23
  channel … 3-13
  DTIM period … 3-23
  maximum stations … 3-19
  rate settings … 3-15
  RTS threshold … 3-21
  screen … 3-6
  self healing offset … 3-24
  short preamble … 3-21
  transmission power … 3-14
antenna … 3-18
auto-channel select (ACS) … 3-36
configured before adoption … 1-67, 3-27, 3-30
configuring a specific radio … 1-67, 3-25
  advanced properties … 3-33
  antenna mode … 3-33
  beacon interval … 3-33
  channel … 3-32
  dedicated detector … 3-29
  DTIM period … 3-34
  maximum stations … 3-33
  placement … 3-32
  rate settings … 3-32
  screen … 3-6
  self healing offset … 3-33
  short preamble … 3-33
  single-channel detector … 3-30
  transmission power … 3-32
configuring multiple radios … 3-36
  description … 3-29
  detector mode … 1-63
  failure … 12-89
  index type … 1-67, 3-30
  placement … 3-12
  resetting … 3-38
  returning to adoption defaults … 3-40
  state … 3-27, 3-29
  viewing RF output … 3-32
  viewing settings … 3-32

Index – 9
radio port ... 1-53, 3-2
802.1X authentication
configuring ... 2-79
overview ... 2-78

adoption
automatic ... 2-70
boot code for ... 2-65
DNS name for Layer 3 ... 2-68
in redundancy group ... 10-5
Layer 2 ... 2-58
Layer 3 ... 2-62
manual ... 2-70, 2-72
adoption preference ID ... 3-19
BSSID ... 1-60
configuring ... 3-5
deleting, or unadopting ... 3-40
deployment requirements ... 1-75
detector mode for radio ... 1-63
failure ... 12-89
licenses ... 1-50, 2-122
additive ... 1-51, 2-122
hardware ID ... 2-128
installing ... 2-127, 2-128
license key ... 2-128
radio port ... 2-135
redundancy group and ... 10-6
registration ID ... 2-128
uninstall verification key ... 2-128
uninstalling ... 2-127, 2-132
load balancing in redundancy group ... 10-5
resetting ... 3-39
See also Radio Port VLAN
traffic ... 1-53
traffic, encapsulated ... 1-53
viewing bootloader version ... 12-37
viewing hardware version ... 12-37
viewing protocol version ... 12-37
viewing software version ... 12-38
VLAN ... 2-58
default ... 2-58
on infrastructure switch ... 2-59
radio port adoption
See adoption ... 2-57
Radio Port VLAN ... 1-8
auto-provisioning ... 1-8
dynamic ... 1-12
manual ... 1-10
RADIUS accounting
enabling on WLAN ... 4-71
internal server ... 11-39
logged information ... 11-38
modes ... 4-74, 11-37
RADIUS authentication required for ... 4-72
retries ... 4-74
specifying server for ... 4-73
timeout ... 4-74
viewing logs on the internal server ... 11-43
RADIUS database
configuring local ... 11-12
group policy ... 11-12
group policy with LDAP ... 11-24
user accounts ... 11-15
guest ... 2-50, 11-16
normal ... 11-15
RADIUS server
802.1X, for ... 4-42
external
shared secret ... 4-38
Web-Auth, for ... 5-5, 5-14
internal ... 1-30
access times in group policy ... 11-14
authenticating wired stations ... 11-31
authenticating wireless stations ... 11-33
CA certificate ... 11-8
certificate (server) ... 11-8
clients ... 11-31
configuration steps ... 11-4
data source for ... 11-9
domain proxy server ... 11-28, 11-30
dynamic VLAN assignment ... 11-13
EAP method for 802.1X ... 11-5, 11-6, 11-11
enabling for a WLAN ... 11-33
group policy ... 11-12
group policy with LDAP ... 11-24
LDAP server and ... 11-9, 11-19
local database ... 11-9, 11-12
overview ... 11-3
See also RADIUS database
shared secret for ... 11-36
starting ... 11-32
stopping ... 11-32
user accounts ... 2-50, 11-15
Web-Auth, for ... 11-36
WebUser Administrator access to ... 2-49
MAC authentication, for ... 4-44, 11-36
overview ... 11-2
Web-Auth, for ... 4-41, 5-13
rate limit, user-based ... 4-88
rate settings
802.11b support ... 3-16
basic ... 3-16
cell size and ... 3-45
specifying for specific radio ... 3-32
specifying in radio adoption defaults ... 3-15
supported ... 3-16
re-authentication ... 4-38, 4-46
reconnaissance attack ... 12-58
redundancy
software image failover ... 2-81, 2-83
redundancy group ... 1-76
active mode ... 10-4
RP adoption ... 10-5
configuration mode context ... 10-9
configuring ... 10-11
defined ... 10-3
enabling ... 10-16
example of ... 10-4
failover capabilities explained ... 10-2
history of events ... 10-21
licenses for RPs ... 10-6
members
adding ... 10-14
matching configurations ... 10-9
maximum number ... 10-3
monitoring ... 10-22
typical combination ... 10-3
process of establishing ... 10-7
radio ports
adoption of ... 10-5
adoption preference ID ... 10-28
licenses ... 2-135
load balancing ... 10-5
view adopted ... 10-19
view licenses ... 10-19, 10-23
view, adopted by other member ... 10-23
reverting RPs ... 10-33
Spanning Tree Protocol (STP) with ... 10-14
standby mode ... 10-4
RP adoption ... 10-6
viewing information about ... 10-18
Redundant Wireless Services zl Module
capabilities of ... 10-2
model ... 1-76
radio ports
adoption in redundancy group ... 10-6
redundancy group and ... 1-76, 10-3, 10-4
See also redundancy group
registration ID ... 2-128
reset
radio ... 3-38
radio port ... 3-39
retries
interference avoidance threshold ... 12-100
viewing average, for a radio ... 12-20
viewing average, for a station ... 12-12, 12-27
Revert button ... 2-13
RF utilization ... 12-20
roaming
achieving best ... 9-10
behavior based on security ... 9-8
counter for station ... 12-10
fast Layer 2
enabling ... 4-58, 9-12
overview ... 9-3
pre-authentication ... 9-3
Layer 2 ... 1-81, 1-82, 9-2
Layer 3 ... 1-84, 9-5
See also Layer 3 mobility
seamless coverage ... 3-44
Web-Auth and ... 5-2, 9-4
route table
default route ... 6-15
one active ... 6-16
overview ... 6-12
static routes in ... 6-14
routing ... 1-23
capabilities requiring ... 6-12
enabling ... 6-12
RP
See radio port
running-config
applying changes to ... 2-13
secure management … 2-9, 2-29
secure Network Time Protocol
   See secure NTP
secure NTP
   ACLs controlling access to … 2-146
      authentication … 2-141
   broadcast mode … 2-139
   client/server mode … 2-139
   configuration steps
      client … 2-142
      server … 2-142
   hierarchy … 2-139
   overview … 2-138
   peer mode … 2-139
Secure Shell access … 2-24
security
   adopting RPs as detectors … 3-11
   authentication … 4-33
   encryption … 1-32, 4-19, 4-47
   for management access … 2-24
   See also authentication
   See also encryption
   WLAN … 4-33
self healing … 12-89
   interference avoidance … 12-100
      See also interference avoidance
   neighbor recovery … 12-89
      See also neighbor recovery
offset
   radio adoption defaults … 3-24
   specific radio configuration … 3-33
serial session
   accessing CLI through … 2-21
sFlow
   agent, viewing … 13-7
   collector … 13-2
   converting 802.11 to Ethernet … 13-11
   counter polling
      defined … 13-3
      interval … 13-16
      manually activating … 13-14
flow sampling
   defined … 13-2
   manually activating … 13-11
   rate … 13-13
   sample size … 13-14
   manual configuration steps … 13-8
   MIB version … 13-8
      overview … 1-50, 13-2
   receiver
      configuration options … 13-4
      defined … 13-2
      manually configuring … 13-8
      timeout … 13-10
   receiver, configured by … 13-5
   shared-key authentication … 4-75
short preamble
   enabling in radio adoption defaults … 3-21
   enabling on specific radio … 3-33
show ip interface command … 2-7
SNMP
   communities … 2-25, 2-109
   default support … 2-109
   receiver
      defining … 2-117
      editing … 2-122
      viewing information about … 2-121
   security … 2-24
      encrypted communications … 2-25
      users … 2-24
   statistics … 2-111
   thresholds … 2-116
   traps … 2-109
      disabling … 2-115
      enabling … 2-112
      v3, controlled by … 2-26, 2-110
   version … 2-24, 2-29
      version 3
      default users … 2-35
      manager … 2-35
      operator … 2-35
      Web-Users … 2-40
Web-Users
   authenticating … 2-44
   creating … 2-42
   roles … 2-41
snmptrap user
   default password … 2-120
software image … 2-81
   failover capabilities … 2-83
   selecting, used to boot … 2-83
   updating manually … 2-85
   viewing … 2-82
source NAT
- configuring dynamic … 8-26
- configuring static … 8-30
- uses for dynamic … 8-5
- uses for static … 8-12

SSH access … 2-24

SSID
- assigned to BSSID
  - normal mode … 3-34, 4-4, 4-11
  - defined … 1-59
- selecting beaconed SSID … 4-18, 4-20
- WLAN and … 4-30, 4-31

standard IP ACL
- defined … 7-3
- source address filter … 7-16

standby mode
- for redundancy group … 1-78, 10-5

startup-config
- factory default … 2-86
- returning, to factory defaults … 2-98
- saving changes in CLI … 2-23
- saving changes to … 2-12, 2-13
- viewing … 2-88

stateful
- ACLs … 7-2
- static index (radio) … 1-67, 3-30

static NAT
- configuring … 8-29
- overview and uses … 8-8

station
- See wireless station

station intrusion detection
- overview … 12-58
- reporting to SNMP server … 12-60
- thresholds … 12-59
- time to filter … 12-60
- viewing blocked stations … 12-62

supported rate settings
- specifying for specific radio … 3-32
- specifying in radio adoption defaults … 3-16

SVP … 1-48, 3-48, 4-90

switch, infrastructure
- radio port VLAN on … 2-59

syslog
- accounting
  - enabling on WLAN … 4-69
  - server, forwarding logs to … 12-65

system time
- manual configuration … 2-136
  
  See also secure NTP

T

TKIP attack … 12-58

TPC … 1-55

Transmit Ops
- defined … 4-92
- radio … 4-108
- station … 4-104

Transmit Power Control … 1-55

trustpoint
- components … 2-167
- defined … 2-166
- deleting … 2-184
- LDAP values
  - for certificate request … 2-178
  - for self-signed certificate … 2-174
  - transferring … 2-187

U

uninstall verification key … 2-128

Update Server
- configuring … 2-104
- explained … 2-98
- guidelines for using … 2-100
- redundancy group config … 2-105
- software image … 2-105
- startup-config file … 2-105
- upgrades
  - software image … 2-85
- uplink port … 1-7, 4-88
  - tagging … 4-86
- uplink VLAN … 1-12, 4-33
- user
  - CLI … 2-7
- user login filter … 11-22
- user-based policies … 1-35
- username
  - Web browser interface … 2-11
WebUser Administrator
adding guest accounts as … 2-50
creating … 2-42
defined … 2-42
deleting guest accounts as … 2-53
printing guest accounts as … 2-55
viewing guest accounts as … 2-53
Web-Users
authenticating … 2-44
creating … 2-42
roles … 2-41
WEP
dynamic (802.1X) … 4-52
open-key authentication … 4-49
shared-key authentication … 4-75
static … 4-48
key length … 4-52
specifying key … 4-50
Wi-Fi Protected Access
See WPA/WPA2
Wired Equivalent Privacy
See WEP
Wireless Edge Services zl Module
accessing CLI … 2-7
accessing Web browser interface … 2-9
IP address … 2-6
model … 1-76
redundancy group … 10-2
route table … 6-12
RP licenses for … 1-50, 2-122
software image … 2-81
system time … 2-138
wireless intrusion detection
See station intrusion detection
wireless LAN
See WLAN
wireless multimedia
See WMM
wireless multimedia (WMM) … 1-48
Wireless Services Module 12 RP License … 2-122
installing … 2-127
PCM, managed by … 2-127
uninstall verification key … 2-128
uninstalling … 2-132
wireless services-enabled switch
auto-provisioning of radio port VLAN … 2-58
Web browser interface for … 2-10
wireless station
disconnecting … 12-6
traffic … 12-12
viewing … 12-4
details … 12-7
IP address … 12-5
MAC address … 12-5
viewing VLAN … 12-6
WMM support … 12-9
wireless traffic
viewing all statistics for the module … 12-34
viewing statistics for a radio … 12-19
viewing statistics for a station … 12-12
viewing statistics for a WLAN … 12-26
wireless-services context
in CLI … 2-22
WISP heartbeats
radio ports … 12-90
WLAN
assigned to BSSID … 3-34, 4-11
authenticating to internal RADIUS server … 11-33
choosing primary on BSSID … 4-18, 4-20
closed system … 4-65
configuration tasks … 4-26
defined … 1-5
enabling … 4-76
enabling more than 16 … 4-13
enabling more than four … 4-7
inactivity timeout … 4-67
Layer 3 mobility for … 9-18
manually assigning to radio … 4-18
manually assigning to radio adoption
defaults … 4-15, 4-16
security for … 4-33
SSID … 4-31
viewing … 4-27
VLAN, mapped to
considerations … 4-84
specifying … 4-32
VLAN Assignment tab … 4-82
WMM
  802.1p
    mapping to access category … 4-93, 4-108, 4-109
    selecting for wireless stations … 4-99
  access category … 4-92
  DSCP
    mapping to access category … 4-93, 4-108, 4-109
    selecting for wireless stations … 4-99
  enabling on a WLAN … 4-95
  overview … 4-91
  prioritization … 1-48, 3-46
  priority queuing … 4-92
  QoS mapping … 4-108
  queue parameters
    customizing for radios (adoption defaults) … 4-106
    customizing for radios (specific) … 4-106
    customizing for stations … 4-102
    defined … 4-92
    viewing stations’ … 4-100
  RP parameters … 3-47
  RP to wireless station … 4-93
  viewing station support for … 12-9
  wireless station to RP … 4-94
WPA/WPA2
  802.1X with (Enterprise mode) … 4-58
  broadcast key … 4-56, 4-57, 4-60
  multicast key … 4-56
  per-session key … 4-56
  selecting protocol … 4-54, 4-56, 4-59
  specifying preshared key … 4-59
  stations supported … 4-56