



# User Guide

ORiNOCO AP-700  
User Guide



**Proxim**  
wireless

**IMPORTANT!**

Before installing and using this product, see the *Safety and Regulatory Compliance Guide* located on the product CD.

## Copyright

© 2007 Proxim Wireless Corporation. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This User Guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Wireless Corporation.

## Trademarks

ORiNOCO and Proxim are registered trademarks, and the Proxim logo is a trademark, of Proxim Wireless Corporation.

Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Ekahau is a trademark of Ekahau, Inc.

HyperTerminal is a registered trademark of HilGraeve, Incorporated.

Microsoft and Windows are a registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

SolarWinds is a registered trademark of SolarWinds.net.

All other trademarks mentioned herein are the property of their respective owners.

## OpenSSL License Note

This product contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>) and that is subject to the following copyright and conditions:

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to refer to, endorse, or promote the products or for any other purpose related to the products without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

This software is provided by the OpenSSL Project "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the OpenSSL Project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

---

# Contents

<b>1</b>	<b>Introduction</b>	<b>8</b>
	Introduction to Wireless Networking	8
	Guidelines for Roaming	8
	Management and Monitoring Capabilities	9
	HTTP/HTTPS Interface	9
	Command Line Interface	9
	SNMP Management	10
	SSH (Secure Shell) Management	10
<b>2</b>	<b>Installation and Initialization</b>	<b>12</b>
	AP-700 Hardware Description	13
	Overview	13
	LED Indicators	13
	Power-over-Ethernet (PoE)	14
	Antennas	14
	Prerequisites	16
	System Requirements	16
	Product Package	17
	Hardware Installation	18
	Attach Cables	18
	Install the Security Cover (Optional)	20
	Mount the AP-700	20
	Power On the Unit	21
	Install External Antennas (Professional Installation Required)	22
	Initialization	25
	Using ScanTool	25
	Logging In	27
	Using the Setup Wizard	28
	Installing the Software	30
<b>3</b>	<b>System Status</b>	<b>34</b>
<b>4</b>	<b>Advanced Configuration</b>	<b>35</b>
	System	37
	Dynamic DNS Support	38
	Network	39
	IP Configuration	39
	DHCP Server	40
	DHCP Relay Agent	42
	Link Integrity	43

---

SNTP (Simple Network Time Protocol) . . . . .	44
Interfaces . . . . .	47
Operational Mode. . . . .	47
Wireless A (802.11a/b/g Radio) . . . . .	51
Ethernet . . . . .	59
Management . . . . .	61
Passwords . . . . .	61
IP Access Table . . . . .	62
Services . . . . .	62
Automatic Configuration (AutoConfig) . . . . .	68
Hardware Configuration Reset (CHRD) . . . . .	70
Filtering . . . . .	73
Ethernet Protocol . . . . .	73
Static MAC . . . . .	74
Advanced . . . . .	77
TCP/UDP Port . . . . .	79
Alarms . . . . .	82
Groups . . . . .	82
Syslog . . . . .	86
Rogue Scan . . . . .	89
Bridge . . . . .	93
Spanning Tree . . . . .	93
Storm Threshold. . . . .	94
Intra BSS . . . . .	95
Packet Forwarding . . . . .	95
QoS . . . . .	96
Wi-Fi Multimedia (WMM)/Quality of Service (QoS) Introduction . . . . .	96
Policy . . . . .	96
Priority Mapping . . . . .	98
Enhanced Distributed Channel Access (EDCA) . . . . .	99
Radius Profiles . . . . .	102
RADIUS Servers per Authentication Mode and per VLAN . . . . .	102
Configuring Radius Profiles . . . . .	103
MAC Access Control Via RADIUS Authentication . . . . .	105
802.1x Authentication using RADIUS . . . . .	105
RADIUS Accounting . . . . .	106
SSID/VLAN/Security . . . . .	108
VLAN Overview . . . . .	108
Management VLAN . . . . .	110
Security Profile. . . . .	111
MAC Access. . . . .	118
Wireless . . . . .	119

---

---

<b>5</b>	<b>Monitoring</b>	<b>125</b>
	Version	126
	ICMP	127
	IP/ARP Table	128
	Learn Table	129
	IAPP	130
	RADIUS	131
	Interfaces	132
	Description of Interface Statistics	132
	Station Statistics	135
	Description of Station Statistics	135
	Mesh Statistics	137
<b>6</b>	<b>Commands</b>	<b>138</b>
	Introduction to File Transfer via TFTP or HTTP	139
	TFTP File Transfer Guidelines	139
	HTTP File Transfer Guidelines	139
	Image Error Checking During File Transfer	139
	Update AP	140
	Update AP via TFTP	140
	Update AP via HTTP	141
	Retrieve File	143
	Retrieve File via TFTP	143
	Retrieve File via HTTP	144
	Reboot	146
	Reset	147
	Help Link	148
<b>7</b>	<b>Troubleshooting</b>	<b>149</b>
	Troubleshooting Concepts	149
	Symptoms and Solutions	150
	Connectivity Issues	150
	Basic Software Setup and Configuration Problems	150
	Client Connection Problems	152
	VLAN Operation Issues	152
	Power-Over-Ethernet (PoE)	153
	Recovery Procedures	154
	Soft Reset to Factory Defaults	154
	Hard Reset to Factory Defaults	154
	Forced Reload	154

---

---

Setting IP Address using Serial Port .....	157
Related Applications .....	159
RADIUS Authentication Server .....	159
TFTP Server.....	159
<b>A Command Line Interface (CLI) .....</b>	<b>160</b>
General Notes .....	161
Prerequisite Skills and Knowledge.....	161
Notation Conventions.....	161
Important Terminology .....	161
Navigation and Special Keys .....	161
CLI Error Messages .....	162
Command Line Interface (CLI) Variations .....	163
Bootloader CLI.....	163
CLI Command Types .....	165
Operational CLI Commands.....	165
Parameter Control Commands .....	169
Using Tables and Strings .....	173
Working with Tables .....	173
Using Strings .....	173
Configuring the AP using CLI commands .....	175
Log into the AP using HyperTerminal.....	175
Log into the AP using Telnet .....	175
Set Basic Configuration Parameters using CLI Commands .....	176
Other Network Settings .....	181
CLI Monitoring Parameters .....	190
Parameter Tables .....	191
System Parameters .....	193
Network Parameters .....	195
Interface Parameters .....	199
Management Parameters.....	205
Filtering Parameters.....	208
Alarms Parameters .....	210
Bridge Parameters.....	212
RADIUS Parameters .....	214
Security Parameters.....	215
VLAN/SSID Parameters.....	217
Other Parameters.....	217
Wireless Multimedia Enhancements (WME)/Quality of Service (QoS) parameters.....	217
CLI Batch File .....	221
Auto Configuration and the CLI Batch File.....	221
CLI Batch File Format and Syntax .....	221

---

---

Reboot Behavior .....	222
<b>B ASCII Character Chart .....</b>	<b>223</b>
<b>C Specifications .....</b>	<b>224</b>
Software Features .....	224
Number of Stations per BSS .....	224
Management Functions .....	224
Advanced Bridging Functions .....	225
Medium Access Control (MAC) Functions .....	225
Security Functions .....	226
Network Functions .....	226
Hardware Specifications .....	227
Available Channels .....	228
802.11a/b/g Channels .....	228
WD SKU Channels by Country .....	229
<b>D Technical Services and Support .....</b>	<b>231</b>
Obtaining Technical Services and Support .....	231
Support Options .....	232
Proxim eService Web Site Support .....	232
Telephone Support .....	232
ServPak Support .....	232
<b>E Statement of Warranty .....</b>	<b>233</b>
Warranty Coverage .....	233
Repair or Replacement .....	233
Limitations of Warranty .....	233
Support Procedures .....	233
Other Information .....	234
Search Knowledgebase .....	234
Ask a Question or Open an Issue .....	234
Other Adapter Cards .....	234

## Introduction

This chapter contains information on the following:

- [Introduction to Wireless Networking](#)
- [Guidelines for Roaming](#)
- [Management and Monitoring Capabilities](#)

### Introduction to Wireless Networking

An Access Point extends the capability of an existing Ethernet network to devices on a wireless network. Wireless devices can connect to a single Access Point, or they can move between multiple Access Points located within the same vicinity. As wireless clients move from one coverage cell to another, they maintain network connectivity.

In a typical network environment (see [Figure 1-1](#)), the AP functions as a wireless network access point to data and voice networks. An AP network provides:

- Seamless client roaming for both data and voice (VoIP)
- Easy installation and operation
- Over-the-air encryption of data
- High speed network links

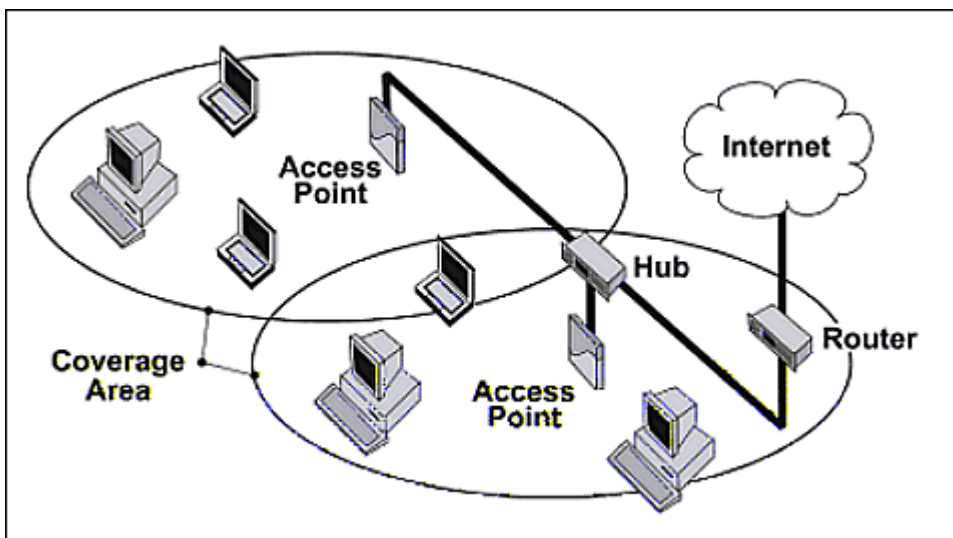


Figure 1-1 Typical Wireless Network Access Infrastructure

### Guidelines for Roaming

- Typical voice network cell coverages vary based on environment. Proxim recommends having a site survey done professionally to ensure optimal performance. For professional site surveyors, Ekahau™ Site Survey software is included in the Xtras folder of the Installation CD.
- An AP can only communicate with client devices that support its wireless standards.
- All Access Points must have the same Network Name to support client roaming.



- All workstations with an 802.11 client adapter installed must use either a Network Name of “any” or the same Network Name as the Access Points that they will roam between. If an AP has Closed System enabled, a client must have the same Network Name as the Access Point to communicate (see [Reboot the AP](#)).
- All Access Points and clients must have matching security settings to communicate.
- The Access Points’ cells should overlap to ensure that there are no gaps in coverage and to ensure that the roaming client will always have a connection available. To ensure optimal AP placement, Proxim recommends having a site survey done professionally to ensure optimal performance. For professional site surveyors, Ekahau™ Site Survey software is included in the Xtras folder of the Installation CD.
- All Access Points in the same vicinity should use a unique, independent channel. By default, the AP automatically scans for available channels during boot-up but you can also set the channel manually (see [Interfaces](#) for details).
- Access Points that use the same channel should be installed as far away from each other as possible to reduce potential interference.

## Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage an AP on the network:

- [HTTP/HTTPS Interface](#)
- [Command Line Interface](#)
- [SNMP Management](#)
- [SSH \(Secure Shell\) Management](#)

### HTTP/HTTPS Interface

The HTTP Interface (Web browser Interface) provides easy access to configuration settings and network statistics from any computer on the network. You can access the HTTP Interface over your LAN (switch, hub, etc.), over the Internet, or with a “crossover” Ethernet cable connected directly to your computer’s Ethernet Port.

HTTPS provides an HTTP connection over a Secure Socket Layer. HTTPS is one of three available secure management options on the AP; the other secure management options are SNMPv3 and SSH. Enabling HTTPS allows the user to access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate.

The AP comes pre-installed with all required SSL files: default certificate, private key and SSL Certificate Passphrase installed.

### Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage an AP.

Users enter Command Statements, composed of CLI Commands and their associated parameters. Statements may be issued from the keyboard for real time control, or from scripts that automate configuration.

For example, when downloading a file, administrators enter the **download** CLI Command along with IP Address, file name, and file type parameters.

You access the CLI over a HyperTerminal serial connection or via Telnet. During initial configuration, you can use the CLI over a serial port connection to configure an Access Point’s IP address. When accessing the CLI via Telnet, you can communicate with the Access Point from over your LAN (switch, hub, etc.), from over the Internet, or with a “crossover” Ethernet cable connected directly to your computer’s Ethernet Port. See [Command Line Interface \(CLI\)](#) for more information on the CLI and for a list of CLI commands and parameters.

## SNMP Management

In addition to the HTTP and the CLI interfaces, you can also manage and configure an AP using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program, like HP Openview or Castlerock's SNMPc. The AP supports several Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Ethernet-like MIB (RFC 1643)
- 802.11 MIB
- ORiNOCO Enterprise MIB

Proxim provides these MIB files on the CD-ROM included with each Access Point. You need to compile one or more of the above MIBs into your SNMP program's database before you can manage an Access Point using SNMP. See the documentation that came with your SNMP manager for instructions on how to compile MIBs.

The Enterprise MIB defines the read and read-write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. See the Enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word, Notepad, or WordPad.

## SNMPv3 Secure Management

SNMPv3 is based on the existing SNMP framework, but addresses security requirements for device and network management.

The security threats addressed by Secure Management are:

- *Modification of information:* An entity could alter an in-transit message generated by an authorized entity in such a way as to effect unauthorized management operations, including the setting of object values. The essence of this threat is that an unauthorized entity could change any management parameter, including those related to configuration, operations, and accounting.
- *Masquerade:* Management operations that are not authorized for some entity may be attempted by that entity by assuming the identity of an authorized entity.
- *Message stream modification:* SNMP is designed to operate over a connectionless transport protocol. There is a threat that SNMP messages could be reordered, delayed, or replayed (duplicated) to effect unauthorized management operations. For example, a message to reboot a device could be copied and replayed later.
- *Disclosure:* An entity could observe exchanges between a manager and an agent and thereby could learn of notifiable events and the values of managed objects. For example, the observation of a set command that changes passwords would enable an attacker to learn the new passwords.

To address the security threats listed above, SNMPv3 provides the following when secure management is enabled:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy (a.k.a Encryption):** Protects against disclosure of message payload.
- **Access Control:** Controls and authorizes access to managed objects.

The default SNMPv3 username is **administrator**, with SHA authentication, and DES privacy protocol.

## SSH (Secure Shell) Management

You may securely also manage the AP using SSH (Secure Shell). The AP supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data.

The SSH server (AP) has **host keys** - a pair of asymmetric keys - a **private key** that resides on the AP and a **public key** that is distributed to clients that need to connect to the AP. As the client has knowledge of the server host keys, the client can verify that it is communicating with the correct SSH server.

**NOTE:** *The remainder of this guide describes how to configure an AP using the HTTP Web interface or the CLI interface. For information on how to manage devices using SNMP or SSH, see the documentation that came with your SNMP or SSH program. Also, see the MIB files for information on the parameters available via SNMP and SSH.*

**IMPORTANT!**

The remainder of the User Guide discusses installing your AP and managing it using the Web and CLI interfaces only.

## Installation and Initialization

In this chapter:

- [AP-700 Hardware Description](#)
  - [Overview](#)
  - [LED Indicators](#)
  - [Power-over-Ethernet \(PoE\)](#)
  - [Antennas](#)
- [Prerequisites](#)
- [System Requirements](#)
- [Product Package](#)
- [Hardware Installation](#)
  - [Attach Cables](#)
  - [Install the Security Cover \(Optional\)](#)
  - [Mount the AP-700](#)
  - [Power On the Unit](#)
  - [Install External Antennas \(Professional Installation Required\)](#)
- [Initialization](#)
  - [Using ScanTool](#)
  - [Logging In](#)
  - [Using the Setup Wizard](#)
  - [Installing the Software](#)

## AP-700 Hardware Description

### Overview

The AP-700 is a tri-mode AP that supports 802.11b, 802.11g, or 802.11a clients. The unit contains one embedded 802.11a/b/g radio that supports the following operational modes:

- 802.11a only mode
- 802.11b only mode
- 802.11g only mode
- 802.11b/g mode
- 802.11g-wifi

**NOTE:** In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.

The AP-700 can be powered through either PoE (802.3af Power-over-Ethernet) or through an external DC power source using the power cord.

The AP-700 includes a power jack, a 10/100 base-T Ethernet port, and an RS-232 serial data communication port. See [Figure 2-1](#). The AP includes an optional security cover that can be installed to protect against access to the power and LAN cables and to the reset and reload buttons.

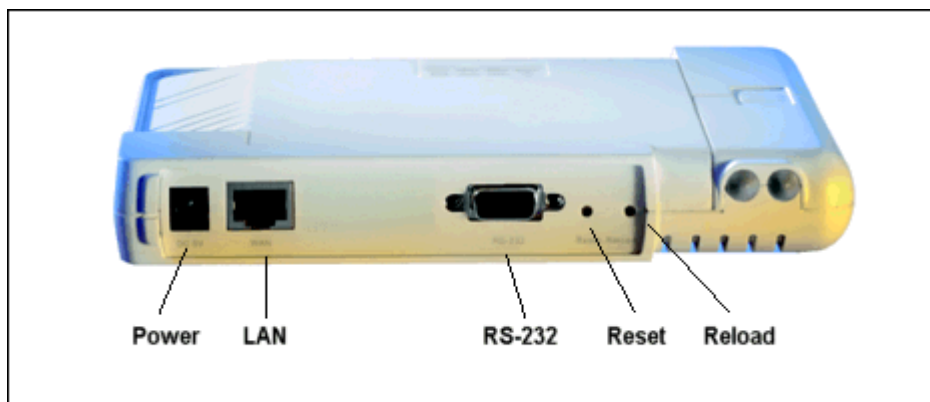


Figure 2-1 Rear Panel

The unit has been designed to rest horizontally on a flat surface, but can be wall- or ceiling- mounted with the long axis vertical. The unit includes screw slots in the bottom plastic for mounting to a flat wall or ceiling.

### LED Indicators

The top panel of the AP-700 has the following LED indicators. See [Power On the Unit](#) for a description of LED behavior.

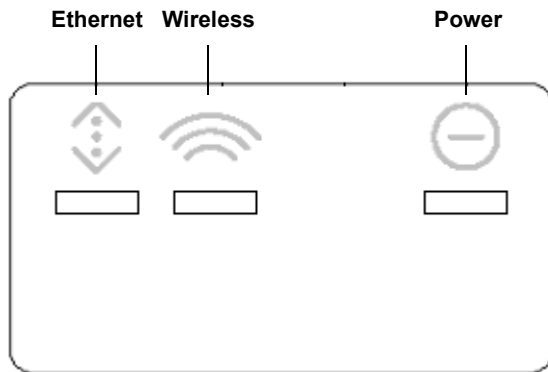


Figure 2-2 LED Indicators on the Top Panel

## Power-over-Ethernet (PoE)

The AP-700 is equipped with an 802.3af-compliant Power-over-Ethernet (PoE) module. PoE delivers both data and power to the access point over a single Ethernet cable. If you choose to use PoE, there is no difference in operation; the only difference is in the power source.

- The PoE integrated module receives ~48 VDC over a standard Category 5 Ethernet cable.
- To use PoE, you must have a PoE hub (also known as a power injector) connected to the network.
- The cable length between the PoE hub and the Access Point should not exceed 100 meters (approximately 325 feet). The PoE hub is not a repeater and does not amplify the Ethernet data signal.
- If connected to an PoE hub and an AC power supply simultaneously, the Access Point draws power from PoE.

Also see [Hardware Installation](#).

**NOTE:** The AP's 802.3af-compliant PoE module is backwards compatible with all ORiNOCO Active Ethernet (PoE) hubs that do not support the IEEE 802.3af standard.

## Antennas

The AP-700 employs two internal antennas for antenna diversity: one is vertically polarized, and the other is horizontally polarized to provide optimal spatial and polarization diversity. When the AP is hung on the wall of an office or building, the horizontally polarized antenna provides coverage for that particular floor level. The vertically polarized antenna provides spatial diversity for the horizontally polarized antenna in the event of an antenna null. In addition, the vertically polarized antenna provides some coverage above and below the current floor level. When the AP is mounted on the ceiling or sitting on a table, the effect is the same, but the roles of the two antennas switch.

The AP supports both receive and transmit diversity. When receiving, the AP chooses the antenna that receives the strongest signal. When transmitting, the AP chooses the antenna with the highest success rate, and broadcasts are transmitted on alternating antennas.

Antenna diversity is enabled by default (set to "auto"). When using the internal antennas, Proxim recommends leaving antenna diversity enabled. However, you may disable antenna diversity by manually selecting which antenna to use through the Command Line Interface. See [Configure Antenna Diversity](#) for information.

See [External Antennas](#) for information and [Install External Antennas \(Professional Installation Required\)](#) for installation instructions.

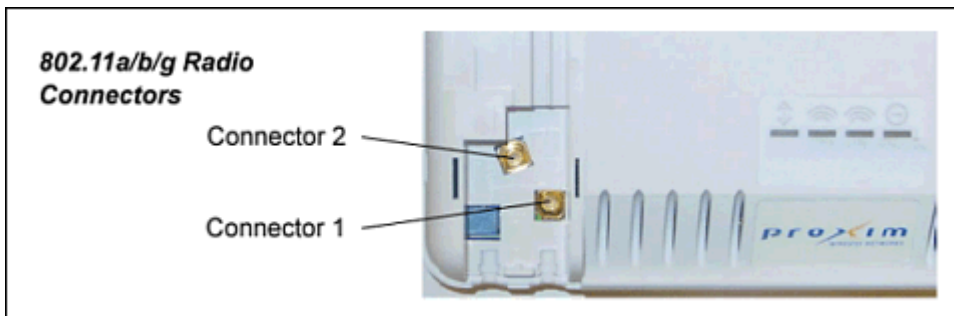
## External Antennas

The AP-700 also has two antenna connectors for use with external antennas.

**NOTE:**

**AP-700 units using external antennas must be installed by a suitably trained professional installation technician or by a qualified installation service.**

**See [Hardware Installation for AP cabling and mounting instructions](#), and [Install External Antennas \(Professional Installation Required\)](#) for external antenna installation instructions.**



**Figure 2-3 AP-700 Antenna Connectors**

When the AP is mounted on a wall, connector 1 corresponds to the horizontally polarized internal antenna, providing a coverage pattern parallel to the wall; connector 2 corresponds to the vertically polarized internal antenna, providing a coverage pattern parallel to the ceiling/floor. When the AP is mounted to a ceiling, connector 1 corresponds to the vertically polarized internal antenna, and connector 2 corresponds to the horizontally polarized internal antenna. Plugging an external antenna in to the antenna connector disables the corresponding internal antenna.

The AP continues to support antenna diversity with external antennas connected. With one external antenna connected to one of the two antenna connectors on a radio, one internal antenna and one external antenna are used for antenna diversity. With two external antennas connected, both external antennas are used for antenna diversity, and both internal antennas are disabled.

With external antennas connected, you may wish to manually select a particular antenna for use. To do so, disable antenna diversity by manually selecting which antenna to use through the Command Line Interface. See [Configure Antenna Diversity](#) for information.

**NOTE:** *Using two external antennas is not recommended.*

For a list of recommended antennas, see <http://www.proxim.com/products/wifi/accessories>.

For installation instructions, see [Install External Antennas \(Professional Installation Required\)](#).

## Prerequisites

Before installing your unit, you need to gather certain network information. The following table identifies the information you need.

Network Name (SSID of the wireless cards)	You must assign the Access Point a Network Name before wireless users can communicate with it. The clients also need the same Network Name. This is not the same as the System Name, which applies only to the Access Point. The network administrator typically provides the Network Name.
AP's IP Address	If you do not have a DHCP server on your network, then you need to assign the Access Point an IP address that is valid on your network.
HTTP Password	Each Access Point requires a read/write password to access the web interface. The default password is <b>public</b> .
CLI Password	Each Access Point requires a read/write password to access the CLI interface. The default password is <b>public</b> .
SNMP Read Password	Each Access Point requires a password to allow get requests from an SNMP manager. The default password is <b>public</b> .
SNMP Read-Write Password	Each Access Point requires a password to allow get and set requests from an SNMP manager. The default password is <b>public</b> .
SNMPv3 Authentication Password	If Secure Management is enabled, each Access Point requires a password for sending authenticated SNMPv3 messages. The default password is <b>public</b> . The default SNMPv3 username is administrator, with SHA authentication, and DES privacy protocol.
SNMPv3 Privacy Password	If Secure Management is enabled, each Access Point requires a password when sending encrypted SNMPv3 data. The default password is <b>public</b> .
Security Settings	You need to determine what security features you will enable on the Access Point.
Authentication Method	A primary authentication server may be configured; a backup authentication server is optional. The network administrator typically provides this information.
Authentication Server Shared Secret	This is a password shared between the Access Point and the RADIUS authentication server (so both passwords must be the same), and is typically provided by the network administrator.
Authentication Server Authentication Port	This is a port number (default is 1812) and is typically provided by the network administrator.
Client IP Address Pool Allocation Scheme	The Access Point can automatically provide IP addresses to clients as they sign on. The network administrator typically provides the IP Pool range.
DNS Server IP Address	The network administrator typically provides this IP Address.
Gateway IP Address and Subnet Mask	The gateway IP address and subnet mask of the network environment where the Access Point is deployed.

## System Requirements

To begin using an AP, you must have the following minimum requirements:







- A 10Base-T Ethernet or 100Base-TX Fast Ethernet switch or hub or cross-over Ethernet cable
- At least one of the following IEEE 802.11-compliant devices:
  - An 802.11a, 802.11b, or 802.11b/g client device
- A computer that is connected to the same IP network as the AP and has one of the following Web browsers installed:
  - Microsoft® Internet Explorer 6 with Service Pack 1 or later and patch Q323308
  - Netscape® 7.1 or later



## Product Package

Each AP-700 shipment includes the items in the following table. Verify that you have received all parts of the shipment.

**NOTE:** Unless noted in this table, cables are not supplied with the unit.

AP-700 Unit	
Power Cord	
Security Cover	
Ceiling/Wall Mount Plate	
Installation CD	
Quick Installation Guide	

## Hardware Installation

**NOTE:**

**AP-700 units using external antennas must be installed by a suitably trained professional installation technician or by a qualified installation service.**

**NOTE:**

**Before installing and using this product, see the Safety and Regulatory Compliance Guide.**

**NOTE:**

**Avant d'installer et d'utiliser ce produit, consultez le manuel Safety and Regulatory Compliance Guide.**

**NOTA:**

**Prima dell'installazione e dell'utilizzo del prodotto, consultare il documento Safety and Regulatory Compliance Guide (Guida per la sicurezza e la conformità alle normative).**

**ANMERKUNG:**

**Lesen Sie vor der Installation und Verwendung dieses Produkts die wichtigen Informationen im Handbuch Safety and Regulatory Compliance Guide.**

**NOTA:**

**Antes de instalar y utilizar este producto, consulte el manual Safety and Regulatory Compliance Guide (Manual de seguridad y cumplimiento de la normativa).**

**注記 :**

**この製品をインストールして使用する前に、『Safety and Regulatory Compliance Guide』。**

Perform the following procedures to install the AP hardware:

- [Attach Cables](#)
- [Install the Security Cover \(Optional\)](#)
- [Mount the AP-700](#)
- [Power On the Unit](#)

### Attach Cables

#### Cabling without Power Over Ethernet (PoE)

1. Plug the barrel of the power cable from the power supply into the power jack (the left-most port in the back of the unit, see figure).
2. Connect one end of an Ethernet cable (not supplied) to the unit's LAN port (see figure). The other end of the cable should not be connected to another device until after installation is complete:
  - Use a straight-through Ethernet cable if you intend to connect the unit to a switch, hub, or patch panel.

- Use a cross-over Ethernet cable or adapter if you intend to connect the unit to a single computer.

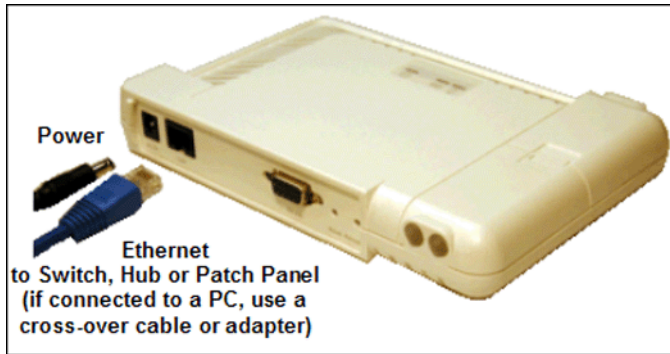


Figure 2-4 Cabling without PoE

3. Optionally, connect an RS-232 cable (not shown) to the RS-232 console port (the right port, labeled “RS-232”).

**NOTE:** You cannot install the security cover to the AP-700 if an RS-232 cable is connected.

4. Continue with [Install the Security Cover \(Optional\)](#).

### Cabling with Power Over Ethernet (PoE)

1. To use PoE, you must use a PoE adapter such as the ORINOCO 1-Port Active Ethernet DC Injector (ordered separately). Connect one end of an Ethernet cable (not supplied) to the unit’s LAN port. Connect the other end to the **Data and Power Out** port of the DC Injector (see figure).
2. Connect one end of a second Ethernet cable (not supplied) to the **Data In** port of the DC Injector (see figure). The other end of the cable should not be connected to another device until after installation is complete:
  - Use a straight-through Ethernet cable if you intend to connect the unit to a switch, hub, or patch panel.
  - Use a cross-over Ethernet cable or adapter if you intend to connect the unit to a single computer.

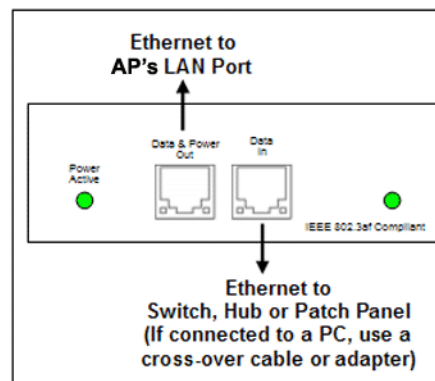
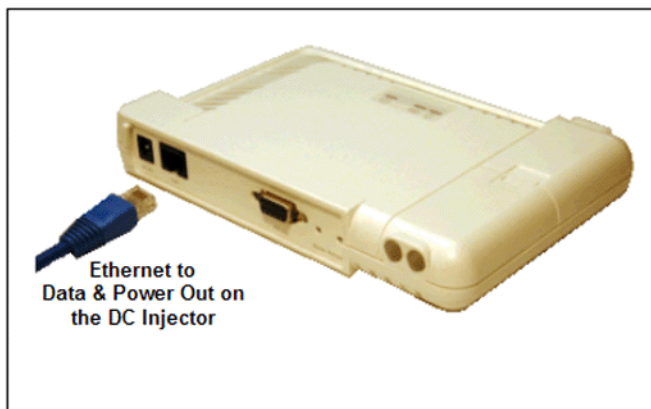


Figure 2-5 Cabling with PoE

3. Optionally, connect an RS-232 cable (not shown) to the RS-232 console port (the right port, labeled “RS-232”).

**NOTE:** You cannot install the security cover to the AP-700 if an RS-232 cable is connected.

4. Continue with [Install the Security Cover \(Optional\)](#) below.

## Install the Security Cover (Optional)

You can optionally install a security cover to deter unauthorized access to the unit. The security cover is a plastic enclosure that prevents access to the cabling and the Reset and Reload buttons.

1. Open the split end of the security cover just enough to slide the power cable (if not using PoE) and the Ethernet cable through the opening until they fit inside the straight clamping portion of the cover (see figure). Exercise care as you slide the cable(s) so you do not accidentally break the cover.
2. Slide the hinging end of the security cover into the hole on the rear panel of the unit to the left of the connectors. Once in place, pivot the right side of the cover to bring it close to the rear panel of the unit.
3. Use the two attached screws to fasten the security cover onto the rear panel of the unit.

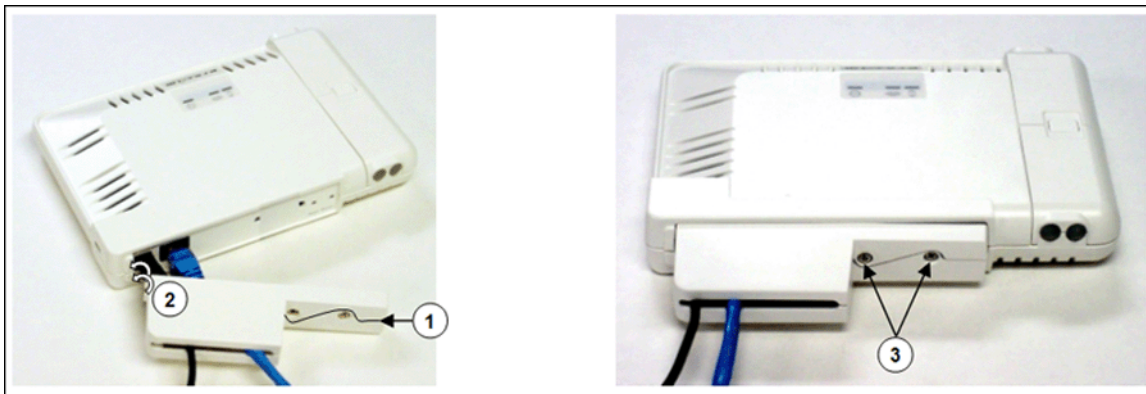


Figure 2-6 Installing the Security Cover

## Mount the AP-700

Proxim recommends that you have a site survey professionally conducted to determine the best location for the AP. For professional site surveyors, Ekahau Site Survey software is included in the Xtras folder on the Installation CD-ROM.

Note that the AP-700 has been certified under UL Standard 2043 and can be installed in the plenum. In an office building, plenum is the space between the structural ceiling and the tile ceiling that is provided to help air circulate. Many companies also use the plenum to house communication equipment and cables. These products and cables must comply with certain safety requirements, such as Underwriter Labs (UL) Standard 2043: "Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces".

**NOTE:** When installed in a plenum, the AP must use PoE.

Once you have chosen a final location for your unit, the following are the mounting options available:

- [Wall Mounting](#)
- [Ceiling Mounting](#)

### Wall Mounting

Follow these steps to mount the unit on a wall:

1. If the unit's power supply is plugged in, unplug it.
2. Put the mounting plate up to the wall so that the embossed letter "L" is on top (see figure). If the plate is correctly oriented, the circular tab that is vertically aligned with the square hole should be on top.
3. Fasten the mounting plate with two screws through the circular holes of the plate. Depending on the type of wall, you may need to use the two fasteners provided.
4. Holding the unit so that the connectors on the rear are facing left, align the two holes on the bottom of the unit with the two tabs on the mounting plate. Press the unit down so it is flush with the plate.

- Carefully slide the unit to the right until the tabs snap securely onto the narrow holes of the unit. If the unit is mounted correctly, no portion of the mounting plate should protrude from any of the sides of the unit.

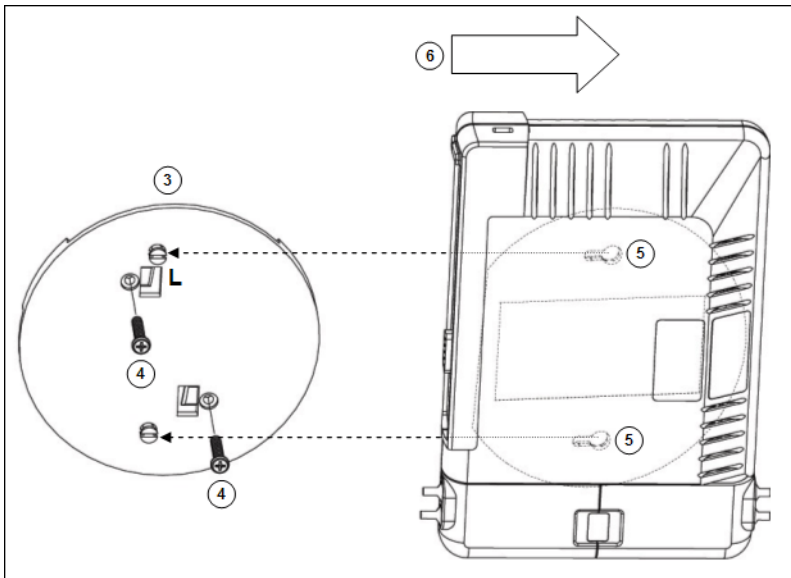


Figure 2-7 Mounting the AP to a Wall

### Ceiling Mounting

Follow these steps to mount the unit to a ceiling:

- If the unit's power supply is plugged in, unplug it.
- Snap the rectangular tabs on the back of the mounting plate onto a ceiling T-bar. You may need to slightly rotate the plate until it securely snaps onto the T-bar.
- Fasten the mounting plate to the ceiling tile with two screws through the circular holes of the plate.
- Position so that the embossed letter "L" on the mounting plate is facing up (see previous figure). Holding the unit so that the connectors on the rear are facing to left, align the two holes on the bottom of the unit with the two tabs on the mounting plate. Press the unit up so it is flush with the plate.
- Carefully slide the unit to the right until the tabs snap securely onto the narrow holes of the unit. If the unit is mounted correctly, no portion of the mounting plate should protrude from any of the sides of the unit.

### Power On the Unit

The AP can be powered by a power supply (just plug the power cord of the power supply into an AC power outlet), or by Power-over-Ethernet (connect a PoE DC injector to the Ethernet cable).

When the unit is powered on, it performs startup diagnostics. When startup is completed, the LEDs show the operational state of the unit.

The LED indicators exhibit the following behavior:

Indication	Ethernet	Wireless Interface (802.11a/b/g radio)	Power
Solid Green	Ethernet interface is connected at 100 Mbps with no traffic.	Wireless interface is preparing for use.	AP image running.
Blinking Green	Ethernet interface is connected at 100 Mbps with traffic.	Wireless interface is transmitting or receiving wireless packets.	n/a
Solid Amber	Ethernet interface is connected at 10 Mbps with no traffic.	n/a	The Bootloader is loading the application software.
Blinking Amber	The Ethernet interface is connected at 10 Mbps with traffic.	n/a	The AP is reloading.
Solid Red	n/a	n/a	Power On Self Test (POST) running.
Blinking Red	n/a	n/a	Rebooting.

### Install External Antennas (Professional Installation Required)

Optionally, you can connect two external antennas to your AP.

All products using external antennas must be professionally installed, and the transmit power of the system must be adjusted by the professional installers to ensure that the system EIRP is in compliance with the limit specified by the regulatory authority of the country of application.

See the following sections for more information:

- [Connecting Antenna\(s\)](#)
- [Adjusting Tx Output Power](#)
- [Antenna Types and Maximum Gain](#)

#### Connecting Antenna(s)

Follow the mounting instructions included with your external antenna, and then connect the antenna cable to the AP, as follows:

1. Press down near the center of the compartment covering and slide open the external antenna access compartments. The compartment closer to the LED panel contains the connectors.

**NOTE:** AP-700 models 8675-US2 and 8675-AU do not provide external antenna connectors for 5 GHz (802.11a) operation.

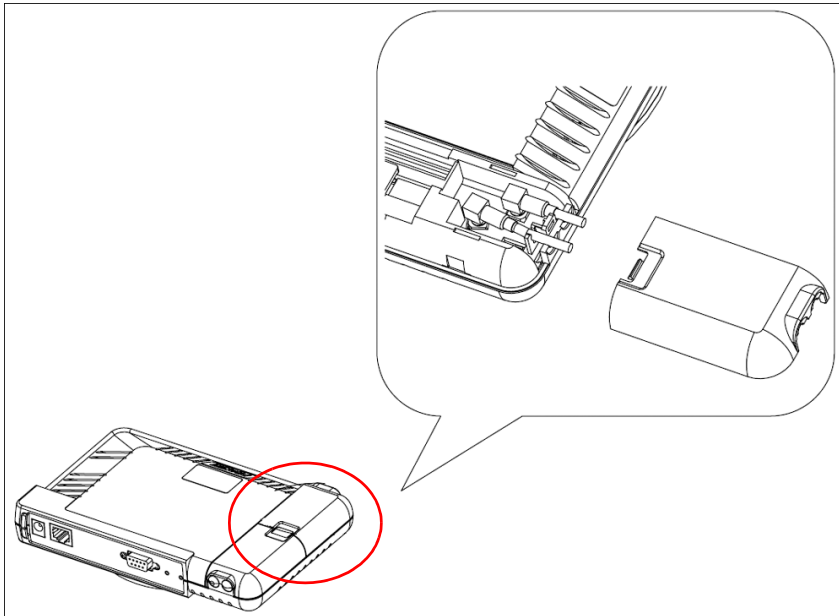


Figure 2-8 Opening the Antenna Compartment

2. There are two antenna connectors in the AP-700, labeled 1 and 2. Connect the antenna cable to connector 1 (the connector closer to the LED panel in the compartment).

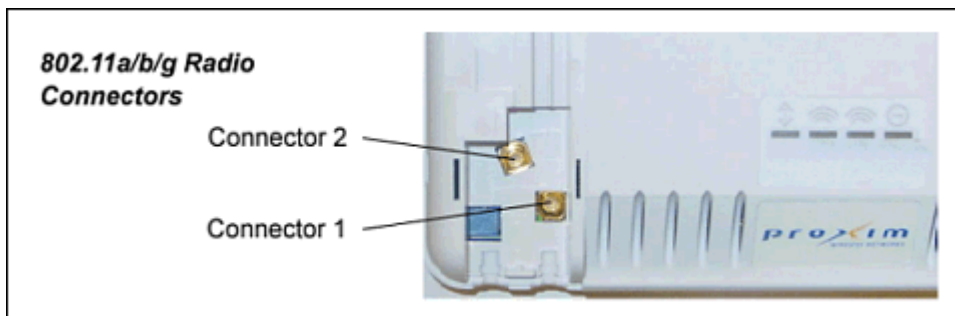


Figure 2-9 Antenna Connectors

3. If installing a second external antenna (*not recommended*), connect the antenna cable to connector 2.
4. Close the external antenna access compartment.
5. If desired, manually select which antenna(s) to use through the Command Line Interface. See [Configure Antenna Diversity](#).

### Adjusting Tx Output Power

**NOTE:** When the system is set to transmit at the maximum power, professional installers must ensure that the maximum EIRP limit is not exceeded. To achieve this, they may have to add attenuation between the device and the antenna when a high gain antenna is used.

Use the following formula in combination with the table of EIRP limits in US, Canada, and EU countries to calculate system transmit power (based on EIRP limits) of these countries:

$$\text{Tx Power (dBm)} = \text{EIRP Limit (dBm)} + \text{FL (dB)} - \text{G (dB)}$$

where:

Tx Power = Output power measured at the antenna input

EIRP Limit = EIRP limits specified below

FL = Feeder loss including loss of connectors

G = Antenna Gain

Band	EIRP Limit (dBm)	
	USA and Canada	EU
2.4 - 2.4835 GHz (Point-to-Multipoint)	36	20
2.4 - 2.4835 GHz (Point-to-Point)	When G < 6: 36 When G >= 6, use the following equation: $36 - \frac{G - 6}{3}$	20
5.15 - 5.25 GHz	23	23
5.25 - 5.35 GHz	30	23
5.47 - 5.725 GHz	30	30
5.725 - 5.850 GHz (Point-to-Multipoint)	36	14
5.725 - 5.850 GHz (Point-to-Point)	No limit	14

**Antenna Types and Maximum Gain**

For devices using external antennas, professional installers should select only the antenna types listed in the following table, with gain not exceeding the listed maximum gain for each type.

Frequency Band	Antenna Type	Maximum Gain
2.4 GHz	Omni	10
	Panel	14
	Yagi	14
	Parabolic	24
5 GHz	Omni	13
	Panel	28.2
	Sector	17
	Parabolic	33.4



## Initialization

The following sections detail how to initialize the AP using ScanTool, log in to the HTTP interface, perform an initial configuration of the AP using the Setup Wizard, and download the required AP software.

- [Using ScanTool](#)
- [Logging In](#)
- [Using the Setup Wizard](#)
- [Installing the Software](#)

## Using ScanTool

ScanTool is a software utility that is included on the installation CD-ROM. It is an initial configuration tool that allows you to find the IP address of an Access Point by referencing the MAC address in a Scan List, or to assign an IP address if one has not been assigned.

The tool automatically detects the Access Points installed on your network, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use set initial device parameters that will allow the AP to retrieve a new software to an AP that does not have a valid software image installed (see [Client Connection Problems](#)).

To access the HTTP interface and configure the AP, the AP must be assigned an IP address that is valid on its Ethernet network. By default, the AP is configured to obtain an IP address automatically from a network Dynamic Host Configuration Protocol (DHCP) server during boot-up. If your network contains a DHCP server, you can run ScanTool to find out what IP address the AP has been assigned. If your network does not contain a DHCP server, the Access Point's IP address defaults to 169.254.128.132. In this case, you can use ScanTool to assign the AP a static IP address that is valid on your network.

## ScanTool Instructions

Follow these steps to install ScanTool and initialize the AP:

1. Power up, reboot, or reset the AP.
2. Double-click the **ScanTool** icon on the Windows desktop to launch the program (if the program is not already running). If the icon is not on your desktop, click **Start > All Programs > ORiNOCO > AP-700 > ScanTool**.

**NOTE:** *If your computer has more than one network adapter installed, you will be prompted to select the adapter that you want ScanTool to use before the **Scan List** appears. You can use either an Ethernet or wireless adaptor. If prompted, select an adapter and click **OK**. You can change your adapter setting at any time by clicking the **Select Adapter** button on the **Scan List** screen.*

ScanTool scans the subnet and displays all detected Access Points. The ScanTool's **Scan List** screen appears, as shown in the following example.

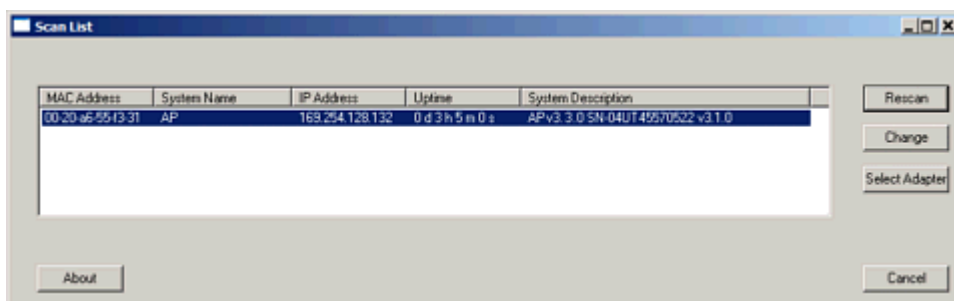


Figure 2-10 Scan List

3. Locate the MAC address of the AP you want to initialize within the Scan List.

**NOTE:** If your Access Point does not appear in the Scan List, click the **Rescan** button to update the display. If the unit still does not appear in the list, see [Troubleshooting](#) for suggestions. Note that after rebooting an Access Point, it may take up to five minutes for the unit to appear in the Scan List.

4. Do one of the following:
  - If the AP has been assigned an IP address by a DHCP server on the network:
    - a. Highlight the entry for the AP you want to configure.
    - b. Click the **Change** button. The **Change** screen appears.
    - c. Click on the **Web Configuration** button at the bottom of the change screen.
    - d. Proceed to the [Logging In](#) section for information on how to access the HTTP interface using this IP address.
  - If the AP has not been assigned an IP address (in other words, the unit is using its default IP address, 169.254.128.132), follow these steps to assign it a static IP address that is valid on your network:
    - a. Highlight the entry for the AP you want to configure.
    - b. Click the **Change** button. The **Change** screen appears.

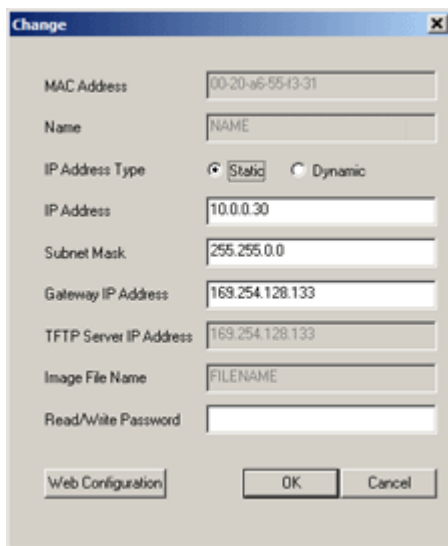


Figure 2-11 Scan Tool Change Screen

- c. Set **IP Address Type** to **Static**.
- d. Enter a static **IP Address** for the AP in the field provided. You must assign the unit a unique address that is valid on your IP subnet. Contact your network administrator if you need assistance selecting an IP address for the unit.
- e. Enter your network's **Subnet Mask**.
- f. Enter your network's **Gateway IP Address**.
- g. Enter the SNMP Read/Write password in the **Read/Write Password** field (for new units, the default SNMP Read/Write password is **public**).

**NOTE:** The **TFTP Server IP Address** and **Image File Name** fields are only available if ScanTool detects that the AP does not have a valid software image installed. See [Client Connection Problems](#).

- h. Click **OK** to save your changes.
- i. The Access Point will need to reboot to apply any changes you made. When the reboot message appears, click **OK** to reboot the device and return to the **Scan List** screen.
- j. After allowing sufficient time for the device to reboot, click **Rescan** to verify that your changes have been applied.

- k. Click the **Change** button to return to the Change screen.
- l. Click the **Web Configuration** button at the bottom of the Change screen.
- m. Proceed to the [Logging In](#) section for information on how to access the HTTP interface using this IP address.

## Logging In

Once the AP has a valid IP Address and an Ethernet connection, you may use your web browser to monitor and configure the AP. (To configure and monitor using the command line interface, see [Command Line Interface \(CLI\)](#).)

1. Open a Web browser on a network computer.
2. If necessary, disable the browser's Internet proxy settings. For Internet Explorer users, follow these steps:
  - Select **Tools > Internet Options**.
  - Click the **Connections** tab.
  - Click **LAN Settings**.
  - If necessary, remove the check mark from the **Use a proxy server** box.
  - Click **OK** twice to save your changes and return to Internet Explorer.
3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter** or **Go**.

This is either the dynamic IP address assigned by a network DHCP server or the static IP address you manually configured. See [Using ScanTool](#) for information on how to determine the unit's IP address and manually configure a new IP address, if necessary.

The **Enter Network Password** screen appears.

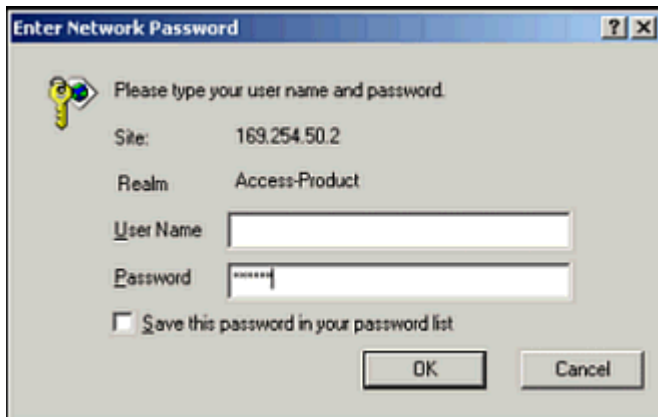


Figure 2-12 Enter Network Password

4. Enter the HTTP password in the **Password** field. Leave the **User Name** field blank. For new units, the default HTTP password is **public**.

If you are logging on for the first time the **Setup Wizard** will launch automatically.

**NOTE:** *Setup Wizard will not relaunch on subsequent logins. To force the Setup Wizard to launch upon login, click **Management > Services** and choose **Enable** from the Setup Wizard drop down menu.*

5. To configure the AP using the Setup Wizard, see [Using the Setup Wizard](#); to configure the AP without using the Setup Wizard, click **Exit**. Upon clicking **Exit**, the **System Status** screen will appear.



Figure 2-13 System Status Screen

The buttons on the left of the screen provide access to the monitoring and configuration options for the AP. See [Advanced Configuration](#) to begin configuring the AP manually.

You can also exit the Web interface or reboot the AP using these buttons.

The Command Line Interface (CLI) also provides a method for monitoring and configuring the AP using Telnet or a serial connection. For more information about monitoring and configuring the AP with the CLI, see [Command Line Interface \(CLI\)](#).

## Using the Setup Wizard

The first time you connect to an AP's HTTP interface, the Setup Wizard launches automatically. The Setup Wizard provides step-by-step instructions for how to configure the Access Point's basic operating parameters, such as Network Name, IP parameters, system parameters, and management passwords.

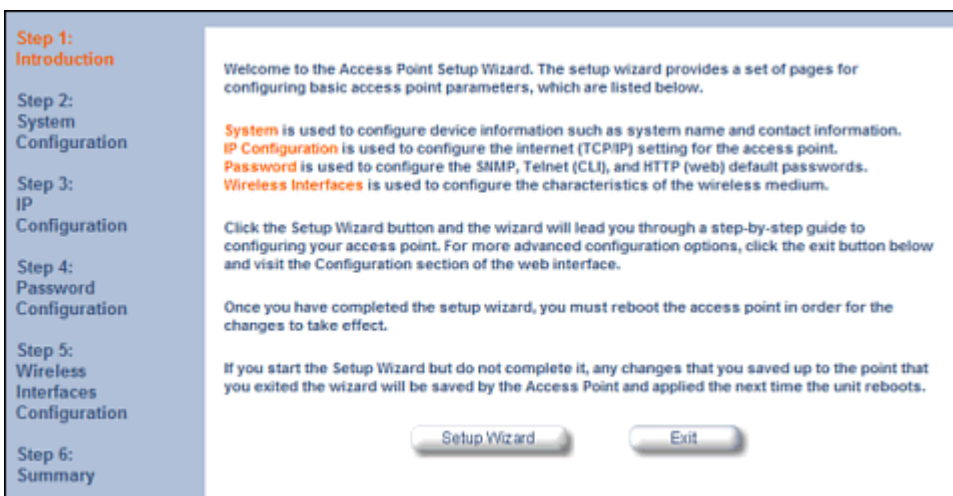


Figure 2-14 Setup Wizard

### Setup Wizard Instructions

1. Click **Setup Wizard** to begin. The Setup Wizard supports the following navigation options:

- **Save & Next Button:** Each Setup Wizard screen has a **Save & Next** button. Click this button to submit any changes you made to the unit's parameters and continue to the next page. The instructions below describe how to navigate the Setup Wizard using the **Save & Next** buttons.
- **Navigation Panel:** The Setup Wizard provides a navigation panel on the left-hand side of the screen. Click the link that corresponds to the parameters you want to configure to be taken to that particular configuration screen. Note that clicking a link in the navigation panel will not submit any changes you made to the unit's configuration on the current page.
- **Exit:** To exit from the Setup Wizard at any time, click **Step 1: Introduction** on the navigation panel, and then click the **Exit** button.

**CAUTION:** If you exit from the Setup Wizard, any changes you submitted (by clicking the **Save & Next** button) up to that point will be saved to the unit but will not take effect until it is rebooted.

2. Configure the **System Configuration** settings and click **Save & Next**. See [System](#) for more information.

**NOTE:** On APs with model numbers ending in **-WD**, you must select the operating country on this page or on the **Configure > System** tab. Setting the country makes the AP automatically compliant with the rules of the regulatory domain in which it is used by configuring the allowed frequency bands, channels, Dynamic Frequency Selection status, Transmit Power Control status, and power levels. If the country is not selected, an informational message will appear on the **Status** page, and you will be unable to configure interface parameters.

3. Configure the Access Point's **IP Configuration**, including basic IP address settings, if necessary, and click **Save & Next**. See [Basic IP Parameters](#) for more information.
4. On the **Password Configuration** screen, assign the AP new passwords to prevent unauthorized access and click **Save & Next**. Each management interface has its own password:
  - SNMP Read Password
  - SNMP Read-Write Password
  - CLI Password
  - HTTP (Web) Password

By default, each of these passwords is set to "public". See [Passwords](#) for more information.

5. Configure the basic **Wireless Interface Configuration** settings:

- Select the Operational Mode as follows and click **Save & Next**:

The Wireless (802.11a/b/g) interface can be configured to operate in the following modes:

- **802.11a only mode:** The radio uses the 802.11a standard only.
- **802.11b mode only:** The radio uses the 802.11b standard only.
- **802.11g mode only:** The radio is optimized to communicate with 802.11g devices. This setting will provide the best results if this radio interface will only communicate with 802.11g devices.
- **802.11b/g mode:** This is the default mode. Use this mode if you want to support a mix of 802.11b and 802.11g devices.
- **802.11g-wifi mode:** The 802.11g-wifi mode has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

**NOTE:** In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.

In general, you should use either 802.11g only mode (if you want to support 802.11g devices only) or 802.11b/g mode to support a mix of 802.11b and 802.11g devices.

- Configure the following available options and click **Save & Next**:

- **Primary Network Name (SSID):** Enter a Network Name (between 1 and 32 characters long) for the wireless network. You must configure each wireless client to use this name as well. Note that the unit supports up to 16 SSIDs/VLANs. Please see the [Advanced Configuration](#) chapter for information on the detailed rules on configuring multiple SSIDs, VLANs, and security profiles.

**NOTE:** Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.

- **Auto Channel Select:** By default, the AP scans the area for other Access Points and selects the best available communication channel, either a free channel (if available) or the channel with the least amount of interference. Remove the check mark to disable this option. See [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) for information and [Available Channels](#) for a list of available channels.
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) for information and [Available Channels](#) for a list of available channels.
- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP. The values depend on the Operational mode. Auto Fallback is the default setting; it allows the AP unit to select the best transmit rate based on the cell size.
  - For 802.11a only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s.

**NOTE:** In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.

- For 802.11b only -- Auto Fallback, 1, 2, 5.5, 11 Mbits/sec.
- For 802.11g only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/sec
- For 802.11b/g -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec
- For 802.11g-wifi -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec

**NOTE:** 802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

Additional advanced settings are available on the [Interfaces](#) tab.

Also see [Security Profile](#) for a description of security features, [Management VLAN](#) for a description of VLAN capabilities, and [Configuring Security Profiles](#) for detailed security configuration procedures.

6. Review the configuration **Summary**. If you want to make any additional changes, use the navigation panel on the left-hand side of the screen to return to an earlier screen. After making a change, click **Save & Next** to save the change and proceed to the next screen.
7. When finished, click **Reboot** on the Summary screen to restart the AP and apply your changes.

## Installing the Software

Proxim periodically releases updated software for the AP on its Web site, <http://support.proxim.com>. Check the Web site for the latest updates after you have installed and initialized the unit.

### Download the Software

1. In your web browser, go to <http://support.proxim.com>.
2. If prompted, create an account to gain access.

**NOTE:** The Knowledgebase is available to all website visitors. First-time users will be asked to create an account to gain access.

3. Click **Search Knowledgebase**.



4. In the **Search Knowledgebase** field, enter **1686**.
5. Click **Search**.
6. Click on the appropriate link to access the download page.
7. Use the instructions in the following sections to install the new software.

### Install Software with HTTP Interface

Use the **Update AP via HTTP** tab to update the AP with the latest software image.

1. Click **Commands > Update AP > via HTTP**.

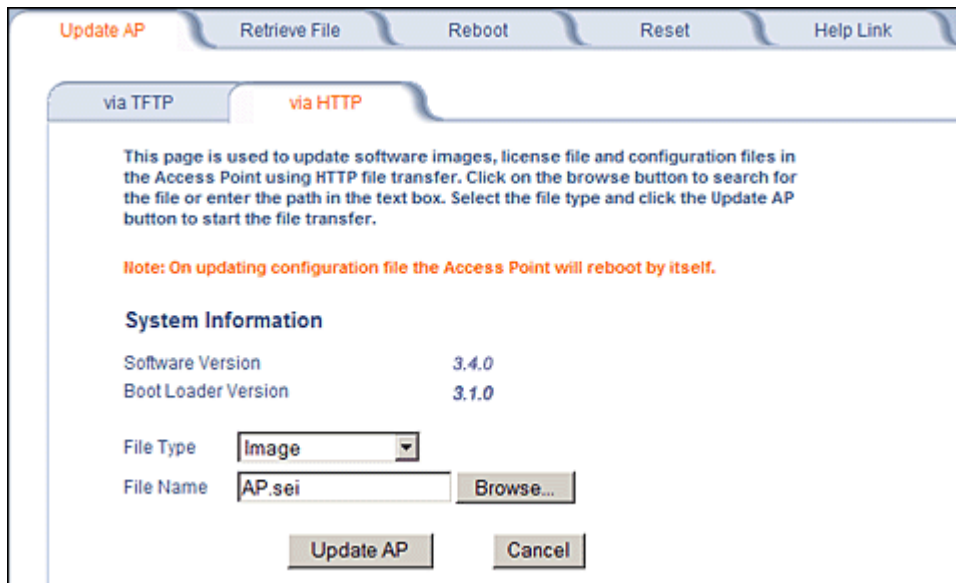


Figure 2-15 Update AP via HTTP Command Screen

2. From the File Type drop-down menu, select **Image**.
3. Use the **Browse** button to locate or manually type in the name of the file (including the file extension) you downloaded from the Proxim Knowledgebase. If typing the file name, you must include the full path and the file extension in the file name text box.
4. To initiate the HTTP Update operation, click the **Update AP** button.  
A warning message advises you that a reboot of the device will be required for changes to take effect.

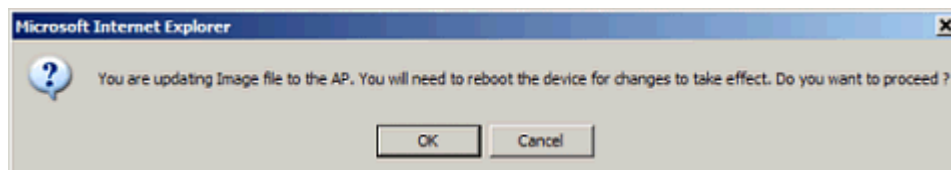


Figure 2-16 Warning Message

5. Click **OK** to continue with the operation or **Cancel** to abort the operation.
6. If the operation is unsuccessful, you will receive an error message. If this occurs, see the [Troubleshooting](#) chapter or attempt installing the software with a TFTP server, as described in the next section.  
If the operation is successful, you will receive a confirmation message.
7. Reboot the AP as follows:
  - Click **Commands > Reboot**.

## Initialization

- Enter **0** in the **Time to Reboot** field.
- Click **OK**.

**Install Software with TFTP Server**

A Trivial File Transfer Protocol (TFTP) server allows you to transfer files across a network. You can upload files from the AP for backup or copying, and you can download the files for configuration and AP Image upgrades. The Solarwinds TFTP server software is located on the AP Installation CD-ROM. You can also download the latest TFTP software from Solarwind's Web site at <http://www.solarwinds.net>. The instructions that follow assume that you are using the Solarwinds TFTP server software; other TFTP servers may require different configurations.

**NOTE:** *If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface. See [Update AP via HTTP](#).*

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP address, the proper AP Image file name, and that the TFTP server is operational.
- Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's **Security** tab), with no automatic shutdown or time-out (on the **Auto Close** tab).

The following types of files can be downloaded to the AP from a TFTP server:

- Config (configuration file)
- Image (AP software image or kernel)
- UpgradeBspBI (BSP/Bootloader firmware file)
- SSL Certificate
- SSL Private Key
- SSH Public Key
- SSH Private Key
- CLI Batch File

**Install Updates from your TFTP Server using the Web Interface**

1. Download the latest software from <http://support.proxim.com>. See [Download the Software](#) for instructions.
2. Copy the latest software updates to your TFTP server.
3. In the Web Interface, click the **Commands** button and select the **Download** tab.
4. Enter the **IP address** of your TFTP server in the field provided.
5. Enter the **File Name** (including the file extension). If the file is located in the default TFTP directory, you need enter only the file name. Otherwise, enter the full directory path and file name.
6. Select the **File Type** from the drop-down menu (use *Img* for software updates).
7. Select **Download & Reboot** from the **File Operation** drop-down menu.
8. Click **OK**. The Access Point will reboot automatically when the download is complete.

**Install Updates from your TFTP Server using the CLI**

1. Download the latest software to <http://support.proxim.com>. See [Download the Software](#) for instructions.
2. Copy the latest software updates to your TFTP server.
3. Open the CLI interface via Telnet or a serial connection.
4. Enter the CLI password when prompted.
5. Enter the command: `download <tftpaddr> <filename> img`

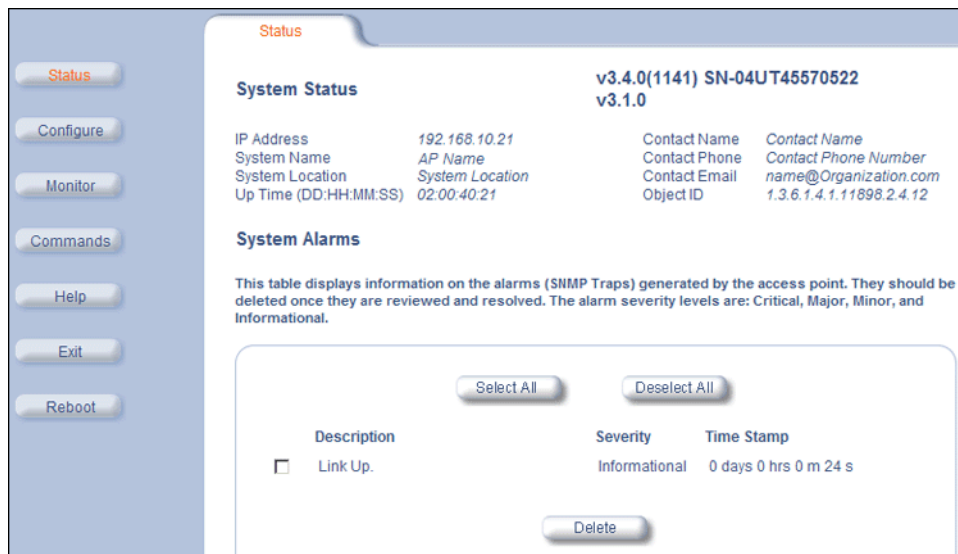
The download will begin, and the image will be downloaded to the Access Point.



6. When the download is complete, type `reboot 0` and press **Enter**.

## System Status

The first screen displayed after [Logging In](#) is the **System Status** screen. You can always return to this screen by clicking the **Status** button.



**Figure 3-1 System Status Screen**

The **System Status** screen provides the following information:

- **System Status:** This area provides system-level information, including the unit's IP address and contact information. See [System](#) for information on these settings.
- **System Alarms:** System traps (if any) appear in this area. Each trap identifies a specific severity level: critical, major, minor, and informational. See [Alarms](#) for a list of possible alarms.

**NOTE:** On APs with model numbers ending in **-WD**, an operating Country must be selected (during the Setup Wizard or on the **Configure > System** tab). If a country has not been selected, an informational message will appear in the **System Alarms** list, and you will be unable to configure interface parameters.

From this screen, you can also access the AP's monitoring and configuration options by clicking on the buttons on the left of the screen.

## Advanced Configuration

This chapter contains information on configuring settings in the following categories:

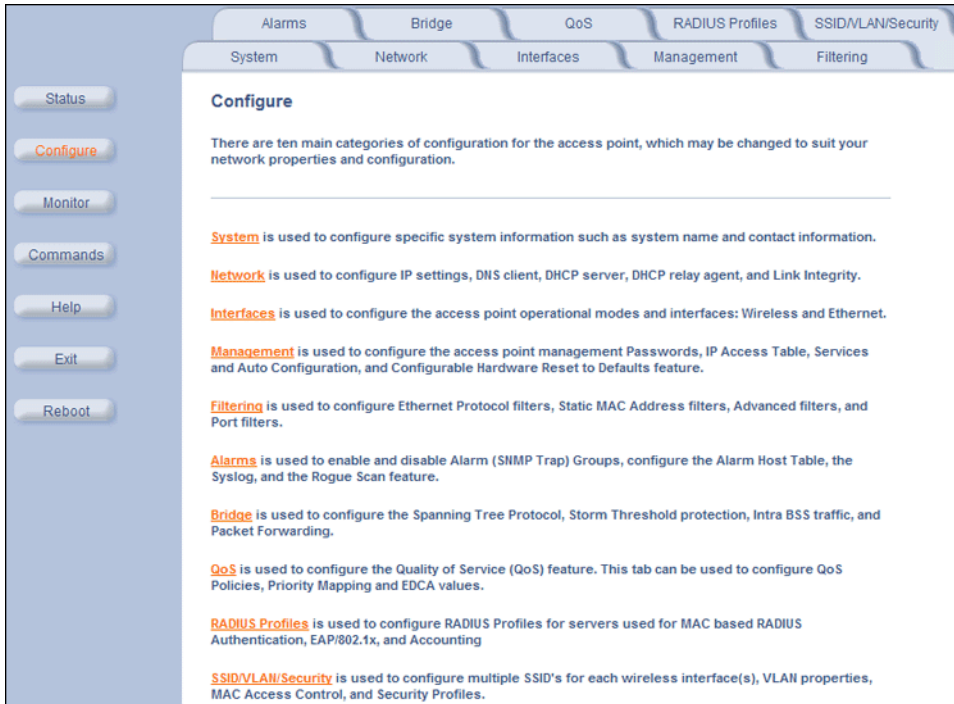
- **System:** Configure specific system information such as system name and contact information.
- **Network:** Configure IP, DNS client, DHCP server, DHCP Relay Agent, DHCP Relay Servers, Link Integrity, and SNMP settings.
- **Interfaces:** Configure the Access Point's interfaces: Wireless and Ethernet. Configure the [Channel Blacklist Table](#) and a [Wireless Distribution System \(WDS\)](#).
- **Management:** Configure the Access Point's management Passwords, IP Access Table, and Services such as configuring secure or restricted access to the AP via SNMPv3, HTTPS, or CLI. Configure Secure Management, SSL, Secure Shell (SSH), and RADIUS Based Access Management. [Set up Automatic Configuration for Static IP](#).
- **Filtering:** Configure Ethernet Protocol filters, Static MAC Address filters, Advanced filters, and Port filters.
- **Alarms:** Configure the Alarm (SNMP Trap) Groups, the Alarm Host Table, and the Syslog features.
- **Bridge:** Configure the Spanning Tree Protocol, Storm Threshold protection, Intra BSS traffic, and Packet Forwarding.
- **QoS:** Configure Wireless Multimedia Enhancements/Quality of Service parameters and QoS policies.
- **Radius Profiles:** Configure RADIUS features such as RADIUS Access Control and Accounting.
- **SSID/VLAN/Security:** Configure SSIDs, VLANs, and security profiles. Configure security features such as MAC Access Control, WPA, 802.11i (WPA2), WEP Encryption, and 802.1x.

To configure the AP using the HTTP/HTTPS interface, you must first log in to a web browser. See [Logging In](#) for instructions.

You may also configure the AP using the command line interface. See [Command Line Interface \(CLI\)](#) for more information.

To configure the AP via HTTP/HTTPS:

1. Click the **Configure** button located on the left-hand side of the screen.



**Figure 4-1 Configure Main Screen**

2. Click the tab that corresponds to the parameter you want to configure. For example, click **Network** to configure the Access Point's TCP/IP settings.

Each **Configure** tab is described in the remainder of this chapter.

## System

You can configure and view the following parameters within the **System Configuration** screen:

- **Name:** The name assigned to the AP. See the [Dynamic DNS Support](#) and [Access Point System Naming Convention](#) sections for rules on naming the AP.
- **Country:** The country in which the AP will be used. Note that some countries have two selectable options (one for indoor use and one for outdoor use). Setting the country makes the AP automatically compliant with the rules of the regulatory domain in which it is used by configuring the allowed frequency bands, channels, Dynamic Frequency Selection status, Transmit Power Control status, and power levels. See [Interfaces](#) for more information about these settings.

**NOTE:** You must reboot the AP in order for country selection to take effect.

**NOTE:** Country selection is available only on APs with model numbers ending in **-WD**. If country selection is available, however, it must be set before any interface parameters can be configured.

- **Location:** The location where the AP is installed.
- **GPS Longitude:** The longitude at which the AP is installed. Enter the value in the format required by your network management system. If using the ProximVision™ Network Management System (recommended), enter the value in decimals (e.g., 78.4523).
- **GPS Latitude:** The latitude at which the AP is installed. Enter the value in the format required by your network management system. If using the ProximVision™ Network Management System (recommended), enter the value in decimals (e.g., 78.4523).
- **GPS Altitude:** The altitude at which the AP is installed. Enter the value in the format required by your network management system. If using the ProximVision™ Network Management System (recommended), enter the value in decimals (e.g., 78.4523).
- **Contact Name:** The name of the person responsible for the AP.
- **Contact Email:** The email address of the person responsible for the AP.
- **Contact Phone:** The telephone number of the person responsible for the AP.
- **Object ID:** This is a read-only field that displays the Access Point's system object identification number; this information is useful if you are managing the AP using SNMP.
- **Ethernet MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's Ethernet interface. The MAC address is assigned at the factory.
- **Descriptor:** This is a read-only field that reports the Access Point's name, serial number, current image software version, and current bootloader software version.
- **Up Time:** This is a read-only field that displays how long the Access Point has been running since its last reboot.

Alarms Bridge QoS RADIUS Profiles SSID/LAN/Security

System Network Interfaces Management Filtering

This tab allows for configuration of system unique parameters and contact information.

Note: Changes to these parameters require access point reboot in order to take effect.

Note: Name is also used as Dynamic DNS hostname

Note: Name can only contain alphanumeric characters. Hyphen is the only special character allowed. No spaces are allowed. First character can't be a numeric.

Name

Country

Location

GPS Longitude

GPS Latitude

GPS Altitude

Contact Name

Contact Email

Contact Phone

Object ID 1.3.6.1.4.1.11898.2.4.12

Ethernet MAC Address 00:20:A6:55:F3:31

Descriptor v3.4.0(1142) SN-04UT45570522 v3.1.0

Up Time (DD:HH:MM:SS) 04:01:33:14

OK Cancel

Figure 4-2 System Tab

## Dynamic DNS Support

DNS is a distributed database mapping the user readable names and IP addresses (and more) of every registered system on the Internet. Dynamic DNS is a lightweight mechanism which allows for modification of the DNS data of host systems whose IP addresses change dynamically. Dynamic DNS is usually used in conjunction with DHCP for mapping meaningful names to host systems whose IP addresses change dynamically.

Access Points provide DDNS support by adding the host name (option 12) in DHCP Client messages, which is used by the DHCP server to dynamically update the DNS server.

## Access Point System Naming Convention

The Access Point's system name is used as its host name. In order to prevent Access Points with default configurations from registering similar host names in DNS, the default system name of the Access Point is uniquely generated. Access Points generate unique system names by appending the last 3 bytes of the Access Point's MAC address to the default system name.

The system name must be compliant with the encoding rules for host name as per DNS RFC 1123. According to the encoding rules, the AP name:

- Can contain alphanumeric or hyphen characters only.
- Can contain up to 31 characters.
- Cannot start or end with a hyphen.
- Cannot start with a digit.

## Network

The Network tab contains the following sub-tabs:

- [IP Configuration](#)
- [DHCP Server](#)
- [DHCP Relay Agent](#)
- [Link Integrity](#)
- [SNTP \(Simple Network Time Protocol\)](#)

### IP Configuration

This tab is used to configure the internet (TCP/IP) settings for the access point.

These settings can be either entered manually (static IP address, subnet mask, and gateway IP address) or obtained automatically (dynamic). The DNS Client functionality can also be configured, so that host names used for configuring the access point can be resolved to their IP addresses.

The screenshot shows the 'IP Configuration' sub-tab within the 'Network' configuration page. The interface includes a navigation bar with tabs for 'Alarms', 'Bridge', 'QoS', 'RADIUS Profiles', and 'SSID/LAN/Security'. Below this, the 'Network' tab is active, with sub-tabs for 'System', 'Network', 'Interfaces', 'Management', and 'Filtering'. The 'IP Configuration' sub-tab is selected, showing a descriptive text block, a note, and several input fields for IP address assignment, DNS client settings, and TTL. The fields are as follows:

Parameter	Value
IP Address Assignment Type	Static
IP Address	192.168.10.21
Subnet Mask	255.255.0.0
Gateway IP Address	169.254.128.133
Enable DNS Client	<input type="checkbox"/>
DNS Primary Server IP Address	0.0.0.0
DNS Secondary Server IP Address	0.0.0.0
DNS Client Default Domain Name	
Default TTL (Time To Live)	64

Buttons for 'OK' and 'Cancel' are located at the bottom of the form.

**Figure 4-3 IP Configuration**

You can configure and view the following parameters within the **IP Configuration** sub-tab:

**NOTE:** You must reboot the AP in order for any changes to the Basic IP or DNS Client parameters to take effect.

### Basic IP Parameters

- **IP Address Assignment Type:** Set this parameter to **Dynamic** to configure the Access Point as a Dynamic Host Configuration Protocol (DHCP) client; the Access Point will obtain IP settings from a network DHCP server automatically during boot-up. If you do not have a DHCP server or if you want to manually configure the Access Point's IP settings, set this parameter to **Static**.
- **IP Address:** The Access Point's IP address. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current IP address. The Access Point will default to 169.254.128.132 if it cannot obtain an address from a DHCP server.
- **Subnet Mask:** The Access Point's subnet mask. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current subnet mask. The subnet mask will default to 255.255.0.0 if the unit cannot obtain one from a DHCP server.
- **Gateway IP Address:** The IP address of the Access Point's gateway. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the IP address of the unit's gateway. The gateway IP address will default to 169.254.128.133 if the unit cannot obtain an address from a DHCP server.

### DNS Client

If you prefer to use host names to identify network servers rather than IP addresses, you can configure the AP to act as a Domain Name Service (DNS) client. When this feature is enabled, the Access Point contacts the network's DNS server to translate a host name to the appropriate network IP address. You can use this DNS Client functionality to identify RADIUS servers by host name.

- **Enable DNS Client:** Place a check mark in the box provided to enable DNS client functionality. Note that this option must be enabled before you can configure the other DNS Client parameters.
- **DNS Primary Server IP Address:** The IP address of the network's primary DNS server.
- **DNS Secondary Server IP Address:** The IP address of a second DNS server on the network. The Access Point will attempt to contact the secondary server if the primary server is unavailable.
- **DNS Client Default Domain Name:** The default domain name for the Access Point's network (for example, "proxim.com"). Contact your network administrator if you need assistance setting this parameter.

### Advanced

- **Default TTL (Time to Live):** Time to Live (TTL) is a field in an IP packet that specifies the number of hops, or routers in different locations, that the request can travel before returning a failed attempt message. The Access Point uses the default TTL for generated packets for which the transport layer protocol does not specify a TTL value. This parameter supports a range from 0 to 255. By default, TTL is 64.

### DHCP Server

If your network does not have a DHCP Server, you can configure the AP as a DHCP server to assign dynamic IP addresses to Ethernet nodes and wireless clients.

**CAUTION:** *Make sure there are no other DHCP servers on the network and do not enable the DHCP server without checking with your network administrator first, as it could disrupt normal network operation. Also, the AP must be configured with a static IP address before enabling this feature.*

When the DHCP Server functionality is enabled, you can create one or more IP address pools from which to assign addresses to network devices.





Figure 4-4 DHCP Server Configuration Screen

You can configure and view the following parameters within the **DHCP Server Configuration** screen:

**NOTE:** You must reboot the AP before changes to any of these DHCP server parameters take effect.

- **Enable DHCP Server:** Place a check mark in the box provided to enable DHCP Server functionality.
  - NOTE:** You cannot enable the DHCP Server functionality unless there is at least one IP Pool Table Entry configured.
- **Subnet Mask:** This field is read-only and reports the Access Point's current subnet mask. DHCP clients that receive dynamic addresses from the AP will be assigned this same subnet mask.
- **Gateway IP Address:** The AP will assign the specified address to its DHCP clients.
- **Primary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Secondary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Number of IP Pool Table Entries:** This is a read-only field that reports the number of entries in the IP Pool Table.
- **IP Pool Table Entry:** This entry specifies a range of IP addresses that the AP can assign to its wireless clients. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following fields:
  - **Start IP Address:** The first IP address in the pool. IP addresses must be within the same subnet as the AP.
  - **End IP Address:** The last IP address in the pool. IP addresses must be within the same subnet as the AP.
  - **Default Lease Time (optional):** The default time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 3600 and 86400 seconds. The default is 86400 seconds. If this field is left blank, the default (86400) is used.
  - **Maximum Lease Time (optional):** The maximum time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 3600 and 86400 seconds. The default is 86400 seconds. If this field is left blank, the default (86400) is used.

**NOTE:** The Default Lease Time cannot be larger than the Maximum Lease Time. If you set the Maximum Lease Time, you should also set the Default Lease Time to ensure that the Default Lease Time is less than the Maximum.

- **Comment (optional)**
- **Status:** IP Pools are enabled upon entry in the table. You can also disable or delete entries by changing this field's value.

**NOTE:** You must reboot the AP before changes to any of these DHCP server parameters take effect.

## DHCP Relay Agent

When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server.

Click the **Configure > Network > DHCP R A** to configure DHCP relay agent servers and enable the DHCP relay agent.

**NOTE:** At least one DHCP server must be enabled before DHCP Relay Agent can be enabled.

**NOTE:** If the DHCP relay agent is unable to reach the external DHCP Server specified in the DHCP Server IP Address Table, the requesting client will receive an IP address from the IP Pool table of the AP's internal DHCP Server, even if the internal DHCP Server is disabled.

**NOTE:** If a client requests an available IP address from the IP Pool table of the AP's internal DHCP Server, the client will receive this address, even if the DHCP server on the AP is disabled. To ensure that clients receive IP addresses only from the DHCP Relay Agent, disable all entries in the IP Pool table of the AP's internal DHCP server.

The DHCP Relay functionality of the AP supports Option 82 and sends the system name of the AP (as a NAS identifier) as a sub-option of Option 82.

The AP makes a DHCP Request for lease renewal five minutes ahead of the expiration of the Rebinding time as specified in the DHCP Offer from the DHCP server obtained during the last renewal.

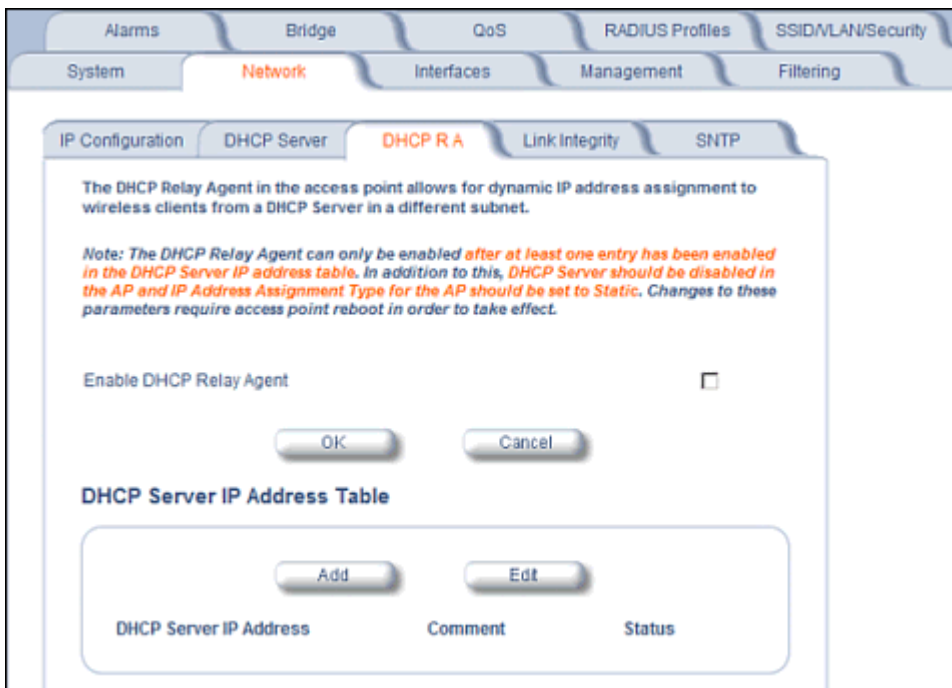


Figure 4-5 DHCP Relay Agent

### DHCP Server IP Address Table

The AP supports the configuration of a maximum of 10 server settings in the DHCP Relay Agents server table. At least one server must be configured to enable DHCP Relay.

To add entries to the table of DHCP Relay Agents, click **Add** in the DHCP Server IP Address Table; to edit existing entries, click **Edit**. The following window is displayed.



Figure 4-6 DHCP Server IP Address Table - Edit Entries

To add an entry, enter the IP Address of the DHCP Server and a comment (optional), and click OK.

To edit an entry, make changes to the appropriate entry. Enable or disable the entry by choosing Enable or Disable from the Status drop-down menu, and click **OK**.

### Link Integrity

The Link Integrity feature checks the link between the AP and any nodes on the backbone. These nodes are listed by IP address in the Link Integrity IP Address Table. The AP periodically pings the nodes listed within the table. If the AP loses network connectivity (that is, the ping attempts fail), the AP disables its wireless interface(s). Note that this feature does not affect WDS links (if WDS links are configured and enabled).

You can configure and view the following parameters within the **Link Integrity Configuration** screen:

- **Enable Link Integrity:** Place a check mark in the box provided to enable Link Integrity.
- **Poll Interval (milliseconds):** The interval between link integrity checks. Range is 500-15000 ms in increments of 500 ms; default is 500 ms.
- **Poll Retransmissions:** The number of times a poll should be retransmitted before the link is considered down. Range is 0 to 255; default is 5.
- **Target IP Address Entry:** This entry specifies the IP address of a host on the network that the AP will periodically poll to confirm connectivity. The table can hold up to five entries. By default, all five entries are set to 0.0.0.0. Click **Edit** to update one or more entries. Each entry contains the following field:
  - **Target IP Address**
  - **Comment (optional)**
  - **Status:** Set this field to **Enable** to specify that the Access Point should poll this device. You can also disable an entry by changing this field's value to **Disable**.



Figure 4-7 Link Integrity Configuration Screen

### SNTP (Simple Network Time Protocol)

SNTP allows a network entity to communicate with time servers in the network/internet to retrieve and synchronize time of day information. When this feature is enabled, the AP will attempt to retrieve the time of day information from the configured time servers (primary or secondary), and, if successful, will update the relevant time objects in the AP. Requests are sent every 10 seconds. If the AP fails to retrieve the information after three attempts, the AP will use the system uptime and update the relevant time objects. If this feature is disabled, the user can manually configure the date and time parameters.

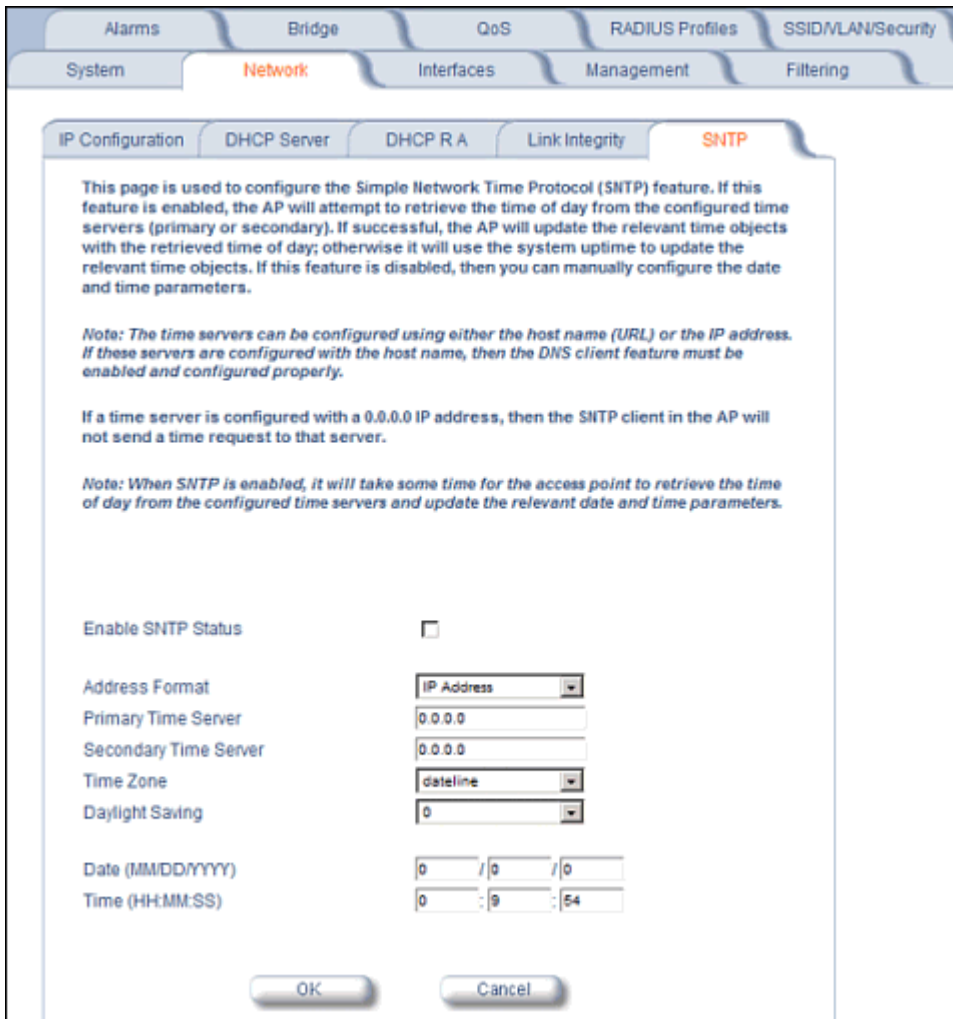


Figure 4-8 SNTP Configuration Screen

You can configure and view the following parameters within the SNTP screen:

- **SNTP Status:** Select Enable or Disable from the drop-down menu. The selected status will determine which of the parameters on the SNTP screen are configurable.
- NOTE:** When SNTP is enabled, it will take some time for the AP to retrieve the time of day from the configured time servers and update the relevant date and time parameters.*
- **Addressing Format:** If SNTP is enabled, choose whether you will use the host name or the IP address to configure the primary/secondary SNTP servers. If these servers are configured with the host name, the DNS client feature must be enabled and configured properly.
  - **Primary Server Name or IP Address:** If SNTP is enabled, enter the host name or IP address of the primary SNTP server.
  - **Secondary Server Name or IP Address:** If SNTP is enabled, enter the host name or IP address of the secondary SNTP server.
  - **Time Zone:** Select the appropriate time zone from the drop down menu.
  - **Daylight Savings Time:** Select the number of hours to adjust for daylight savings time.
  - **Time and Date Information:** When SNTP is disabled, the following time-relevant objects are manually configurable. When SNTP is enabled, these objects are grayed out:

- Year: Enter the current year.
- Month: Enter the month in digits (1-12).
- Day: Enter the day in digits (1-31).
- Hour: Enter the hour in digits (0-23).
- Minutes: Enter the minutes in digits (0-59).
- Seconds: Enter the seconds in digits (0-59).

## Interfaces

From the **Interfaces** tab, you configure the Access Point's operational mode settings, power control settings, wireless interface settings and Ethernet settings. You may also configure a Wireless Distribution System for AP-to-AP communications. The **Interfaces** tab contains the following sub-tabs:

- [Operational Mode](#)
- [Wireless A \(802.11a/b/g Radio\)](#)
- [Ethernet](#)

**NOTE:** On APs with model numbers ending in **-WD**, the operating country must be selected on the [System](#) tab before any of these sub-tabs are available.

## Operational Mode

From this tab, you can configure and view the operational mode for the Wireless interface.

The screenshot shows the 'Operational Mode' configuration screen for the Wireless interface. The page has a navigation bar at the top with tabs for 'Alarms', 'Bridge', 'QoS', 'RADIUS Profiles', 'SSID/WLAN/Security', 'System', 'Network', 'Interfaces' (selected), 'Management', and 'Filtering'. Below this, there are sub-tabs for 'Operational Mode' (selected), 'Wireless', and 'Ethernet'. The main content area contains the following text and configuration options:

The operational mode of the wireless interface determines the mode of communication between wireless clients and the access point

*Note: Changes to these parameters require access point reboot in order to take effect.*

**Note: Select the desired operational mode prior to configuring other wireless interface parameters.**

*Note: 802.11d needs to be enabled before enabling IBSS Power Control.*

**Wireless - A**

Operational Mode	<input type="text" value="802.11a only"/>
Enable Super Mode	<input type="checkbox"/>
Enable Turbo Mode	<input type="checkbox"/>
Enable 802.11d	<input type="checkbox"/>
ISOMEC 3166-1 CountryCode	<input type="text" value="UNITED STATES"/>
Enable TX Power Control	<input type="checkbox"/>
Wireless - A: Transmit Power Level	<input type="text" value="100%"/>

At the bottom of the screen, there are two buttons: 'OK' and 'Cancel'.

**Figure 4-9 Operational Mode Screen**

The Wireless (802.11a/b/g) interface can be configured to operate in the following modes:

- **802.11a only mode:** The radio uses the 802.11a standard only.
- **802.11b mode only:** The radio uses the 802.11b standard only.
- **802.11g mode only:** The radio is optimized to communicate with 802.11g devices. This setting will provide the best results if this radio interface will only communicate with 802.11g devices.

- **802.11b/g mode:** This is the default mode. Use this mode if you want to support a mix of 802.11b and 802.11g devices.
- **802.11g-wifi mode:** The 802.11g-wifi mode has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

**NOTE:** *In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.*

### Enable H Band Support

In compliance with FCC regulations, Dynamic Frequency Selection is required in the middle frequency band (M band: 5.25 GHz - 5.25 GHz) and high frequency band (H band: 5.470 GHz - 5.725 GHz). DFS is enabled automatically when you use one or both of these frequency bands.

If the AP's Wireless Card A is variant **2, 3, or 6**, the M band channels are enabled by default, and DFS is performed automatically and cannot be disabled. To add H band channels to the list of available channels, select **Enable H Band Support** on the Op Mode page. When the H band is enabled, DFS is enabled automatically, and is performed on both M and H band channels.

If the AP's Wireless Card A is variant **8, 10, or 11**, both M and H band channels are enabled automatically. DFS is performed on both M and H band channels and cannot be disabled.

To identify your AP's software variant, click **Monitor > Version** to view the [Version](#) tab.

For a full discussion of Dynamic Frequency Selection, see [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#).

### Super Mode and Turbo Mode

Super mode improves throughput between the access point and wireless clients that support this capability. For wireless clients that support this capability the AP will negotiate and treat them accordingly, for other clients that do not support super mode, the AP will treat them as normal wireless clients.

Super mode can be configured only when the wireless operational mode is one of the following:

- 802.11a only mode
- 802.11g only mode
- 802.11b/g mode

**NOTE:** *Super mode is not available in 802.11b and 802.11g-wifi operational modes. Turbo mode is available only in 802.11a mode in the FCC regulatory domain. Turbo Mode is not available in frequency bands in which DFS is required.*

Turbo mode is supported in 802.11a mode in the FCC regulatory domain when DFS is not required. Turbo mode supports turbo speeds at twice the standard data rates, and also dynamically switches between Turbo mode speeds and normal speeds depending on the wireless client. All connected clients must be using Turbo mode in order for the AP to operate at Turbo mode speed. If turbo mode is enabled, then this is displayed in the web UI and the transmit speeds and channels pull-down menus are updated with the valid values.

When Turbo mode is enabled, only a subset of the wireless channels in the 5.0 GHz spectrum can be used. If any wireless clients do not support turbo mode, the AP will fall back to normal mode.

Turbo mode can be configured only when Super mode has already been enabled.

Super mode is supported in the 2.4 GHz and 5 GHz frequency bands in all regulatory domains. Turbo mode is available in the 5 GHz frequency band in the FCC regulatory domain when DFS is not required.

### IEEE 802.11d Support for Additional Regulatory Domains

The IEEE 802.11d specification allows conforming equipment to operate in more than one regulatory domain over time. IEEE 802.11d support allows the AP to broadcast its radio's regulatory domain information in its beacon and probe responses to clients. This allows clients to passively learn what country they are in and only transmit in the allowable



spectrum. When a client enters a regulatory domain, it passively scans to learn at least one valid channel, i.e., a channel upon which it detects IEEE Standard 802.11 frames.

The beacon frame contains information on the country code, the maximum allowable transmit power, and the channels to be used for the regulatory domain.

The same information is transmitted in probe response frames in response to a client's probe requests. Once the client has acquired the information required to meet the transmit requirements of the regulatory domain, it configures itself for operation in the regulatory domain.

On some AP models, the regulatory domain and associated parameters are automatically configured when a country is selected on the System tab. On APs in which country selection is not available on the system tab, the regulatory domain is pre-programmed into the AP prior to shipment. Depending on the regulatory domain, a default country code is chosen that is transmitted in the beacon and probe response frames.

### **Configuring 802.11d Support**

Perform the following procedure to enable 802.11d support and select the country code:

1. Click **Configure > Interfaces > Operational Mode**.
2. Select **Enable 802.11d**.
3. Select the Country Code from the ISO/IEC 3166-1 CountryCode drop-down menu.  
***NOTE:** On APs with model numbers ending in **-WD**, this object is not configurable.*
4. Click **OK**.
5. Configure Transmit Power Control and Transmit Power Level if required.

### **Transmit Power Control/Transmit Power Level**

Transmit Power Control uses standard 802.11d frames to control transmit power within an infrastructure BSS (Basic Service Set, or combination of AP and associated clients that can communicate to each other and/or to the backhaul connection via the AP). This method of power control is considered to be an interim way of controlling the transmit power of 802.11d enabled clients in lieu of implementation of 802.11h.

When an AP comes online, it automatically uses the maximum TX power allowed in the regulatory domain. The Transmit Power Control feature lets the user manually lower the transmit power level by setting a "back-off" value between 0 and 35 dBm.

When Transmit Power Control is enabled, the transmit power level of the card in the AP is set to the maximum transmit power level minus the back-off value. This power level is advertised in Beacon and Probe Response frames as the 802.11d maximum transmit power level.

When an 802.11d-enabled client learns the regulatory domain related information from Beacon and Probe Response frames, it learns the power level advertised in Beacon and Probe response frames as the maximum transmit power of the regulatory domain and configures itself to operate with that power level.

As a result, the transmit power level of the BSS is configured to the power level set in the AP (assuming that the BSS has only 802.11d enabled clients and an 802.11d enabled AP).

***NOTE:** In FCC DFS-enabled bands, power control is adjusted from beacon information only.*

In addition, ATPC (Automatic Transmit Power Control) is a feature to automatically adapt transmit power when the quality of the link is more than sufficient to maintain a good communication with reduced transmit power. This feature is required for FCC DFS. It works by monitoring the quality of the link and reducing the output power of the radio by up to 6 dB when good link quality can still be achieved. When link quality reduces, the output power is automatically increased up to the original power level to maintain a good link. For a full discussion of DFS, see [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#).

***Configuring TX Power Control***

1. Click **Configure > Interfaces > Operational Mode**.
2. Select **Enable Transmit Power Control**.
3. Enter the desired backoff from the maximum Transmit Power level (between 0 and 35 dBm) in the **Wireless-A: Transmit Power Level Back-Off** field.
4. Click **OK**.

### Wireless A (802.11a/b/g Radio)

Alarms Bridge QoS RADIUS Profiles SSID/LAN/Security  
System Network **Interfaces** Management Filtering

Op Mode **Wireless** Ethernet

Wireless interface properties determine the characteristics of the wireless medium as well as how wireless clients will communicate with the access point.

Verify configuration of the desired operational mode prior to configuring the wireless interface properties below.

Note: This page allows configuration of a single SSID (Wireless Network Name); in order to configure more than one SSID, please visit the [SSID/LAN/Security](#) page.

Note: Changes to these parameters except Wireless Service Status require access point reboot in order to take effect.

Physical Interface Type 802.11g (OFDM/DSSS 2.4 GHz)  
 MAC Address 00:20:A6:49:9A:C6  
 Regulatory Domain USA (FCC)  
 Network Name (SSID) My Wireless Network A  
 Enable Auto Channel Select   
 Frequency Channel 2 - 2.417 GHz  
 Transmit Rate Auto Fallback  
 DTIM Period (1-255) 1  
 RTS/CTS Medium Reservation (2347=off) 2347  
 Enable Closed System   
 Wireless Service Status Resume  
 Load Balancing Max Clients 63

OK Cancel

#### Channel Blacklist Table

This table is used to configure blacklist channels. A channel can be blacklisted automatically if radar is detected on the operating channel (this is applicable only to specific regulatory domains). If radar is detected on a channel, that channel will be blacklisted for 30 minutes. A channel can also be blacklisted by the administrator in case that channel is not to be used when ACS is enabled.

Edit

Channel	Radar Detected	Elapsed Time (Minutes)	Blacklist Status
1	FALSE	0	Disable
2	FALSE	0	Disable
3	FALSE	0	Disable
4	FALSE	0	Disable
5	FALSE	0	Disable
6	FALSE	0	Disable
7	FALSE	0	Disable
8	FALSE	0	Disable
9	FALSE	0	Disable
10	FALSE	0	Disable
11	FALSE	0	Disable
12	FALSE	0	Disable
13	FALSE	0	Disable

#### Wireless Distribution System (WDS)

WDS can be used to establish point-to-point (i.e. wireless backhaul) connections with other access points. This table is used to configure WDS partner access points.

Edit

Port Index	Partner MAC Address	Status
1	00:00:00:00:00:00	Disable
2	00:00:00:00:00:00	Disable
3	00:00:00:00:00:00	Disable
4	00:00:00:00:00:00	Disable
5	00:00:00:00:00:00	Disable
6	00:00:00:00:00:00	Disable

Figure 4-10 Wireless Interface

You can view and configure the following parameters for the Wireless interface:

**NOTE:** You must reboot the Access Point before any changes to these parameters take effect.

- **Physical Interface Type:** Depending on the Operational Mode, this field reports:

- For 802.11a mode: "802.11a (OFDM 5 GHz)."

**NOTE:** In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.

- For 802.11b mode only: "802.11b (DSSS 2.4 GHz)"
- For 802.11g mode: "802.11g (OFDM/DSSS 2.4 GHz)"
- For 802.11b/g mode: "802.11g (OFDM/DSSS 2.4 GHz)"
- For 802.11g-wifi mode: "802.11g (OFDM/DSSS 2.4 GHz)"

OFDM stands for Orthogonal Frequency Division Multiplexing; this is the name for the radio technology used by 802.11a/4.9 GHz devices. DSSS stands for Direct Sequence Spread Spectrum; this is the name for the radio technology used by 802.11b devices.

- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's wireless interface. The MAC address is assigned at the factory.
- **Regulatory Domain:** Reports the regulatory domain for which the AP is certified. Not all features or channels are available in all countries.
- **Network Name (SSID):** Enter a Network Name (between 1 and 32 characters long) for the primary wireless network. You must configure each wireless client using this network to use this name as well. Additional SSIDs and VLANs may be configured under **Configure > SSID/VLAN/Security**. Up to 16 SSID/VLANs may be configured.

**NOTE:** Do not use quotation marks (single or double) in the Network Name; this will cause the AP to misinterpret the name.

- **Enable Auto Channel Select:** When the Enable Auto Channel Select option is enabled, the AP scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled. See [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) for more information and [Available Channels](#) for a list of available channels.
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating Channel. When Auto Channel Select is disabled, you can specify the Access Point's operating channel. If you decide to manually set the unit's Channel, ensure that nearby devices do not use the same frequency (unless you are setting up WDS links). Available channels vary based on regulatory domain. See [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) for more information and [Available Channels](#) for a list of available channels.
- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP. The values depend on the Operational mode. Auto Fallback is the default setting; it allows the AP unit to select the best transmit rate based on the cell size.

- For 802.11a only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s.

**NOTE:** In countries in which 802.11a (5 GHz) is not available for use, the AP-700 provides dual-band (802.11b and 802.11g) support only. 802.11a functionality covered in this User Guide is not supported.

- For 802.11b only -- Auto Fallback, 1, 2, 5.5, 11 Mbits/sec.
- For 802.11g only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/sec
- For 802.11b/g -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec
- For 802.11g-wifi -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec

**NOTE:** 802.11g-wifi has been defined for Wi-Fi testing purposes. It is not recommended for use in your wireless network environment.

**NOTE:** Turbo mode is supported in only in 802.11a mode in the FCC regulatory domain when DFS is not required. If turbo mode is enabled, then this is displayed in the web UI and the transmit speeds and channels pull-down menus are updated with the valid values.

- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) Period determines when to transmit broadcast and multicast packets to all clients. If any clients are in power save mode, packets are sent at the end of the DTIM period. This parameter supports a range between 1 and 255; it is recommended to leave the DTIM at its default value unless instructed by technical support. Higher values conserve client battery life at the expense of network performance for broadcast or multicast traffic.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See [RTS/CTS Medium Reservation](#) for more information.
- **Antenna Gain:** This parameter modifies the sensitivity of the radio card when detecting radar signals in accordance with [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) requirements. Given that the radar detection threshold is fixed by the regulatory codes in the country of operation, and that a variety of antennas with different gains may be attached to the unit, adjust this threshold to account for higher than expected antenna gains and avoid false radar detection events. Set this parameter to a value between 0 and 35. The default value is 0.
- **Wireless Service Status:** Select **Shutdown** to shutdown the wireless service on a wireless interface, or to **Resume** to resume wireless service. See [Wireless Service Status](#) for more information.
- **Load Balancing Max Clients:** Load balancing distributes clients among available access points. Enter a number between 1 and 63 to specify the maximum number of clients to allow.
- **Channel Blacklist Table:** The Channel Blacklist table contains all available channels. It can be used to manually blacklist channels, and it also reflects channels that have been automatically blacklisted by the [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) function. See [Channel Blacklist Table](#) for configuration information.
- **Wireless Distribution System:** A Wireless Distribution system can be used to establish point-to-point (i.e. wireless backhaul) connections with other access points. See [Wireless Distribution System \(WDS\)](#) for configuration information.

### Dynamic Frequency Selection/Radar Detection (DFS/RD)

In order to prevent interference with radar systems and other devices that occupy the 5 GHz band, 802.11a APs certified in the ETSI, TELEC, FCC, and IC regulatory domains (see [Affected Countries](#)) and operating in the middle and high frequency bands select an operating channel through a combination of Auto Channel Select (ACS) and Dynamic Frequency Selection (DFS)/Radar Detection (RD).

During boot-up, ACS scans the available channels and selects the best channel. Once a channel is selected, the AP performs a channel availability check for 60 seconds to ensure that the channel is not busy or occupied by radar, and then commences normal operation. (In Canada, if the channel was previously blacklisted, the AP scans for 600 seconds before commencing normal operation if the selected channel frequency is in the 5600 - 5650 MHz range). When the AP enters normal operation, DFS works in the background to detect interference in that channel. If interference is detected, the AP sends a trap, disassociates all clients, blacklists the channel, and reboots. After it reboots, ACS re-scans and selects a better channel that is not busy and is free of radar interference.

If ACS is disabled, only channels in the lower, upper, and ISM frequency bands are available for use:

- 36: 5.180 GHz (default)
- 40: 5.200 GHz
- 44: 5.220 GHz
- 48: 5.240 GHz
- 149: 5.745 GHz
- 153: 5.765 GHz
- 157: 5.785 GHz

- 161: 5.805 GHz
- 165: 5.825 GHz

If you are using the unit in a country and band that require DFS, keep in mind the following:

- DFS is not a configurable parameter; it is always enabled and cannot be disabled.
- You cannot manually select the device's operating channel; you must let the unit select the channel. You may make channels unavailable by manually "blacklisting" them and preventing those channels being selected, in accordance with local regulations or interference. You can also display the Channel Blacklist Table to view the channels that have been blacklisted by the AP.
- In compliance with FCC regulations, the AP uses ATPC (Automatic Transmit Power Control) to automatically adapt transmit power when the quality of the link is more than sufficient to maintain a good communication with reduced transmit power. See [Transmit Power Control/Transmit Power Level](#) for more information.

DFS is required for three purposes:

1. *Radar avoidance both at startup and while operational.* To meet these requirements, the AP scans available frequencies at startup. If a DFS enabled channel is busy or occupied with radar, the system will blacklist the channel for a period of 30 minutes in accordance with FCC, IC, ETSI, and TELEC regulations. Once fully operational on a frequency, the AP actively monitors the occupied frequency. If interference is detected, the AP blacklists the channel, logs a message and rescans to find a new frequency that is not busy and is free of radar interference.
2. *Guarantee the efficient use of available frequencies by all devices in a certain area.* To meet this requirement, the AP scans each available frequency upon startup and selects a frequency based upon the least amount of noise and interference detected. This lets multiple devices operate in the same area with limited interference. This procedure is done only at startup; if another UNII device comes up on the same frequency, the AP does not detect this or rescan because of it. It is expected that other devices using these frequencies also are in compliance with country regulations, so this should not happen.
3. *Uniform Channel Spreading.* To meet this requirement, the AP randomly selects its operating channel from the available channels with least interference.

### Affected Countries

Japan is certified in the TELEC regulatory domain, Canada is certified in the IC regulatory domain, and the USA is certified in the FCC regulatory domain for operation in the 5 GHz band.

The following countries are certified in the ETSI regulatory domain for operation in the 5 GHz band:

- |                  |               |               |
|------------------|---------------|---------------|
| – Austria        | – Greece      | – Norway      |
| – Belgium        | – Hungary     | – Poland      |
| – Czech Republic | – Ireland     | – Portugal    |
| – Cyprus         | – Italy       | – Spain       |
| – Denmark        | – Latvia      | – Sweden      |
| – Estonia        | – Lithuania   | – Switzerland |
| – Finland        | – Luxembourg  | – UK          |
| – France         | – Malta       |               |
| – Germany        | – Netherlands |               |

### RTS/CTS Medium Reservation

The 802.11 standard supports optional RTS/CTS communication based on packet size. Without RTS/CTS, a sending radio listens to see if another radio is already using the medium before transmitting a data packet. If the medium is free, the sending radio transmits its packet. However, there is no guarantee that another radio is not transmitting a packet at the same time, causing a collision. This typically occurs when there are hidden nodes (clients that can communicate with the Access Point but are out of range of each other) in very large cells.

When RTS/CTS occurs, the sending radio first transmits a Request to Send (RTS) packet to confirm that the medium is clear. When the receiving radio successfully receives the RTS packet, it transmits back a Clear to Send (CTS) packet to the sending radio. When the sending radio receives the CTS packet, it sends the data packet to the receiving radio. The RTS and CTS packets contain a reservation time to notify other radios (including hidden nodes) that the medium is in use for a specified period. This helps to minimize collisions. While RTS/CTS adds overhead to the radio network, it is particularly useful for large packets that take longer to resend after a collision occurs.

RTS/CTS Medium Reservation is an advanced parameter and supports a range between 0 and 2347 bytes. When set to 2347 (the default setting), the RTS/CTS mechanism is disabled. When set to 0, the RTS/CTS mechanism is used for all packets. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. You should not need to enable this parameter for most networks unless you suspect that the wireless cell contains hidden nodes.

### Wireless Service Status

The user can shut down (or resume) the wireless service on the wireless interface of the AP through the CLI, HTTP, or SNMP interface. When the wireless service on a wireless interface is shut down, the AP will:

- Stop the AP services to wireless clients connected on that wireless interface by disassociating them
- Disable the associated BSS ports on that interface
- Disable the transmission and reception of frames on that interface
- Indicate the wireless service shutdown status of the wireless interface through LED and traps
- Enable Ethernet interface so that it can receive a wireless service resume command through CLI/HTTP/SNMP interface

**NOTE:** WSS disables BSS ports.

**NOTE:** The wireless service cannot be shutdown on an interface where Rogue Scan is enabled.

In shutdown state, AP will not transmit and receive frames from the wireless interface and will stop transmitting periodic beacons. Moreover, none of the frames received from the Ethernet interface will be forwarded to that wireless interface.

Wireless service on a wireless interface of the AP can be resumed through CLI/HTTP/SNMP management interface. When wireless service on a wireless interface is resumed, the AP will:

- Enable the transmission and reception of frames on that wireless interface
- Enable the associated BSS port on that interface
- Start the AP services to wireless clients
- Indicate the wireless service resume status of the wireless interface through LED and traps

After wireless service resumes, the AP resumes beaconing, transmitting and receiving frames to/from the wireless interface and bridging the frames between the Ethernet and the wireless interface.

### Traps Generated During Wireless Service Shutdown (and Resume)

The following traps are generated during wireless service shutdown and resume, and are also sent to any configured Syslog server.

When the wireless service is shut down on a wireless interface, the AP generates a trap called *oriTrapWirelessServiceShutdown*.

When the wireless service is resumed on a wireless interface, the AP generate a trap called *oriTrapWirelessServiceResumed*.

### Channel Blacklist Table

The Channel Blacklist table contains all available channels (channels vary based on regulatory domain). It can be used to manually blacklist channels, and it also reflects channels that have been automatically blacklisted by the [Dynamic Frequency Selection/Radar Detection \(DFS/RD\)](#) function. In the IC, FCC, ETSI, and TELEC regulatory domains, a



channel is blacklisted automatically if it is found to be busy or occupied by radar during a scan at start-up. When a channel has been automatically blacklisted, it will remain blacklisted for 30 minutes. Additionally, an administrator can blacklist channels manually to prevent them from being used when ACS is enabled. To blacklist a channel manually:

1. Click on **Configure > Interfaces > Wireless A**.
2. Scroll down to the **Channel Blacklist** heading.

**Channel Blacklist Table**

This table is used to configure blacklist channels. A channel can be blacklisted automatically if radar is detected on the operating channel (this is applicable only to specific regulatory domains). If radar is detected on a channel, that channel will be blacklisted for 30 minutes. A channel can also be blacklisted by the administrator in case that channel is not to be used when ACS is enabled.

Channel	Radar Detected	Elapsed Time (Minutes)	Blacklist Status
1	FALSE	0	Disable
2	FALSE	0	Disable
3	FALSE	0	Disable
4	FALSE	0	Disable
5	FALSE	0	Disable
6	FALSE	0	Disable
7	FALSE	0	Disable
8	FALSE	0	Disable
9	FALSE	0	Disable
10	FALSE	0	Disable
11	FALSE	0	Disable
12	FALSE	0	Disable
13	FALSE	0	Disable

Figure 4-11 Channel Blacklist Table

3. Click **Edit** in the Channel Blacklist Table
4. Set **Blacklist Status** to **Enable**.

**Channel Blacklist Table**

This page is used to configure blacklisted channels. You can blacklist a channel by setting the Blacklist Status to Enable.

Channel	1
Blacklist Status	<input type="text" value="Enable"/>
Channel	2
Blacklist Status	<input type="text" value="Disable"/>
Channel	3
Blacklist Status	<input type="text" value="Enable"/>

Figure 4-12 Channel Blacklist Table - Edit Screen



### Wireless Distribution System (WDS)

A Wireless Distribution System (WDS) creates a link between two 802.11a, 802.11b, or 802.11b/g APs over their radio interfaces. This link relays traffic from one AP that does not have Ethernet connectivity to a second AP that has Ethernet connectivity. WDS allows you to configure up to six (6) ports.

In the WDS example below, AP 1 and AP 2 communicate over a WDS link (represented by the blue line). This link provides Client 2 with access to network resources even though AP 2 is not directly connected to the Ethernet network. Packets destined for or sent by the client are relayed between the Access Points over the WDS link.

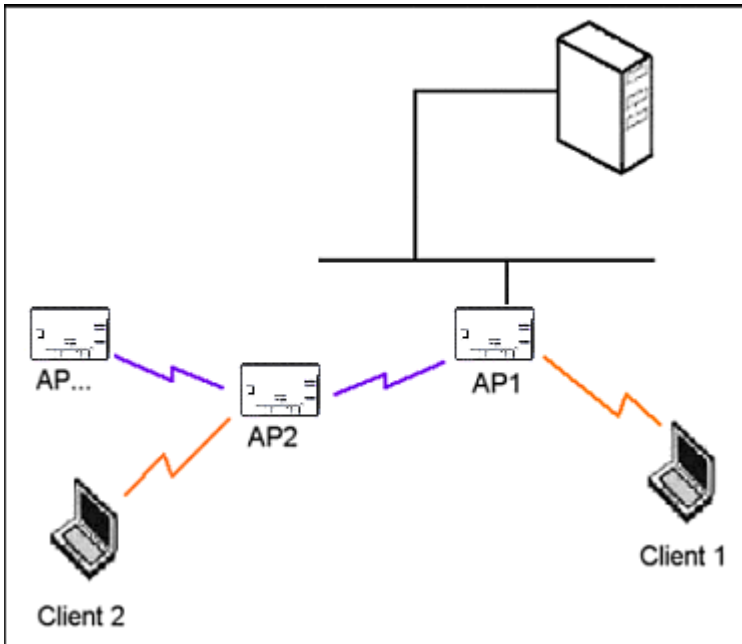


Figure 4-13 WDS Example

#### Bridging WDS

Each WDS link is mapped to a logical WDS port on the AP. WDS ports behave like Ethernet ports rather than like standard wireless interfaces: on a BSS port, an Access Point learns by association and from frames; on a WDS or Ethernet port, an Access Point learns from frames only. When setting up a WDS, keep in mind the following:

- There are separate security settings for clients and WDS links. The same WDS link security mode must be configured (currently we only support none or WEP) on each Access Point in the WDS and the same WEP key must be configured.
- The WDS link shares the communication bandwidth with the clients. Therefore, while the maximum data rate for the Access Point's cell is 54 Mbits/second (802.11a, 802.11g only, or 802.b/g modes) or 11 Mbits/second (802.11b only mode), client throughput will decrease when traffic is passing over the WDS link.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- A WDS port on a single AP should have a unique partner MAC address. Do not enter the same MAC address twice in an AP's WDS port list.
- Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.
- If your network does not support spanning tree, be careful to avoid creating network loops between APs. For example, creating a WDS link between two Access Points connected to the same Ethernet network will create a network loop (if spanning tree is disabled). For more information, see the [Spanning Tree](#) section.

- When WDS is enabled, Spanning Tree protocol is automatically enabled. It may be manually disabled. If Spanning Tree protocol is enabled by WDS and WDS is subsequently disabled, Spanning tree will remain enabled until it is manually disabled. See [Spanning Tree](#).

### WDS Setup Procedure

**NOTE:** You must disable Auto Channel Select to create a WDS. Each Access Point that is a member of the WDS must have the same channel setting to communicate with each other.

To setup a wireless backbone follow the steps below for each AP that you wish to include in the Wireless Distribution System.

1. Confirm that Auto Channel Select is disabled.
2. Write down the MAC Address of the radio that you wish to include in the Wireless Distribution System.
3. Click on **Configure > Interfaces > Wireless A**.
4. Scroll down to the **Wireless Distribution System** heading.

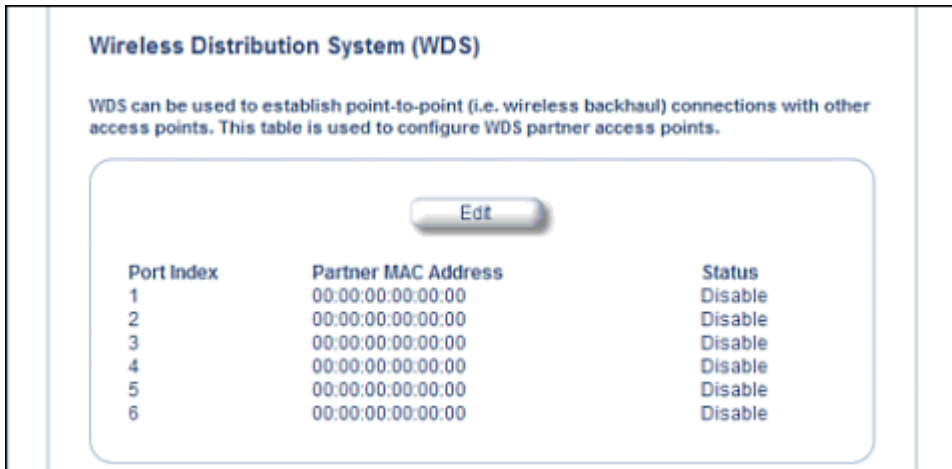


Figure 4-14 WDS Configuration

5. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.

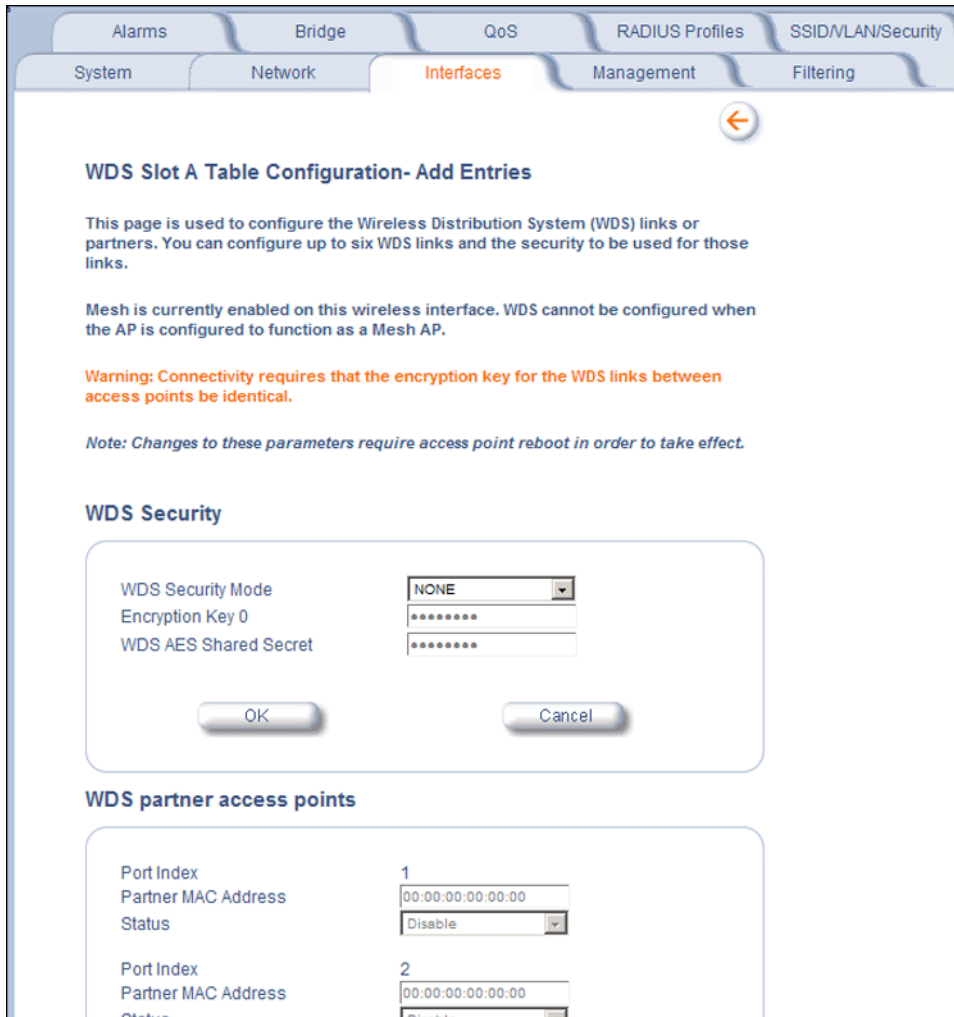


Figure 4-15 Adding WDS Links

6. Select which encryption method to use (if any) from the **WDS Security Mode** drop-down menu.
7. If you selected a WDS Security Mode, do one of the following:
  - If you selected WEP: Enter an encryption key.
  - If you selected AES: Enter a shared secret.
8. Enter the MAC Address that you wrote down in Step 2 in one of the **Partner MAC Address** field of the Wireless Distribution Setup window.
9. Set the **Status** of the device to **Enable**.
10. Click **OK**.
11. Reboot the AP.

## Ethernet

Select the desired speed and transmission mode from the drop-down menu. Half-duplex means that only one side can transmit at a time and full-duplex allows both sides to transmit. When set to auto-duplex, the AP negotiates with its switch or hub to automatically select the highest throughput option supported by both sides.



Figure 4-16 Ethernet Sub-tab

For best results, Proxim recommends that you configure the Ethernet setting to match the speed and transmission mode of the device the Access Point is connected to (such as a hub or switch). If in doubt, leave this setting at its default, **auto-speed-auto-duplex**. Choose between:

- 10 Mbit/s - half duplex or full duplex
- 100 Mbit/s - half duplex or full duplex
- Auto speed - auto duplex

## Management

The Management tab contains the following sub-tabs:

- [Passwords](#)
- [IP Access Table](#)
- [Services](#)
- [Automatic Configuration \(AutoConfig\)](#)
- [Hardware Configuration Reset \(CHRD\)](#)

### Passwords

Passwords are stored in flash memory and secured using encryption. You can configure the following password:

- **SNMP Read Community Password:** The password for read access to the AP using SNMP. Enter a password between 6 and 32 characters in both the **Password** field and the **Confirm** field. The default password is **public**.
- **SNMP Read/Write Community Password:** The password for read and write access to the AP using SNMP. Enter a password between 6 and 32 characters in both the **Password** field and the **Confirm** field. The default password is **public**.
- **SNMPv3 Authentication Password:** The password used when sending authenticated SNMPv3 messages. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters, but a length of at least 8 characters is recommended. The default password is **public**. Secure Management (Services tab) must be enabled to configure SNMPv3.

The default SNMPv3 username is **administrator**, with SHA authentication and DES privacy protocol.

- **SNMPv3 Privacy Password:** The password used when sending encrypted SNMPv3 data. Enter a password in both the **Password** field and the **Confirm** field. This password must be between 6 and 32 characters, but a length of at least 8 characters is recommended. The default password is **public**. Secure Management (Services tab) must be enabled to configure SNMPv3.
- **Telnet (CLI) Password:** The password for the CLI interface (via serial or Telnet). Enter a password between 6 and 32 characters in both the **Password** field and the **Confirm** field. The default password is **public**.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password between 6 and 32 characters in both the **Password** field and the **Confirm** field. The default password is **public**.

**NOTE:** For security purposes Proxim recommends changing ALL PASSWORDS from the default “public” immediately, to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform a [Soft Reset to Factory Defaults](#) or [Hard Reset to Factory Defaults](#).

The screenshot shows a web-based configuration interface for an Access Point. The top navigation bar includes tabs for Alarms, Bridge, QoS, RADIUS Profiles, and SSID/VLAN/Security. Below this, a secondary navigation bar highlights the 'Management' tab, with other tabs for System, Network, Interfaces, and Filtering. Under the 'Management' tab, there are sub-tabs for Passwords, IP Access Table, Services, AutoConfig, and CHR. The 'Passwords' sub-tab is active, displaying a configuration page with the following text: 'This tab is used to configure SNMPv1/v2c community, SNMPv3 authentication, SNMPv3 privacy, Telnet (CLI), and HTTP (web) passwords.' Below this is a note: 'Change the default passwords to a value known only to you. If this is not done, then users may be able to manage the access point and modify its configuration without your knowledge.' Another note states: 'Note: Changes to Password must be between 6 and 32 characters'. The form contains several password fields, each with a 'Confirm' field: 'SNMP Read Community Password', 'SNMP Read/Write Community Password', 'SNMPv3 Authentication Password', 'SNMPv3 Privacy Password', 'Telnet (CLI) Password', and 'HTTP (web) Password'. At the bottom of the form are 'OK' and 'Cancel' buttons.

## IP Access Table

The Management IP Access table limits in-band management access to the IP addresses or range of IP addresses specified in the table. This feature applies to all management services (SNMP, HTTP, and CLI) except for CLI management over the serial port. To configure this table, click **Add** and set the following parameters:

- **IP Address:** Enter the IP Address for the management station.
- **IP Mask:** Enter a mask that will act as a filter to limit access to a range of IP Addresses based on the IP Address you already entered.
  - The IP mask 255.255.255.255 would authorize the single station defined by the IP Address to configure the Access Point. The AP would ignore commands from any other IP address. In contrast, the IP mask 255.255.255.0 would allow any device that shares the first three octets of the IP address to configure the AP. For example, if you enter an IP address of 10.20.30.1 with a 255.255.255.0 subnet mask, any IP address between 10.20.30.1 and 10.20.30.254 will have access to the AP's management interfaces.
- **Comment:** Enter an optional comment, such as the station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

## Services

You can configure the following management services:

### Secure Management

Secure Management allows the use of encrypted and authenticated communication protocols such as SNMPv3, Secure Socket Link (SSL), and Secure Shell (SSH) to manage the Access Point.

- **Secure Management Status:** Enables the further configuration of HTTPS Access, SNMPv3, and Secure Shell (SSH). After enabling Secure Management, you can choose to configure HTTPS (SSL) and Secure Shell access on the Services tab, and to configure SNMPv3 passwords on the Passwords tab.

### SNMP Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**Ethernet, Wireless, All Interfaces**) from which you will manage the AP via SNMP. You can also select **Disabled** to prevent a user from accessing the AP via SNMP.

### HTTP Access

- **HTTP Interface Bitmap:** Configure the interface or interfaces (**Ethernet, Wireless, All Interfaces**) from which you will manage the AP via the Web interface. For example, to allow Web configuration via the Ethernet network only, set **HTTP Interface Bitmap** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the AP from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the AP via the Web interface. By default, the HTTP port is 80. You must reboot the Access Point if you change the HTTP Port.
- **HTTP Wizard Status:** The Setup Wizard appears automatically the first time you access the HTTP interface. If you exited out of the Setup Wizard and want to relaunch it, enable this option, click **OK**, and then close your browser or reboot the AP. The Setup Wizard will appear the next time you access the HTTP interface.

### HTTPS Access (Secure Socket Layer)

**NOTE:** SSL requires Internet Explorer version 6, 128 bit encryption, Service Pack 1, and patch Q323308.

**NOTE:** You need to reboot the AP after enabling or disabling SSL for the changes to take effect.

- **HTTPS (Secure Web Status):** The user can access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP comes pre-installed with all required SSL files: default certificate and private key installed. Use the drop-down menu to enable/disable this feature.
- **SSL Certificate Passphrase:** After enabling SSL, the only configurable parameter is the SSL passphrase. The default SSL passphrase is **proxim**.

The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate.

If you decide to upload a new certificate and private key (using TFTP or HTTP File Transfer), you need to change the SSL Certificate Passphrase for the new SSL files.

### Accessing the AP through the HTTPS interface

The user should use a SSL intelligent browser to access the AP through the HTTPS interface. After configuring SSL, access the AP using **https://** followed by the AP's management IP address.

Alarms	Bridge	QoS	RADIUS Profiles	SSID/LAN/Security
System	Network	Interfaces	<b>Management</b>	Filtering
Passwords	IP Access Table	<b>Services</b>	AutoConfig	CHRD

This tab is used to configure Secure Management, SNMP, Telnet (CLI), and HTTP (web) parameters.

Secure Management option allows the use of encrypted and authenticated communication protocols such as SNMPv3, and Secure Socket Link (SSL), to manage the Access Point. When Secure Management is turned on, the scope and access for the traditional non-secure means to manage the Access Point is automatically curtailed.

*Note: Changes to the parameters in this page except Radius Based Management Access Parameters and Secure Shell parameters (SSH Enable/Disable and SSH Key Status) require access point reboot in order to take effect.*

**Warning!** Generation of SSH keys may take up to 3-4 minutes and the Access Point may not respond during that time.

SSH keys can be generated by setting the SSH Host Key Status to create or by enabling SSH when no keys are present.

If Secure Management is enabled when SSH is not enabled, the key generation will happen after the next reboot.

Secure Management Status:

---

SNMP Interface Bitmask:

---

HTTP Interface Bitmask:

HTTP Port:

HTTP Wizard Status:

HTTPS (Secure Web) Status:

SSL Certificate Passphrase:

---

Telnet Interface Bitmask:

Telnet Port Number:

Telnet Login Idle Timeout (seconds):

Telnet Session Idle Timeout (seconds):

SSH (Secure Shell) Status:

SSH Host Key Status:

SSH Host Key FingerPrint:

---

Serial Baud Rate:

Serial Flow Control:

Serial Data Bits:

Serial Parity:

Serial Stop Bits:

---

HTTP RADIUS Access Control Status:

Telnet RADIUS Access Control Status:

Radius Profile for Management Access Control:

Local User Status:

Local User Password (6-32 characters):

Confirm Password:

Figure 4-17 Management Services Configuration Screen



### Telnet Configuration Settings

- **Telnet Interface Bitmask:** Select the interface (**Ethernet, Wireless, All Interfaces**) from which you can manage the AP via telnet. This parameter can also be used to **Disable** telnet management.
- **Telnet Port Number:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select). You must reboot the Access Point if you change the Telnet Port.
- **Telnet Login Idle Timeout (seconds):** Enter the number of seconds the system will wait for a login attempt. The AP terminates the session when it times out. The range is 30 to 300 seconds; the default is 60 seconds.
- **Telnet Session Idle Timeout (seconds):** Enter the number of seconds the system will wait during a session while there is no activity. The AP will terminate the session on timeout. The range is 60 to 36000 seconds; the default is 900 seconds.

### Secure Shell (SSH) Settings

The AP supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data.

The SSH server (AP) has **host keys** - a pair of asymmetric keys - a **private key** that resides on the AP and a **public key** that is distributed to clients that need to connect to the AP. As the client has knowledge of the server host keys, the client can verify that it is communicating with the correct SSH server. The client authentication is performed as follows:

- Using a username/password pair if RADIUS Based Management is enabled; otherwise, using a password to authenticate the user over a secure channel created using SSH.

#### SSH Session Setup

An SSH session is setup through the following process:

- The SSH server public key is transferred to the client using out-of-band or in-band mechanisms.
- The SSH client verifies the correctness of the server using the server's public key.
- The user/client authenticates to the server.
- An encrypted data session starts. The maximum number of SSH sessions is limited to two. If there is no activity for a specified amount of time (the Telnet Session Timeout parameter), the AP will timeout the connection.

#### SSH Clients

The following SSH clients have been verified to interoperate with the AP's server. The following table lists the clients, version number, and the website of the client.

Clients	Version	Website
OpenSSH	V3.4-2	<a href="http://www.openssh.com">http://www.openssh.com</a>
Putty	Rel 0.53b	<a href="http://www.chiark.greenend.org.uk">http://www.chiark.greenend.org.uk</a>
Zoc	5.00	<a href="http://www.emtec.com">http://www.emtec.com</a>
Axessh	V2.5	<a href="http://www.labf.com">http://www.labf.com</a>

For key generation, OpenSSH client has been verified.

#### Configuring SSH

Perform the following procedure to set the SSH host key and enable or disable SSH:

1. Click **Configure > Management > Services**
2. Select the **SSH Host Key Status** from the drop down menu.

**NOTE:** SSH Host Key Status can not be changed if SSH status or Secure Management is enabled.

3. To enable/disable SSH, select Enable/Disable from the **SSH (Secure Shell) Status** drop-down menu.

**NOTE:** When Secure Management is enabled on the AP, SSH will be enabled by default and cannot be disabled.

Host keys must either be generated externally and uploaded to the AP (see [Uploading Externally Generated Host Keys](#)), generated manually, or auto-generated at the time of SSH initialization if SSH is enabled and no host keys are present. There is no key present in an AP that is in a factory default state.

To manually generate or delete host keys on the AP:

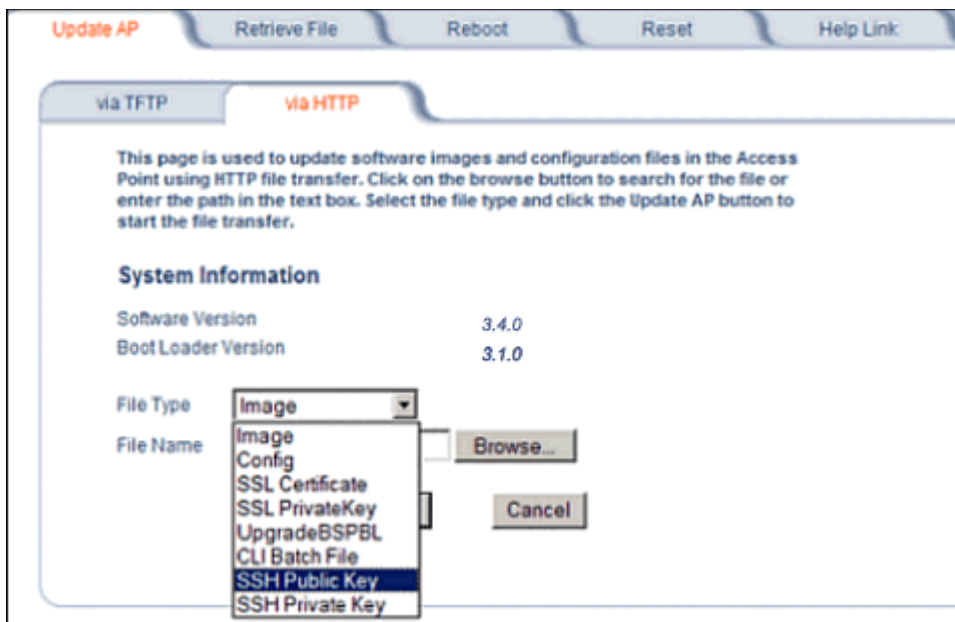
**CAUTION:** SSH Host key creation may take 3 to 4 minutes during which time the AP may not respond.

- Select **Create** to generate a new pair of host keys.
- Select **Delete** to remove the host keys from the AP. If no host keys are present, the AP will not allow connections using SSH. When host keys are created or deleted, the AP updates the fingerprint information displayed on the **Management > Services** page.

### Uploading Externally Generated Host Keys

Perform the following procedure to upload externally generated host keys to the AP. You must upload both the SSH public key and SSH private key for SSH to work.

1. Verify that the host keys have been externally generated. The OpenSSH client has been verified to interoperate with AP's SSH server.
2. Click **Commands > Update AP > via HTTP** (or via TFTP).



**Figure 4-18** Uploading an Externally Generated SSH Public Key and SSH Private Key

3. Select **SSH Public Key** from the File Type drop-down menu.
4. Click **Browse**, select the SSH Public Key file on your local machine.
5. Click **Open**.
6. to initiate the file transfer, click the **Update AP** button.
7. Select **SSH Private Key** from the File Type drop-down menu.
8. Click **Browse**, select the SSH Private Key on your local machine.
9. Click **Open**.
10. To initiate the file transfer, click the **Update AP** button.

The fingerprint of the new SSH public key will be displayed in the **Management > Services** page.

## Serial Configuration Settings

The serial port interface on the AP is enabled at all times. See [Setting IP Address using Serial Port](#) for information on how to access the CLI interface via the serial port. You can configure and view the following parameters:

- **Serial Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Serial Flow Control:** Select either **None** (default) or **Xon/Xoff** (software controlled) data flow control.

**NOTE:** To avoid potential problems when communicating with the AP through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).

- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

**NOTE:** The serial port bit configuration is commonly referred to as **8N1**.

## RADIUS Based Management Access

User management of APs can be centralized by using a RADIUS server to store user credentials. The AP cross-checks credentials using RADIUS protocol and the RADIUS server accepts or rejects the user.

HTTP/HTTPS and Telnet/SSH users can be managed with RADIUS. Serial CLI and SNMP cannot be managed by RADIUS. Two types of users can be supported using centralized RADIUS management:

- **Super User:** The super user has access to all functionality of a management interface. A super user is configured in the RADIUS server by setting the filter ID attribute (returned in the RADIUS Accept packet) for the user to a value of “super user” (not case sensitive). A user is considered a super user if the value of the **filter-id** attribute returned in the RADIUS Accept packet for the user is “super user” (not case sensitive).
- **Limited User:** A limited user has access to only a limited set of functionality on a management interface. All users who are not super users are considered limited users. However, a limited user is configured in the RADIUS server by setting the **filter-id** attribute (returned in the RADIUS Accept packet) to “limited user” (not case sensitive). Limited users do not have access to the following configuration capabilities:
  - Update/retrieve files to and from APs
  - Reset the AP to factory defaults
  - Reboot the AP
  - Change management properties related to RADIUS, management modes, and management passwords.

**NOTE:** When a user has both “limited user” and “super user” filter-ids configured in the Radius server, the user has limited user privileges.

When RADIUS Based Management is enabled, a **local user** can be configured to provide Telnet, SSH, and HTTP(S) access to the AP when RADIUS servers fail. The local user has super user capabilities. When secure management is enabled, the local user can only login using secure means (i.e., SSH or SSL). When the local user option is disabled the only access to the AP when RADIUS servers are down will be through serial CLI or SNMP.

The Radius Based Management Access parameters allows you to enable HTTP or Telnet Radius Management Access, to configure a RADIUS Profile for management access control, and to enable or disable local user access, and configure the local user password. You can configure and view the following parameters:

- **HTTP RADIUS Access Control Status:** Enable RADIUS management of HTTP/HTTPS users.
- **Telnet RADIUS Access Control Status:** Enable RADIUS management of Telnet/SSH users.

- **RADIUS Profile for Management Access Control:** Specifies the RADIUS Profile to be used for RADIUS Based Management Access.
- **Local User Status:** Enables or disables the local user when RADIUS Based Management is enabled. The default local user ID is root.
- **Local User Password and Confirm Password:** The default local user password is public. "Root" cannot be configured as a valid user for Radius based management access when local user access is enabled.

## Automatic Configuration (AutoConfig)

The Automatic Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Automatic Configuration is disabled by default. The configuration process for Automatic Configuration varies depending on whether the AP is configured for dynamic or static IP.

When an AP is configured for dynamic IP, the Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. When configured for static IP, these parameters are instead configured in the AP interface.

After setting up automatic configuration you must reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If Syslog is configured, a Syslog message will appear indicating the success or failure of the Automatic Configuration.

### Auto Configuration and the CLI Batch File

The Auto Configuration feature allows download of the LTV (Length, Type, Value) format configuration file or the CLI Batch file. The LTV file contains parameters used by the AP; the CLI Batch file contains CLI executable commands used to set AP parameters. The AP detects whether the uploaded file is LTV format or a CLI Batch file. If the AP detects an LTV file, it stores the file in the AP's flash memory. If the AP detects a CLI Batch file (a file with an extension of .cli), the AP executes the commands contained in the file immediately. The AP will reboot after executing the CLI Batch file. Auto Configuration will not result in repeated reboots if the CLI Batch file contains rebootable parameters.

For more information, see the [CLI Batch File](#) section.

### Set up Automatic Configuration for Static IP

Perform the following procedure to enable and set up Automatic Configuration when you have a static IP address for the TFTP server.

1. Click **Configure > Management > AutoConfig**. The Automatic Configuration Screen appears.
2. Check **Enable Auto Configuration**.
3. Enter the **Configuration Filename**. The default is **config**.
4. Enter the IP address of the TFTP server in the **TFTP Server Address** field. The default is **169.254.128.133**.

**NOTE:** The default filename is "config". The default TFTP IP address is **169.254.128.133**.

5. Click **OK** to save the changes.
6. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:
  - AutoConfig for Static IP
  - TFTP server address and configuration filename
  - AutoConfig Successful

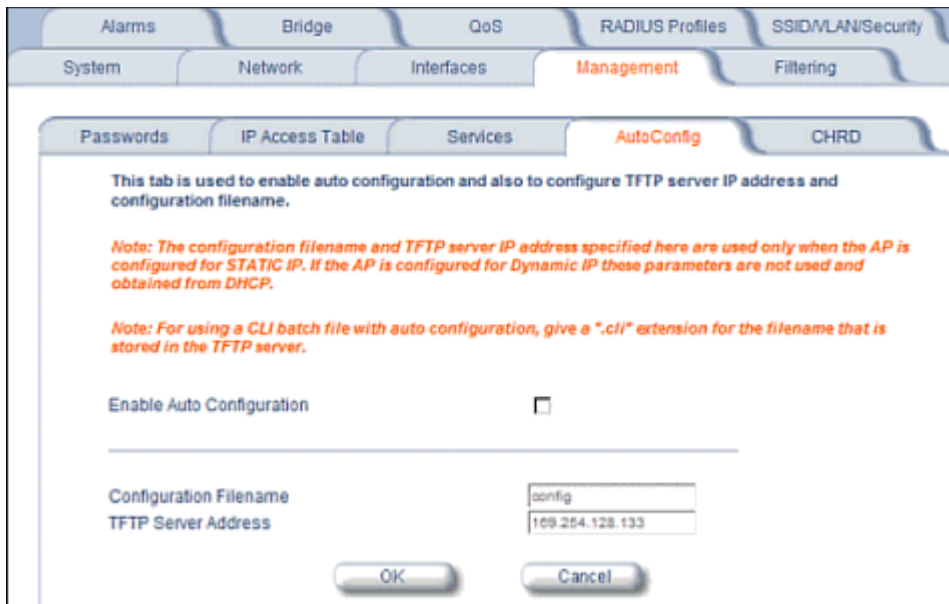


Figure 4-19 Automatic Configuration Screen

#### Set up Automatic Configuration for Dynamic IP

Perform the following procedure to enable and set up Automatic Configuration when you have a dynamic IP address for the TFTP server via DHCP.

The Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. A Syslog server address is also contained in the DHCP response, allowing the AP to send Auto Configuration success and failure messages to a Syslog server.

**NOTE:** The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP.

1. Click **Configure > Management > AutoConfig**.  
The **Automatic Configuration** screen appears.
2. Check **Enable Auto Configuration**.  
When the AP is Configured with Dynamic IP, the DHCP server should be configured with the TFTP Server IP address ("Boot Server Host Name", option 66) and Configuration file ("Bootfile name", option 67) as follows (note that this example uses a Windows 2000 server):
3. Select **DHCP Server > DHCP Option > Scope**.  
The **DHCP Options: Scope** screen appears.

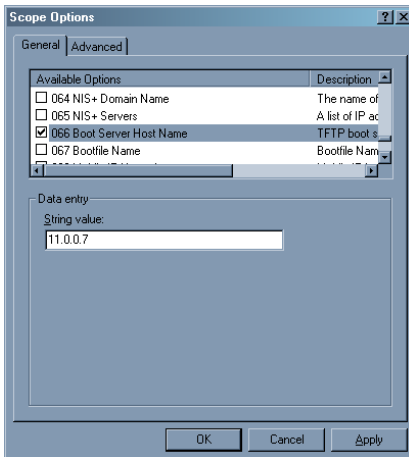


Figure 4-20 DHCP Options: Setting the Boot Server Host Name

4. Add the Boot Server Hostname and Boot Filename parameters to the **Available Options** list.
5. Set the value of the Boot Server Hostname Parameter to the hostname or IP Address of the TFTP server. For example: 11.0.0.7.

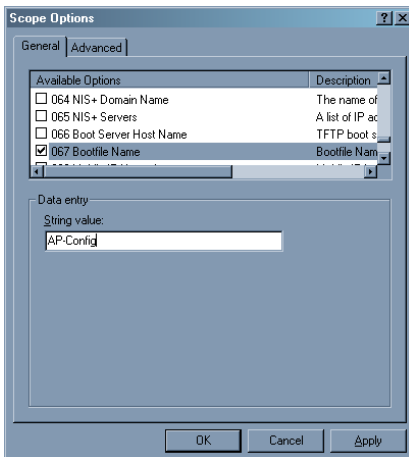


Figure 4-21 DHCP Options: Setting the Bootfile Name

6. Set the value of the Bootfile Name parameter to the Configuration filename. For example: AP-Config.
7. If using Syslog, set the Log server IP address (option 7, Log Servers).
8. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:
  - AutoConfig for Dynamic IP
  - TFTP server address and configuration filename
  - AutoConfig Successful

## Hardware Configuration Reset (CHRD)

Hardware Configuration Reset Status is a parameter that defines the hardware configuration reset behavior of the AP.

If a user loses or forgets the AP's HTTP/Telnet/SNMP password, the Reload button on the power injector provides a way to reset the AP to default configuration values and gain access to the AP. However, in AP deployments where physical

access to the AP is not protected, an unauthorized person could reset the AP to factory defaults and thus gain control of the AP. The user can disable the hardware configuration reset functionality to prevent unauthorized access.

The hardware configuration reset feature operates as follows:

- When hardware configuration reset is enabled, the user can press the Reload button on the power injector for 10 seconds when the AP is in normal operational mode in order to delete the AP configuration.
- When hardware configuration reset is disabled, pressing the Reload button when the AP is in normal operational mode does not have any effect on the AP.
- The hardware configuration reset parameter does not have any effect on the functionality of the reload button to delete the AP image during AP boot loader execution.
- The default hardware configuration reset status is enabled. When disabling hardware configuration reset, the user is recommended to configure a configuration reset password. A configuration reset option appears on the serial port during boot up, before the AP reads its configuration and initializes.
- Whenever the AP is reset to factory default configuration, hardware configuration reset status is enabled and the configuration reset password is set to the default, "public".
- If secure mode is enabled in the AP, only secure (SSL, SNMPv3, SSH) users can modify the values of the Hardware Configuration Reset Status and the configuration reset password.

### Configuration Reset via Serial Port During Bootup

If hardware configuration reset is disabled, the user gets prompted by a configuration reset option to reset the AP to factory defaults during boot up from the serial interface. By pressing a key sequence (ctrl-R), the user gets prompted to enter a configuration reset password before the configuration is reset.

**NOTE:** *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disabled.*

### Configuring Hardware Configuration Reset

Perform the following procedure to configure Hardware Configuration Reset and to set the Configuration Reset Password. See [Figure 4-22](#).

1. Click **Configure > Management > CHR.D**.

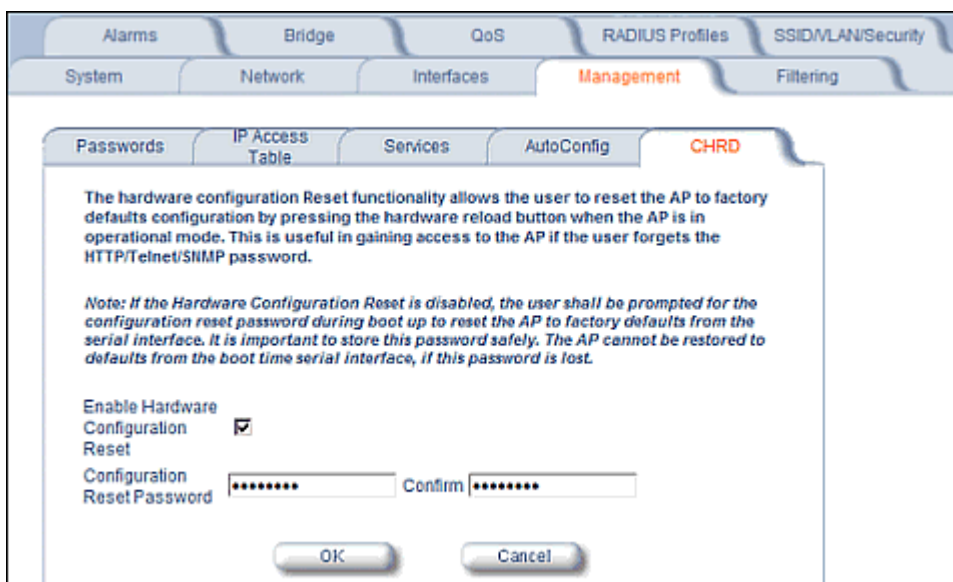


Figure 4-22 Hardware Configuration Reset

2. Check (enable) or uncheck (disable) the **Enable Hardware Configuration Reset** checkbox.
3. Change the default Configuration Reset Password in the “Configuration Reset Password” and “Confirm” fields.
4. Click OK.
5. Reboot the AP.

**NOTE:** *It is important to safely store the configuration reset password. If a user forgets the configuration reset password, the user will be unable to reset the AP to factory default configuration if the AP becomes inaccessible and the hardware configuration reset functionality is disabled.*

**Procedure to Reset Configuration via the Serial Interface**

1. During boot up, observe the message output on the serial interface.  
The AP prompts the user with the message: “Press ctrl-R in 3 seconds to choose configuration reset option.”
2. Enter ctrl-R within 3 seconds after being prompted.  
The AP prompts the user with “Press ctrl-Z to continue with normal boot up or enter password to reset configuration.” If the user enters ctrl-Z, the AP continues to boot with the stored configuration.
3. Enter the configuration reset password. The default configuration reset password is “public”.  
When the correct configuration reset password is entered, the AP gets reset to factory defaults and displays the message “AP has been reset to Factory Default Settings.” The AP continues to boot up. If an incorrect configuration reset password is entered, the AP shows an error message and reprompts the user. If the incorrect password is entered three times in a row, the AP proceeds to boot up.



## Filtering

The Access Point's Packet Filtering features help control the amount of traffic exchanged between the wired and wireless networks. There are four sub-tabs under the Filtering heading:

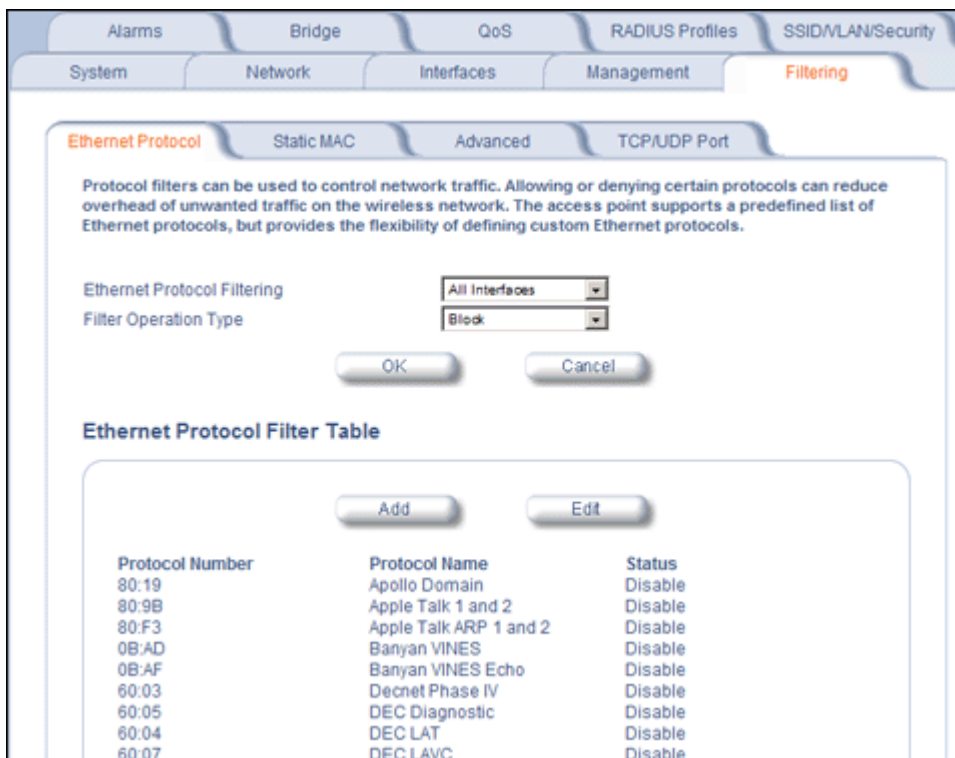
- [Ethernet Protocol](#)
- [Static MAC](#)
- [Advanced](#)
- [TCP/UDP Port](#)

### Ethernet Protocol

The Ethernet Protocol Filter blocks or forwards packets based on the Ethernet protocols they support.

Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interface or interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
  - **Ethernet:** Packets are examined at the Ethernet interface
  - **Wireless:** Packets are examined at the Wireless interface
  - **All Interfaces:** Packets are examined at both interfaces
  - **Disabled:** The filter is not used
2. Select the **Filter Operation Type**.
  - If set to **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table will pass through the bridge.
  - If set to **Block**, the bridge will block enabled Ethernet Protocols listed in the Filter Table.



**Figure 4-23 Ethernet Protocol Filter Configuration**

3. Configure the **Ethernet Protocol Filter Table**. This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.

- To add an entry, click **Add**, and then specify the **Protocol Number** and a **Protocol Name**.
  - Protocol Number:** Enter the protocol number. See <http://www.iana.org/assignments/ethernet-numbers> for a list of protocol numbers.
  - Protocol Name:** Enter related information, typically the protocol name.

Figure 4-24 Ethernet Protocol Filter Table - Add Entries

- To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

**NOTE:** An entry's status must be enabled in order for the protocol to be subject to the filter.

Figure 4-25 Ethernet Protocol Filter Table - Edit Entries

## Static MAC

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is properly configured, the AP can block traffic between wired devices and wireless devices based on MAC address.

For example, you can set up a Static MAC filter to prevent wireless clients from communicating with a specific server on the Ethernet network. You can also use this filter to block unnecessary multicast packets from being forwarded to the wireless network.

**NOTE:** The Static MAC Filter is an advanced feature. You may find it easier to control wireless traffic via other filtering options, such as Ethernet Protocol Filtering.

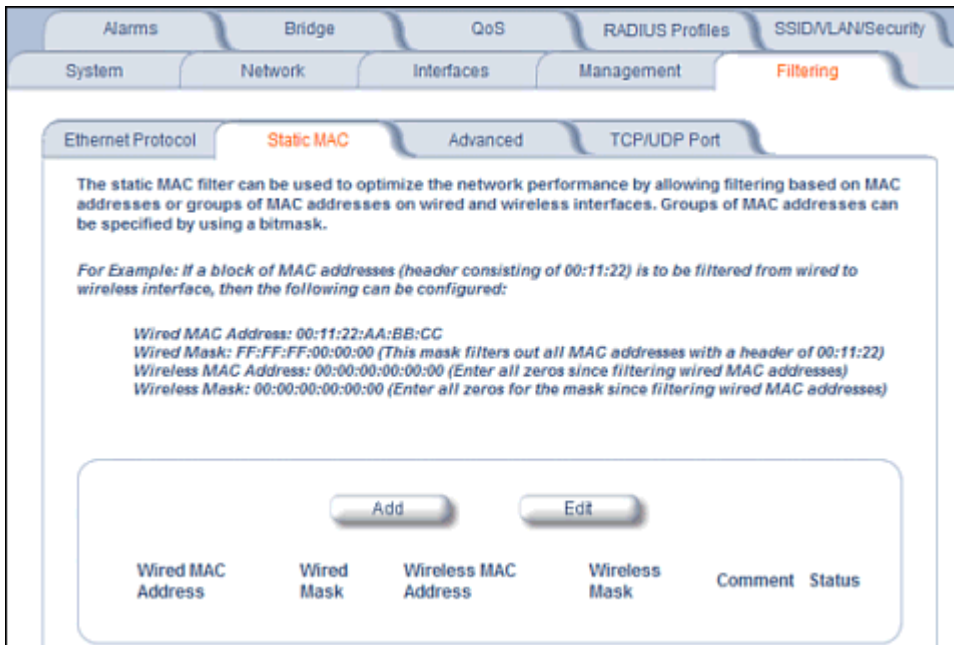


Figure 4-26 Static MAC Filter Configuration

Each static MAC entry contains the following fields:

- **Wired MAC Address**
- **Wired Mask**
- **Wireless MAC Address**
- **Wireless Mask**
- **Comment:** This field is optional.

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1).)

Taken together, a MAC Address/Mask pair specifies an address or a range of MAC addresses that the AP will look for when examining packets. The AP uses Boolean logic to perform an “AND” operation between the MAC Address and the Mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the Mask (where 0 is any value and F is the value specified in the MAC address). A Mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a Mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC Address.

For example, if the MAC Address is 00:20:A6:12:54:C3 and the Mask is FF:FF:FF:00:00:00, the AP will examine the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the Mask is FF:FF:FF:FF:FF:FF, the AP will only look for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want block:

- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC Address and Wired Mask (leave the Wireless MAC Address and Wireless Mask set to all zeros).
- To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC address and Wireless Mask (leave the Wired MAC Address and Wired Mask set to all zeros).
- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

A maximum of 200 entries can be created in the Static MAC filter table. To create an entry, click **Add** and enter the appropriate MAC addresses and Masks to setup a filter. The entry is enabled automatically when saved.

**Figure 4-27 Static MAC Filter Table - Add Entries**

To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

### Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC address for each unit is as follows:

- Wired Server: 00:40:F4:1C:DB:6A
- Wireless Client 1: 00:02:2D:51:94:E4
- Wireless Client 2: 00:02:2D:51:32:12
- Wireless Client 3: 00:20:A6:12:4E:38

#### ***Prevent Two Specific Devices from Communicating***

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 can still communicate with the Wired Server.

#### ***Prevent Multiple Wireless Devices from Communicating with a Single Wired Device***

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical “AND” is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

***Prevent All Wireless Devices from Communicating with a Single Wired Device***

Configure the following settings to prevent all three Wireless Clients from communicating with Wired Server 1:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point blocks all traffic between Wired Server 1 and all wireless clients.

***Prevent a Wireless Device from Communicating with the Wired Network***

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet:

- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The Access Point blocks all traffic between Wireless Client 3 and the Ethernet network.

***Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN***

If there are devices on your Ethernet network that use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

**Advanced**

You can configure the following advanced filtering options:

- **Enable Proxy ARP:** Place a check mark in the box provided to allow the Access Point to respond to Address Resolution Protocol (ARP) requests for wireless clients. When enabled, the AP answers ARP requests for wireless stations without actually forwarding them to the wireless network. If disabled, the Access Point will bridge ARP requests for wireless clients to the wireless LAN.
- **Enable IP/ARP Filtering:** Place a check mark in the box provided to allow IP/ARP filtering based on the IP/ARP Filtering Address and IP Mask. Leave the box unchecked to prevent filtering. If enabled, you should also configure the
  - **IP/ARP Filtering Address:** Enter the Network filtering IP Address.
  - **IP/ARP IP Mask:** Enter the Network Mask IP Address.

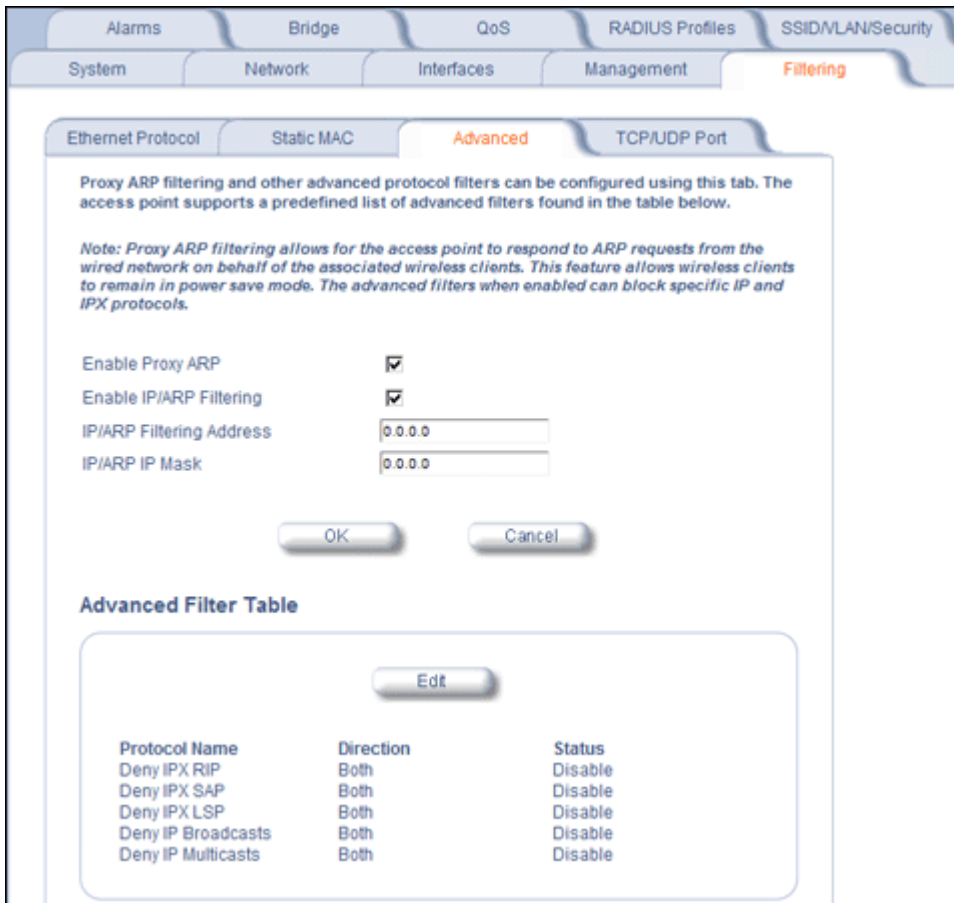


Figure 4-28 Advanced Filter Configuration

The following protocols are listed in the Advanced Filter Table:

- **Deny IPX RIP**
- **Deny IPX SAP**
- **Deny IPX LSP**
- **Deny IP Broadcasts**
- **Deny IP Multicasts**

The AP can filter these protocols in the wireless-to-Ethernet direction, the Ethernet-to-wireless direction, or in both directions. Click **Edit** and use the **Status** field to Enable or Disable the filter.

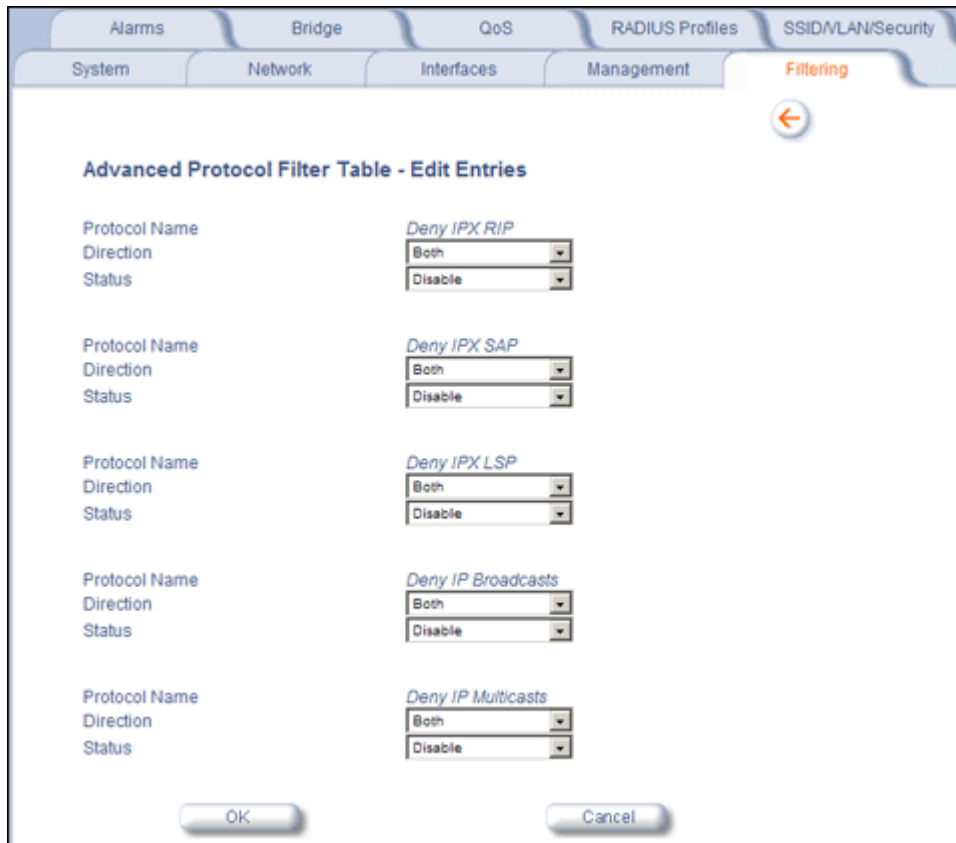


Figure 4-29 Static MAC Filter Table - Edit Entries

### TCP/UDP Port

Port-based filtering enables you to control wireless user access to network services by selectively blocking TCP/UDP protocols through the AP. A user specifies a Protocol Name, Port Number, Port Type (TCP, UDP, or TCP/UDP), and filtering interfaces (Wireless only, Ethernet only, a combination of Wireless and Ethernet, or all interfaces) in order to block access to services, such as Telnet and FTP, and traffic, such as NETBIOS and HTTP.

For example, an AP with the following configuration would discard frames received on its Ethernet interface with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets.

Protocol Type (TCP/UDP)	Destination Port Number	Protocol Name	Interface	Status (Enable/Disable)
UDP	137	NETBIOS Name Service	Ethernet	Enable

### Adding TCP/UDP Port Filters

1. Place a check mark in the box labeled **Enable TCP/UDP Port Filtering**.

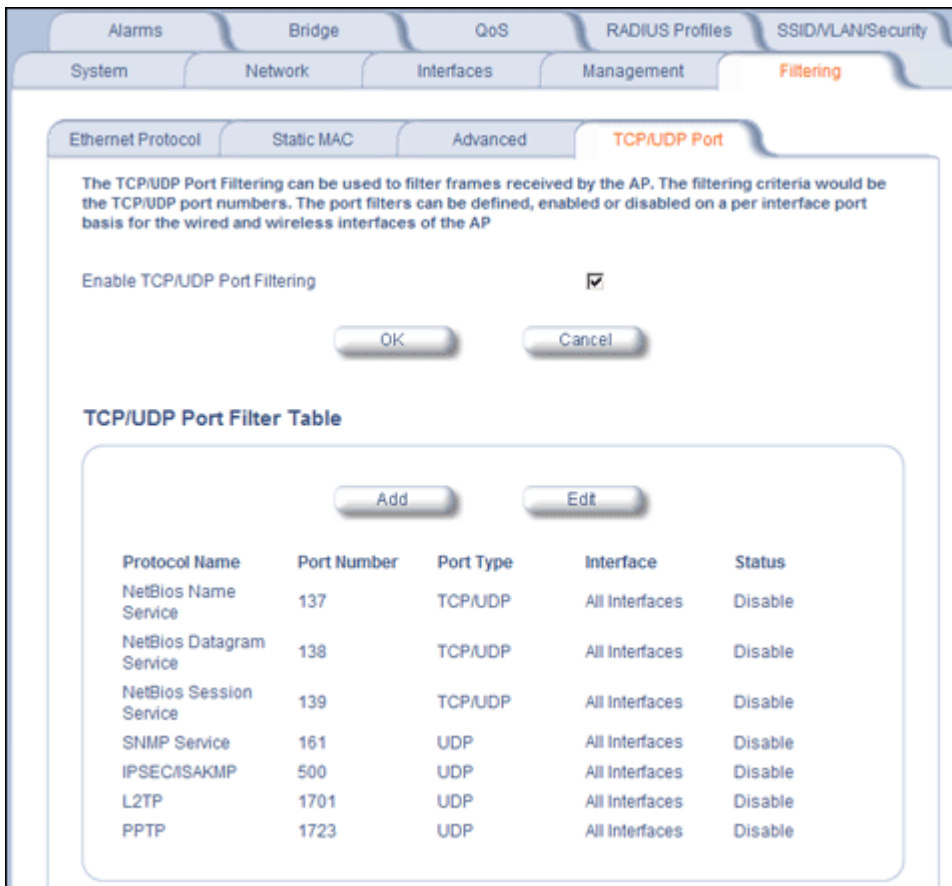


Figure 4-30 TCP/UDP Port Filter Configuration

2. Click **Add** under the **TCP/UDP Port Filter Table** heading.
3. In the **TCP/UDP Port Filter Table**, enter the Protocol Names to filter.
4. Set the destination Port Number (a value between 1 and 65535) to filter. See the IANA Web site at <http://www.iana.org/assignments/port-numbers> for a list of assigned port numbers and their descriptions.
5. Set the Port Type for the protocol: **TCP**, **UDP**, or both (**TCP/UDP**).
6. Set the **Interface** to filter:
  - Only Ethernet
  - Only Wireless
  - All interfaces
7. Click **OK**.



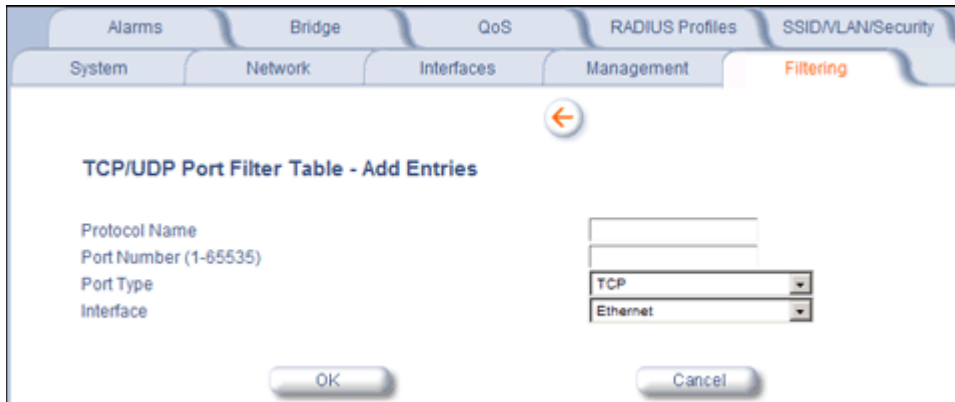


Figure 4-31 TCP/UDP Port Filter Table - Add Entries

### Editing TCP/UDP Port Filters

1. Click **Edit** under the *TCP/UDP Port Filter Table* heading.
2. Make any changes to the Protocol Name or Port Number for a specific entry, if necessary.
3. In the row that defines the port, set the **Status** to **Enable**, **Disable**, or **Delete**, as appropriate.
4. Select **OK**.

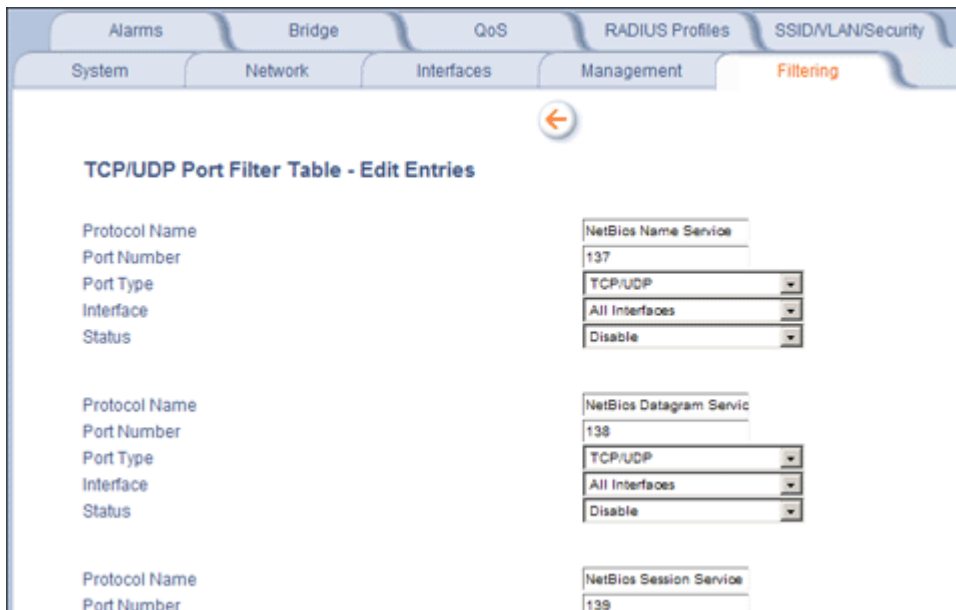


Figure 4-32 TCP/UDP Port Filter Table - Edit Entries

## Alarms

The Alarms tab has the following sub-tabs:

- [Groups](#)
- [Alarm Host Table](#)
- [Syslog](#)
- [Rogue Scan](#)

## Groups

Alarm groups can be enabled or disabled via the Web interface. Place a check mark in the box provided to enable a specific group. Remove the check mark from the box to disable the alarms. Alarm severity levels are as follows:

- **Critical alarms** will often result in severe disruption in network activity or an automatic reboot of the AP.
- **Major alarms** are usually activated due to a breach in the security of the system. Clients cannot be authenticated because an attempt at unauthorized access into the AP has been detected.
- **Informational alarms** provide the network administrator with some general information about the activities the AP is performing.

### Configuration Trap Group

Trap Name	Description	Severity Level
oriTrapDNSIPNotConfigured	DNS IP address not configured	Major
oriTrapRADIUSAuthenticationNotConfigured	RADIUS Authentication not configured	Major
oriTrapRADIUSAccountingNotConfigured	RADIUS Accounting not configured	Major
oriTrapDuplicateIPAddressEncountered	Another network device with the same IP address exists	Major
oriTrapDHCPRelayServerTableNotConfigured	The DHCP relay agent server table is empty or not configured	Major
oriTrapVLANIDInvalidConfiguration	A VLAN ID configuration is invalid	Major
oriTrapAutoConfigFailure	Auto configuration failed	Minor
oriTrapBatchExecFailure	The CLI Batch execution fails for the following reasons: <ul style="list-style-type: none"> <li>• Illegal Command is parsed in the CLI Batch file</li> <li>• Execution error is encountered while executing CLI Batch file</li> <li>• Bigger file size than 100 Kbytes</li> </ul>	Minor
oriTrapBatchFileExecStart	The CLI Batch execution begins after file is uploaded	Minor
oriTrapBatchFileExecEnd	The execution of CLI Batch file ends.	Minor

### Security Trap Group

Trap Name	Description	Severity Level
oriTrapInvalidEncryptionKey	Invalid encryption key has been detected.	Critical

Trap Name	Description	Severity Level
oriTrapAuthenticationFailure	Client authentication failure has occurred. Authentication failures can range from: <ul style="list-style-type: none"> <li>• MAC Access Control table</li> <li>• RADIUS MAC authentication</li> <li>• 802.1x authentication specifying the EAP-Type</li> <li>• WORP mutual authentication</li> <li>• SSID authorization failure specifying the SSID</li> <li>• VLAN ID authorization failure specifying the VLAN ID</li> </ul>	Major
oriTrapUnauthorizedManagerDetected	Unauthorized manager has attempted to view and/or modify parameters	Major
oriTrapRADScanComplete	RAD scan is successfully completed	Informational
oriTrapRADScanResults	Provides information on the RAD Scan results	Informational
oriTrapRogueScanStationDetected	Rogue station detected	Informational
oriTrapRogueScanCycleComplete	Rogue scan successfully completed	Informational

**Wireless Interface/Card Trap Group**

Trap Name	Description	Severity Level
oriTrapWLCFailure	General failure wireless interface/card failure.	Critical
oriTrapWLCRadarInterferenceDetected	Radar interference detected on the channel being used by the wireless interface	Major
MIC Attack Detected	Supported in Web interface only	Major
MIC Attack Report Detected	Supported in Web interface only	Major

**Operational Trap Group**

Trap Name	Description	Severity Level
oriTrapUnrecoverableSoftwareErrorDetected	Unrecoverable software error detected. Causes software watch dog timer to expire, which in turn causes the device to reboot.	Critical
oriTrapRADIUServerNotResponding	RADIUS server not responding to authentication requests sent from the RADIUS client in the device	Major
oriTrapModuleNotInitialized	Module (hardware or software) not initialized	Major
oriTrapDeviceRebooting	Device rebooting	Informational
oriTrapTaskSuspended	Task suspended	Critical
oriTrapBootPFailed	Response to the BootP request not received; device not dynamically assigned an IP address	Major

## Alarms

Trap Name	Description	Severity Level
oriTrapDHCPFailed	Response to the DHCP client request not received; device not dynamically assigned an IP address	Major
oriTrapDNSClientLookupFailure	DNS client attempts to resolve a specified hostname (DNS lookup) and a failure occurs because either the DNS server is unreachable or there is an error for the hostname lookup. Trap specifies the hostname that was being resolved.	Major
oriTrapSSLInitializationFailure	SSL initialization failure	Major
oriTrapWirelessServiceShutdown	Wireless interface has shutdown services for wireless clients	Informational
oriTrapWirelessServiceResumed	Wireless interface has resumed service and is ready for wireless client connections	Informational
oriTrapSSHInitializationStatus	SSH initialization status	Major
oriTrapVLANIDUserAssignment	User is assigned a VLAN ID from the RADIUS server	Informational
oriTrapDHCPLeaseRenewal	AP requests DHCP renewal and receives new information from the DHCP server. Information includes the DHCP server IP address that replied to the DHCP client request, and the IP address, subnet mask, and gateway IP address returned from the DHCP server.	Informational
oriTrapTemperatureAlert	Temperature is above or below acceptable operating margin. Temperature is within 5°C of upper or lower limit.	Critical Major

## Flash Memory Trap Group

Trap Name	Description	Severity Level
oriTrapFlashMemoryEmpty	No data present in flash memory	Informational
Flash Memory Corrupted	Flash memory corrupted	Critical
oriTrapFlashMemoryRestoringLastKnownGoodConfiguration	Current/original configuration data file is found to be corrupted, and the device loads the last known good configuration file	Informational

## TFTP Trap Group

Trap Name	Description	Severity Level
oriTrapTFTPFailedOperation	TFTP operation failed	Major
oriTrapTFTPOperationInitiated	TFTP operation Initiated	Informational
oriTrapTFTPOperationCompleted	TFTP operation completed	Informational

## Image Trap Group

Trap Name	Description	Severity Level
oriTrapZeroSizeImage	Zero size image loaded onto device	Major

Trap Name	Description	Severity Level
oriTrapInvalidImage	Invalid image loaded onto device	Major
oriTrapImageTooLarge	Image loaded on the device exceeds the size limitation of flash	Major
oriTrapIncompatibleImage	Incompatible image loaded onto device	Major
oriTrapInvalidImageDigitalSignature	Image with invalid digital signature is loaded onto device	Major

**SNTP Trap Group**

Trap Name	Description	Severity Level
oriTrapSNTPFailure	SNTP time retrieval failure	Minor
oriTrapSNTPFailure	SNTP sync-up failure	Minor

In addition, the AP supports these standard traps, which are always enabled:

**RFC 1215-Trap**

Trap Name	Description	Severity Level
coldStart	AP is on or rebooted	Informational
linkUp	AP's Ethernet interface link is up (working)	Informational
linkDown	AP's Ethernet interface link is down (not working)	Informational

**Bridge MIB (RFC 1493) Alarms**

Trap Name	Description	Severity Level
New Root	AP has become the new root in the Spanning Tree network	Informational
topologyChange	Trap is not sent if a newRoot trap is sent for the same transition	Informational

All these alarm groups correspond to System Alarms that are displayed in the [System Status Screen](#), including the traps that are sent by the AP to the SNMP managers specified in the [Alarm Host Table](#).

**Alarm Host Table**

To add an entry and enable the AP to send SNMP trap messages to a Trap Host, click **Add**, and then specify the IP Address and Password for the Trap Host.

**NOTE:** Up to 10 entries are possible in the Alarm Host table.

- **IP Address:** Enter the Trap Host IP Address.
- **Password:** Enter the password in the **Password** field and the **Confirm** field.
- **Comment:** Enter an optional comment, such as the alarm (trap) host station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

## Syslog

The Syslog messaging system enables the AP to transmit event messages to a central server for monitoring and troubleshooting. The access point logs “Session Start (Log-in)” and “Session Stop (Log-out)” events for each wireless client as an alternative to RADIUS accounting.

See RFC 3164 at <http://www.rfc-editor.org> for more information on the Syslog standard.

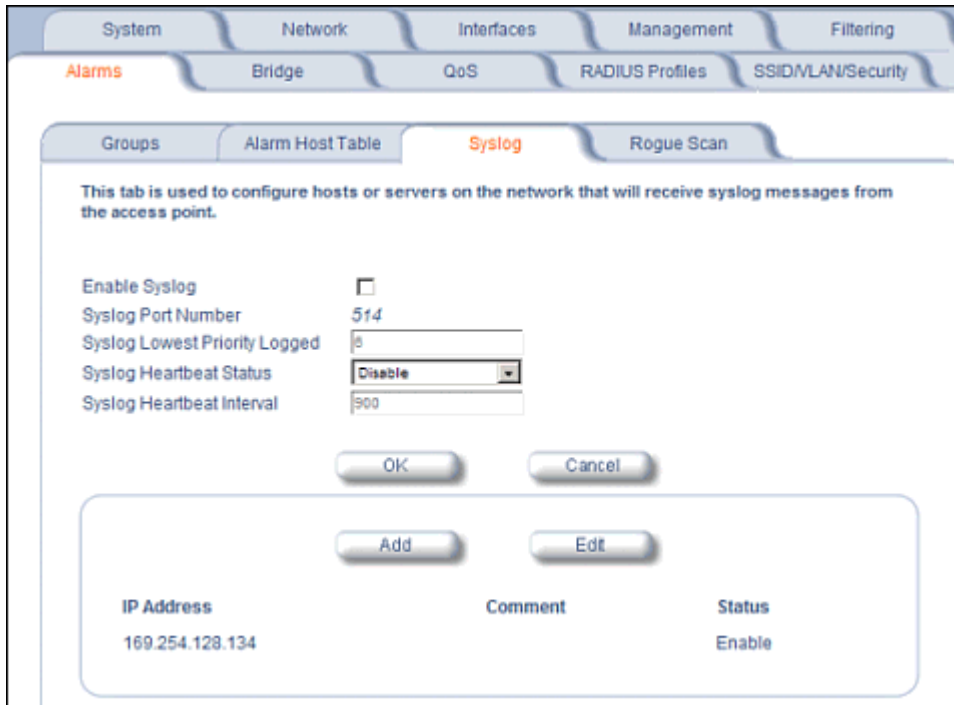


Figure 4-33 Syslog Configuration Screen

### Setting Syslog Event Notifications

Syslog Events are logged according to the level of detail specified by the administrator. Logging only urgent system messages will create a far smaller, more easily read log than a log of every event the system encounters. Determine which events to log by selecting a priority defined by the following scale:

Event	Priority	Description
LOG_EMERG	0	System is unusable
LOG_ALERT	1	Action must be taken immediately
LOG_CRIT	2	Critical conditions
LOG_ERR	3	Error conditions
LOG_WARNING	4	Warning conditions
LOG_NOTICE	5	Normal but significant condition
LOG_INFO	6	Informational
LOG_DEBUG	7	Debug-level messages

### Configuring Syslog Event Notifications

You can configure the following Syslog settings from the HTTP interface:

- **Enable Syslog:** Place a check mark in the box provided to enable system logging.
- **Syslog Port Number:** This field is read-only and displays the port number (514) assigned for system logging.

## Alarms

- **Syslog Lowest Priority Logged:** The AP will send event messages to the Syslog server that correspond to the selected priority number and any priority numbers below it. For example, if set to 6, the AP will transmit event messages labeled priority 1 to 6 to the Syslog server. This parameter supports a range between 1 and 7; 6 is the default.
- **Syslog Heartbeat Status:** When Heartbeat is enabled, the AP periodically sends a message to the Syslog server to indicate that it is active.
- **Syslog Heartbeat Interval:** If Syslog Heartbeat Status is enabled this field provides the interval for the heartbeat in seconds (between 1 and 604800). The default is 900 seconds.
- **Syslog Host Table:** This table specifies the IP addresses of a network servers that the AP will send Syslog messages to. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  - **IP Address:** Enter the IP Address for the management host.
  - **Comment:** Enter an optional comment such as the host name.
  - **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field's value.

## Syslog Messages

The following messages are supported in the AP:

Syslog Message Name	Priority	Severity	Description
Auto Configuration using DHCP	6	Informational	Configuration filename and TFTP server address are obtained from DHCP when dynamic IP is configured on the device.
Auto Configuration using Static IP	6	Informational	Configured TFTP server address and configuration filename is used when Static IP is configured on the device.
TFTP Server IP and configuration filename not present in DHCP response	4	Minor	Configuration filename and/or TFTP server address is not present in the DHCP response when using DHCP.
TFTP Server IP Address used in AutoConfig feature	6	Informational	TFTP server IP address used for AutoConfig.
TFTP Server filename used in AutoConfig feature	6	Informational	TFTP filename used for AutoConfig.
Auto Configuration TFTP Download Failure	4	Minor	TFTP download of a configuration file for AutoConfig fails for the following reasons: <ul style="list-style-type: none"> <li>• Incorrect or non-reachable TFTP server address</li> <li>• Incorrect or unavailable configuration filename</li> <li>• TFTP transfer timeout.</li> </ul>
Image Compatibility Check, Invalid Image	2	Major	One of the following failures occurs: <ul style="list-style-type: none"> <li>• Invalid Signature</li> <li>• Zero File Size</li> <li>• Large File</li> <li>• Non VxWork Image</li> <li>• Incompatible Image</li> </ul>
AP Heartbeat Status	5	Informational	AP syslog keep alive message.

Syslog Message Name	Priority	Severity	Description
Client Login Authentication Status	6	Informational	<p>Client logs in/authenticates. Message includes:</p> <ul style="list-style-type: none"> <li>Client MAC Address</li> <li>Authentication Type = None, ACL, RADIUS MAC, 802.1X</li> <li>Cipher Type = None, WEP, TKIP, AES</li> <li>Status = Allow, Deny</li> <li>SSID to which client is connecting</li> </ul> <p>Sample Message: &lt;client mac address&gt;   Status = &lt;value&gt;   SSID = &lt;value&gt;   Auth Type = &lt;value&gt;   Cipher Type = &lt;value&gt;</p>
Client De-Authentication Status	6	Informational	<p>Client de-authenticates. Message includes:</p> <ul style="list-style-type: none"> <li>Client MAC Address</li> <li>Cipher Type = None, WEP, TKIP, AES</li> <li>Status = De-authentication reason, which can be any of the following: <ul style="list-style-type: none"> <li>Unknown reason</li> <li>Stale authentication information</li> <li>Authenticated STA leaving BSS</li> <li>Inactivity</li> <li>Association error</li> <li>Class 2 frame received from non-authenticated STA</li> <li>Class 3 frame received from non-associated STA</li> <li>Associated STA leaving BSS</li> <li>STA requesting information, but not yet authenticated</li> <li>Enhanced security (RSN) required</li> <li>Enhanced security (RSN) used inconsistently</li> <li>Invalid Information Element</li> <li>MIC Failure</li> <li>WPA module de-auth</li> </ul> </li> <li>SSID to which client was connected</li> </ul> <p>Sample Message: &lt;client mac address&gt;   Status = &lt;value&gt;   SSID = &lt;value&gt;   Cipher Type = &lt;value&gt;</p>
RADIUS Accounting Start and Stop Messages	6	Informational	Start and Stop accounting messages for wireless clients.
CLI Configuration File Start Execution	6	Informational	CLI configuration file execution starts.
CLI Configuration File End Execution	6	Informational	CLI configuration file execution ends.

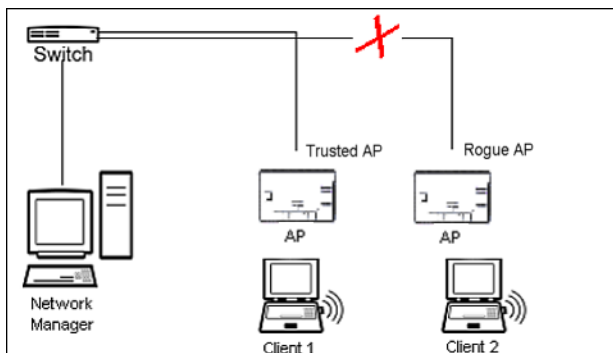


Syslog Message Name	Priority	Severity	Description
CLI Configuration File Execution Errors	4	Minor	There is an error in execution of the CLI configuration file. The message specifies the filename, line number, and error reason.
SSH Initialization Failure	3	Major	One of the following failures occurs: Keys not present Keys cannot be generated Internal error (no available resources)
SSH Key Generation Successful	6	Informational	SSH Key generation is successful.
Wireless Service Shutdown	6	Informational	Wireless service is shutdown.
Wireless Service Resume	6	Informational	Wireless service resumes.
MIC Attack Occurred	4	Minor	MIC attack occurred; wireless interface is shut down for 60 seconds
MIC Attack from Wireless Station	4	Minor	A MIC attack is detected from a wireless station.
SNTP Time Retrieval Failure	4	Minor	SNTP Client in the AP fails to retrieve time information from the configured SNTP servers. Also included in message: IP Address of SNTP server.
SNTP Time Sync-Up Failure	4	Minor	SNTP Client in the AP fails to synchronize the time with the SNTP server it was communicating with. Also included in message: IP Address of SNTP server.

## Rogue Scan

The Rogue Scan feature provides an additional security level for wireless LAN deployments. Rogue Scan uses the selected wireless interface(s) for scanning its coverage area for Access Points and clients.

A centralized *Network Manager* receives MAC address information from the AP on all wireless clients detected by the AP. The Network Manager then queries all wired switches to find out the inbound switch/port of these wireless clients. If the switch/port does not have a valid Access Point connected to it as per a pre-configured database, the Network Manager proceeds to block that switch/port and prevent the Rogue AP from connecting to the wired network.



**Figure 4-34 Preventing Rogue AP Attacks**

The figure above shows Client 1 connected to a Trusted AP and Client 2 connected to a Rogue AP. The Trusted AP scans the networks, detects Client 2, and notifies the Network Manager. The Network Manager uses SNMP/CLI to query the wired switch to find the inbound switch port of Client 2's packets. The Network Manager verifies that this switch/router

and port does not have a valid Access Point as per the administrator's database. Thus it labels Client 2's AP as a Rogue AP and proceeds to prevent the Rogue AP attack by blocking this switch's port.

APs can be detected either by active scanning using 802.11 probe request frames or passively by detecting periodic beacons, or both. Wireless clients are detected by monitoring 802.11 connection establishment messages such as association/authentication messages or data traffic to or from the wireless clients.

There are two scanning modes available per wireless interface: continuous scanning mode and background scanning mode.

### Continuous Scanning Mode

The continuous scanning mode is a dedicated scanning mode where the wireless interface performs scanning alone and does not perform the normal AP operation of servicing client traffic.

In continuous scanning mode the AP scans each channel for a channel scan time of one second and then moves to the next channel in the scan channel list. With a channel scan time of one second, the scan cycle time will take less than a minute (one second per channel). Once the entire scan channel list has been scanned the AP restarts scanning from the beginning of the scan channel list.

### Background Scanning Mode

In background scanning mode the AP performs background scanning while performing normal AP operations on the wireless interface.

You can configure the **scan cycle time** between 1-1440 minutes (24 hours). The scan cycle time indicates how frequently a channel is sampled and defines the minimum attack period that can go unnoticed.

In background scanning mode the AP will scan one channel then wait for a time known as channel scan time. The channel scan time affects the amount of data collected during scanning and defines the maximum number of samples (possible detections) in one scan. This is increased to improve scanning efficiency; the tradeoff is that it decreases throughput. The optimum value for this parameter during background scanning mode is 20ms. The channel scan time is calculated from the scan cycle time parameter and the number of channels in the scan channel list as follows:

$\text{intra-channel scan time} = (\text{scan cycle time} - (\text{channel scan time} * \text{number of channels in the scan list})) / \text{number of channels in the scan list}$ .

### Rogue Scan Data Collection

The AP stores information gathered about detected stations during scanning in a Rogue Scan result table. The Rogue Scan result table can store a maximum of 2000 entries. When the table fills, the oldest entry gets overwritten. The Rogue Scan result table lists the following information about each detected station:

- Station Type: indicates one of the following types of station:
  - Unknown station
  - AP station
  - Infrastructure Client Station
  - IBSS Client Station
- MAC Address of the detected station
- Channel: the working channel of the detected station
- SNR: the SNR value of the last frame from the station as received by the AP
- BSSID: the BSSID field stores the:
  - MAC address of the associated Access Point in the case of a client.
  - Zero MAC address or MAC address of the partner Access Point if the AP is a partner of a WDS link

The AP ages out older entries in the Rogue Scan result table if a detected station is inactive for more than the Scan Result Table Ageing Time.

### Rogue Scan

Perform this procedure to enable Rogue Scan and define the Scan Interval and Scan Interface. See [Figure 4-35](#).

The Rogue Scan screen also displays the number of new access points and clients detected in the last scan on each wireless interface.

1. Enable the Security Alarm Group. Select the Security Alarm Group link from the Rogue Scan screen. Configure a Trap Host to receive the list of access points (and clients) detected during the scan.
2. Click **Configure > Alarms > Rogue Scan**.
3. Enable Rogue Scan by checking **Enable Rogue Scan**.

**NOTE:** *Rogue Scan cannot be enabled on a wireless interface when the Wireless Service Status on that interface is shutdown. First, resume service on the wireless interface.*

**NOTE:** *Enabling Rogue Scan simultaneously with Broadcast Unique Beacon will cause a drift in the beacon interval and the occasional missing of beacons.*

4. Enter the **Scan Mode**. Select Background Scanning or Continuous Scanning. In Continuous Scanning mode the AP stops normal operation and scans continuously on that interface. In Background Scanning mode, the AP performs background scanning while doing normal AP operation on that interface.
5. If the Scan Mode is Background Scanning, then enter the **Scan Interval**.
  - The Scan Interval specifies the time period in minutes between scans in Background Scanning mode and can be set to any value between 1 and 1440 minutes.
6. Configure the **Scan Result Table Ageing Time**. The AP ages out older entries in the Rogue Scan result table if a detected station is inactive for more than this time. The valid range is from 60-7200 minutes, the default is 60 minutes.
7. Configure the **Scan Results Trap Notification Mode** to control the notification behavior when APs or stations are detected in a scan:
  - No Notification
  - Notify AP
  - Notify Client
  - Notify All (Notify both AP and Client detection)
8. Configure the **Scan Results Trap Report Style** to control the way detected stations are reported in the notification:
  - Report all detected stations since last scan (default)
  - Report all detected stations since start of scan
9. Click **OK**.

The results of the Rogue Scan can be viewed in the **Status** page in the HTTP interface.

The screenshot shows a web-based configuration interface for an AP-700. At the top, there are navigation tabs: System, Network, Interfaces, Management, and Filtering. Below these, a sub-menu is open with tabs for Alarms, Bridge, QoS, RADIUS Profiles, and SSID/LAN/Security. The 'Alarms' tab is selected, and within it, the 'Rogue Scan' sub-tab is active. The main content area contains a detailed explanation of Rogue Scan functionality, two notes, and configuration fields for two wireless interfaces (A and B). The 'Scan Mode' for both is set to 'Background', and the 'Scan Interval' is set to '1' minute. The 'Enable Rogue Scan' checkboxes are unchecked. The 'Number of New Stations detected in last scan' is 0 for both. The 'Scan Result Table' ageing time is set to '60' minutes. The 'Scan Result Notification' section has 'Scan results trap notification mode' set to 'Notify All' and 'Scan results trap report style' set to 'Report Since Last Scan'. At the bottom, there are 'OK' and 'Cancel' buttons.

System   Network   Interfaces   Management   Filtering

Alarms   Bridge   QoS   RADIUS Profiles   SSID/LAN/Security

Groups   Alarm Host Table   Syslog   **Rogue Scan**

Rogue Scan uses the selected wireless interface for scanning its coverage area for Access Points and Clients. To dedicate the AP's wireless interface to scanning set the scan mode to continuous scan. Note that while the wireless interface is in continuous scan mode it does not perform normal AP operations. To enable the AP's wireless interface to scan in the background while still performing normal AP operations, set the scan cycle time in minutes and set the scan mode to background scanning mode. Note that AP throughput decreases with an increase in scanning efficiency.

*Note1: When Rogue Scan is enabled, the [Security Alarm Group](#) must also be enabled and a [Trap Host](#) configured to receive the list of access points and clients detected during the scan.*

*Note2: The scan parameter scan interval time can only be modified for background scanning mode.*

**Wireless - A**  
Scan Mode: Background  
Scan Interval (1-1440 minutes): 1  
Enable Rogue Scan:   
Number of New Stations detected in last scan: 0

**Wireless - B**  
Scan Mode: Background  
Scan Interval (1-1440 minutes): 1  
Enable Rogue Scan:   
Number of New Stations detected in last scan: 0

**Scan Result Table**  
Ageing time (60-7200 minutes): 60

**Scan Result Notification**  
Scan results trap notification mode: Notify All  
Scan results trap report style: Report Since Last Scan

OK   Cancel

Figure 4-35 Rogue Scan Screen

## Bridge

The AP is a bridge between your wired and wireless networking devices. As a bridge, the functions performed by the AP include:

- MAC address learning
- Forward and filtering decision making
- Spanning Tree protocol used for loop avoidance

Once the AP is connected to your network, it learns which devices are connected to it and records their MAC addresses in the Learn Table. The table can hold up to 10,000 entries. To view the Learn Table, click on the **Monitor** button in the web interface and select the [Learn Table](#) tab.

The **Bridge** tab has four sub-tabs:

- [Spanning Tree](#)
- [Intra BSS](#)
- [Packet Forwarding](#)

## Spanning Tree

A Spanning Tree is used to avoid redundant communication loops in networks with multiple bridging devices. Bridges do not have any inherent mechanism to avoid loops, because having redundant systems is a necessity in certain networks. However, redundant systems can cause Broadcast Storms, multiple frame copies, and MAC address table instability problems.

Complex network structures can create multiple loops within a network. The Spanning Tree configuration blocks certain ports on AP devices to control the path of communication within the network, avoiding loops and following a spanning tree structure.

For more information on Spanning Tree protocol, please see Section 8.0 of the IEEE 802.1d standard. The Spanning Tree configuration options are advanced settings. Proxim recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

**NOTE:** *Spanning Tree protocol is disabled by default. When WDS is enabled, Spanning Tree protocol is automatically enabled. It may be manually disabled. If Spanning Tree protocol is enabled by WDS and WDS is subsequently disabled, Spanning tree will remain enabled until it is manually disabled.*

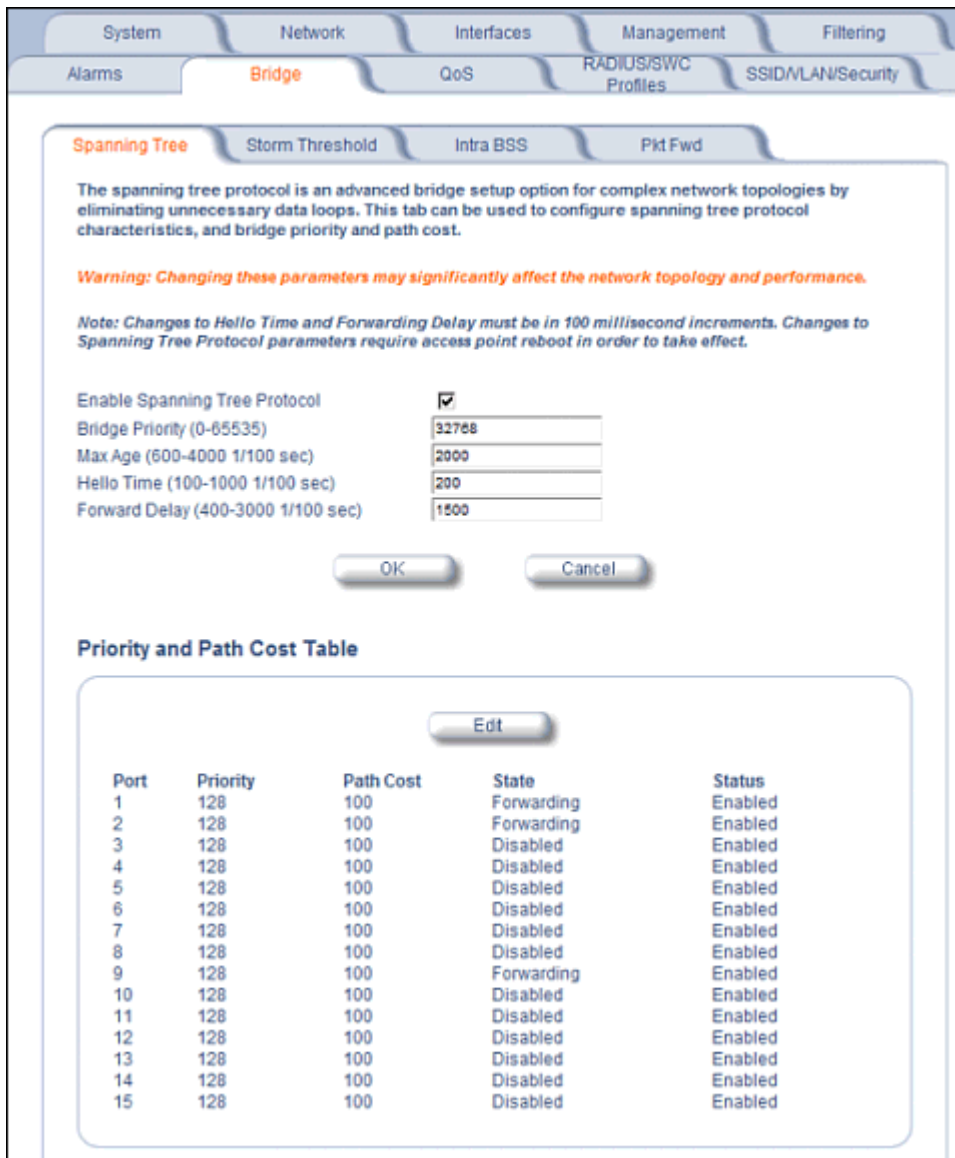


Figure 4-36 Spanning Tree Sub-Tab

## Storm Threshold

Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- Specifying an absolute maximum number of messages per interface.

The Storm Threshold parameters allow you to specify a set of thresholds for each interface of the AP, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for an interface or from a single network device exceeds the maximum value per second, the AP will ignore all subsequent messages in that second received on that interface or from that network device.

- **Address Threshold:** Enter the maximum allowed number of packets per second.
- **Ethernet Threshold:** Enter the maximum allowed number of packets per second.

- **Wireless Threshold:** Enter the maximum allowed number of packets per second.

## Intra BSS

The wireless clients (or *subscribers*) that associate with a certain AP form the Basic Service Set (BSS) of a network infrastructure. By default, wireless subscribers in the same BSS can communicate with each other. However, some administrators (such as wireless public spaces) may wish to block traffic between wireless subscribers that are associated with the same AP to prevent unauthorized communication and to conserve bandwidth. This feature enables you to prevent wireless subscribers within a BSS from exchanging traffic.

Although this feature is generally enabled in public access environments, Enterprise LAN administrators use it to conserve wireless bandwidth by limiting communication between wireless clients. For example, this feature prevents peer-to-peer file sharing or gaming over the wireless network.

To block Intra BSS traffic, set **Intra BSS Traffic Operation** to **Block**.

To allow Intra BSS traffic, set **Intra BSS Traffic Operation** to **Passthru**.

## Packet Forwarding

The Packet Forwarding feature enables you to redirect traffic generated by wireless clients that are all associated to the same AP to a single MAC address. This filters wireless traffic without burdening the AP and provides additional security by limiting potential destinations or by routing the traffic directly to a firewall. You can redirect to a specific port (Ethernet or WDS) or allow the bridge's learning process (and the forwarding table entry for the selected MAC address) to determine the optimal port.

**NOTE:** *The gateway to which traffic will be redirected should be node on the Ethernet network. It should not be a wireless client.*

### Configuring Interfaces for Packet Forwarding

Configure your AP to forward packets by specifying port(s) to which packets are redirected and a destination MAC address.

1. Within the **Packet Forwarding Configuration** screen, check the box labeled **Enable Packet Forwarding**.
2. Specify a destination **Packet Forwarding MAC Address**. The AP will redirect all unicast, multicast, and broadcast packets received from wireless clients to the address you specify.
3. Select a **Packet Forwarding Interface Port** from the drop-down menu. You can redirect traffic to:
  - Ethernet
  - A WDS connection (see [Wireless Distribution System \(WDS\)](#) for details)
  - Any (traffic is redirected to a port based on the bridge learning process)
4. Click **OK** to save your changes.

## QoS

### Wi-Fi Multimedia (WMM)/Quality of Service (QoS) Introduction

The AP supports Wi-Fi Multimedia (WMM), which is a solution for QoS functionality based on the IEEE 802.11e specification. WMM defines enhancements to the MAC for wireless LAN applications with Quality of Service requirements, which include transport of voice traffic over IEEE 802.11 wireless LANs.

The enhancement are in the form of changes in protocol frame formats (addition of new fields and information elements), addition of new messages, definition of new protocol actions, channel access mechanisms (differentiated control of access to medium) and network elements (QoS/WME aware APs, STAs), and configuration management.

WME supports Enhanced Distributed Channel Access (EDCA) for prioritized QoS services. The WME/QoS feature can be enabled or disabled per wireless interface. For more information on QoS, see “Technical Bulletin 69504 Revision 2” at [http://keygen.proxim.com/support/orinoco/tb/tb69504\\_3wmm.pdf](http://keygen.proxim.com/support/orinoco/tb/tb69504_3wmm.pdf).

### Policy

Perform the following procedure to enable QoS and add QoS policies:

1. Click **Configure > QoS > Policy**.

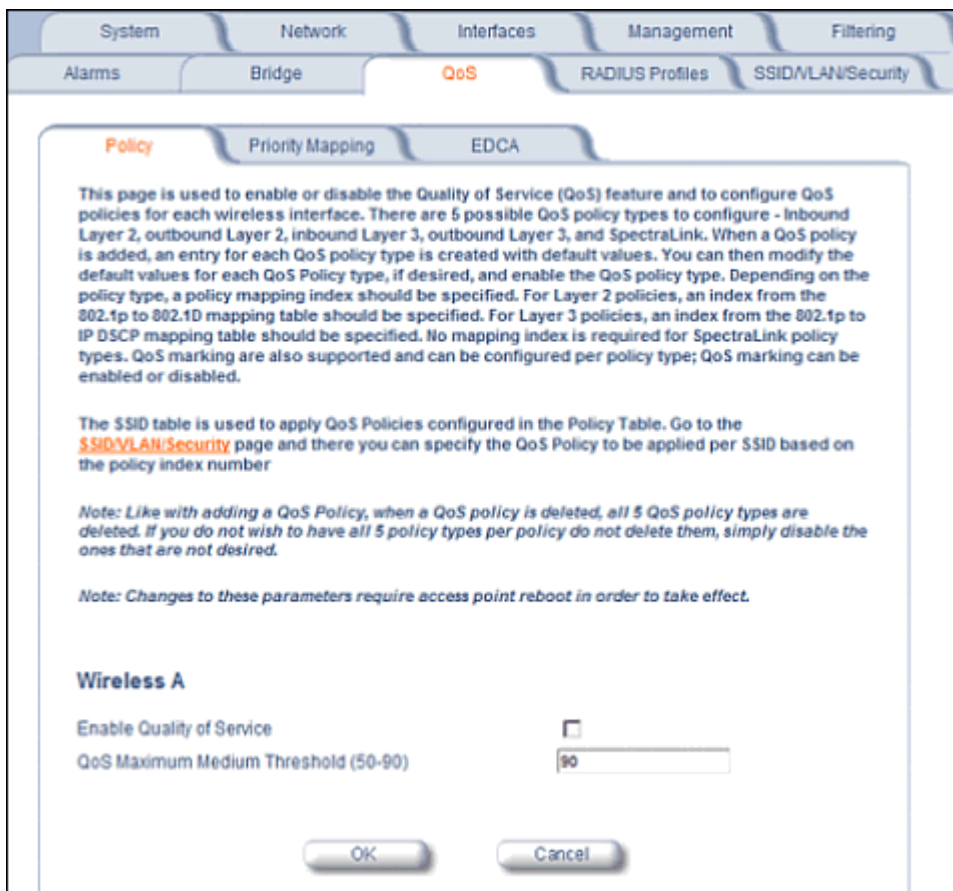


Figure 4-37 QoS Policy Sub-Tab

2. To enable QoS, check the **Enable Quality of Service** checkbox.
3. Configure the **QoS Maximum Medium Threshold** for all Admission Controls. Admission will be granted if the new requested traffic stream and already admitted time is less than the *medium maximum threshold*.



- To add a QoS Policy, click the **Add** button in the “QoS Policies Table” box. The Add Entries box appears.

**QoS Policies Table - Add Entries**

This page is used to create QoS Policies. By default when adding a QoS policy, all 5 QoS policy types are added. For Layer 2 policies, a priority mapping index from the 802.1p to 802.1d mapping table should be specified. For Layer 3 policies, a priority mapping index from the 802.1p to IP DSCP mapping table should be specified. No priority mapping index is needed for SpectraLink QoS policy types. You can also enable or disable QoS marking on each policy type and enable or disable the different types.

*Note: Changes to these parameters require access point reboot in order to take effect.*

Policy Name	<input type="text"/>
Policy Type	<i>inboundLayer2</i>
Priority Mapping Index	<input type="text"/>
Enable QoS Marking	<input type="checkbox"/>
Policy Name	<input type="text"/>
Policy Type	<i>inboundLayer3</i>
Priority Mapping Index	<input type="text"/>
Enable QoS Marking	<input type="checkbox"/>
Policy Name	<input type="text"/>
Policy Type	<i>outboundLayer2</i>
Priority Mapping Index	<input type="text"/>
Enable QoS Marking	<input type="checkbox"/>
Policy Name	<input type="text"/>
Policy Type	<i>outboundLayer3</i>
Priority Mapping Index	<input type="text"/>
Enable QoS Marking	<input type="checkbox"/>
Policy Name	<input type="text"/>
Policy Type	<i>spectralink</i>
Priority Mapping Index	<input type="text"/>
Enable QoS Marking	<input type="checkbox"/>

OK Cancel

**Figure 4-38 Add QoS Policy**

- Enter the **Policy Name**.
- Select the **Policy Type**:
  - inlayer2**: inbound traffic direction, Layer 2 traffic type
  - inlayer3**: inbound traffic direction, Layer 3 traffic type
  - outlayer2**: outbound traffic direction, Layer 2 traffic type
  - outlayer3**: inbound traffic direction, Layer 3 traffic type
  - spectralink**: SpectraLink traffic
- Enter the **Priority Mapping Index**.  
For layer 2 policies, an index from the 802.1p to 802.1d mapping table should be specified. For layer 3 policies, an index from the 802.1p to IP DSCP mapping table should be specified. No mapping index is required for SpectraLink.
- Select whether to **Enable QoS Marking**.
- Click **OK**.

## Priority Mapping

Use this page to configure QoS 802.1p to 802.1d priority mappings (for layer 2 policies) and IP DSCP to 802.1d priority mappings (for layer 3 policies). The first entry in each table contains the recommended priority mappings. Custom entries can be added to each table with different priority mappings.

1. Click **Configure > QoS > Priority Mapping**.

This page is used to configure QoS 802.1D to 802.1p priority mappings and 802.1D To IP DSCP priority mappings. The first entry in each table contains the recommended priority mappings and cannot be deleted. Custom entries can be added to each table with different priority mappings.

### 802.1D to 802.1p Priority Mapping Table

Index	802.1D Priority	802.1p Priority	Status
1	0	0	Enable
1	1	1	Enable
1	2	2	Enable
1	3	3	Enable
1	4	4	Enable
1	5	5	Enable
1	6	6	Enable
1	7	7	Enable

### 802.1D to IP DSCP Priority Mapping Table

Index	802.1D Priority	IP DSCP Range	Status
1	0	0..7	Enable
1	1	8..15	Enable
1	2	16..23	Enable
1	3	24..31	Enable
1	4	32..39	Enable
1	5	40..47	Enable
1	6	48..55	Enable
1	7	56..63	Enable

Figure 4-39 Priority Mapping

2. Click **Add** in the 802.1p and 802.1d priority mapping table.

**QoS 802.1D to 802.1p Mapping Table - Add Entries**

This page is used to add 802.1D to 802.1p mappings. This table contains a one-to-one mapping of 802.1D to 802.1p priorities, so it requires all priorities to be specified. Please enter the desired values for 802.1p priorities and press the Ok button.

802.1D Priority	802.1p Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

OK Cancel

**Figure 4-40 Add Priority Mapping Entry**

3. Select the 802.1p Priority (from 0-7) for 802.1d Priorities 0-7.
4. Click **OK**.
5. Click **Add** in the IP Precedence/DSCP ranges and 802.1d Priority table.
6. Select the IP DSCP Range for each 802.1d Priority.
7. Click **OK**.

**NOTE:** Changes to Priority Mapping require a reboot of the AP to take effect.

## Enhanced Distributed Channel Access (EDCA)

WME uses Enhanced Distributed Channel Access, a prioritized CSMA/CA access mechanism used by WME-enabled clients/AP in a WME enabled BSS to realize different classes of differentiated Channel Access.

A wireless Entity is defined as all wireless clients and APs in the wireless medium contending for the common wireless medium. EDCA uses a separate channel access function for each of the Access Categories (Index) within a wireless entity. Each channel access function in a wireless entity that contends for the wireless medium as if it were a separate client contending for the wireless medium. Different channel access functions in a given Wireless Entity contend among themselves for access to the wireless medium in addition to contending with other clients.

### STA EDCA Table and AP EDCA Table

This page is used to configure the client (STA) and AP Enhanced Distributed Channel Access (EDCA) parameters. You can modify the EDCA values.

The EDCA parameter set provides information needed by the client stations for proper QoS operation during the wireless contention period. These parameters are used by the QoS enabled AP to establish policy, to change policies when accepting new stations or new traffic, or to adapt to changes in the offered load. The EDCA parameters assign priorities to traffic types where higher priority packets gain access to the wireless medium more frequently than lower priority packets.

**NOTE:** Default recommended values for EDCA parameters have been defined; Proxim recommends not modifying EDCA parameters unless strictly necessary.

Perform the following procedure to configure the Station and AP EDCA tables.

1. Click **Configure > QoS > EDCA**.

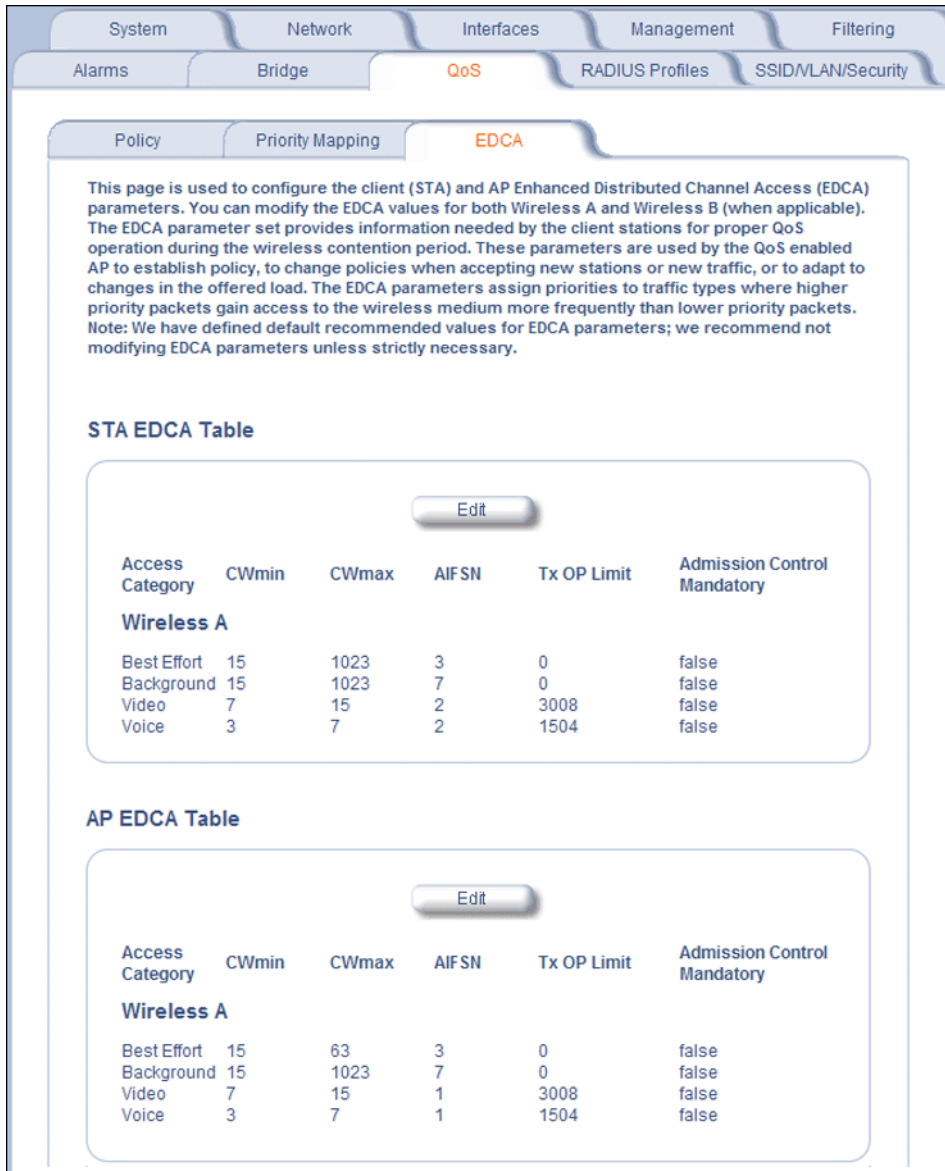


Figure 4-41 EDCA Tables

2. Click **Edit** and configure the following parameters in each table:

**NOTE:** Changes to EDCA parameters require a reboot of the AP to take effect.

- **Index:** read-only. Indicates the index of the Access Category (1-4) being defined:
  - 1 = Best Effort
  - 2 = Background
  - 3 = Video
  - 4 = Voice
- **CWMin:** minimum Contention Window. Configurable range is 0 to 255.
- **CWMax:** maximum Contention Window. Configurable range is 0 to 65535.

- **AIFSN:** Arbitration IFS per access category. Configurable range is 2 to 15.
- **Tx OP Limit:** The Transmission Opportunity Limit. The Tx OP is an interval of time during which a particular QoS enhanced client has the right to initiate a frame exchange sequence onto the wireless medium. The Tx OP Limit defines the upper limit placed on the value of Tx OP a wireless entity can obtain for a particular access category. Configurable range is 0 to 65535.
- **MSDU Lifetime:** specifies the maximum elapsed time between a MSDU transfer request and delivery to the destination, beyond which delivery becomes unnecessary. Configurable range is 0 to 500 seconds.
- **Admission Control Mandatory:** Possible values are True or False. Admission control defines if an Access Point accepts or rejects a requested traffic stream with certain QoS specifications, based on available channel capacity and link conditions. Admission control can be configured for each Access Category (Index).

On the [Policy](#) sub-tab, the user can also configure a *medium maximum threshold* for all Admission Controls. Admission will be granted if the new requested traffic stream and already admitted time is less than the *medium maximum threshold*.

## Radius Profiles

Configuring Radius Profiles on the AP allows the administrator to define a profile for RADIUS Servers used by the system or by a VLAN. The network administrator can define [RADIUS Servers per Authentication Mode and per VLAN](#).

The AP communicates with the RADIUS server defined in a profile to provide the following features:

- [MAC Access Control Via RADIUS Authentication](#)
- [802.1x Authentication using RADIUS](#)
- [RADIUS Accounting](#)

Also, [RADIUS Based Management Access](#) allows centralized user management.

The network administrator can configure default RADIUS authentication servers to be used on a system-wide basis, or in networks with VLANs enabled the administrator can also configure separate authentication servers to be used for MAC authentication, EAP authentication, or Accounting in each VLAN. You can configure the AP to communicate with up to six different RADIUS servers per VLAN/SSID:

- Primary Authentication Server (MAC-based authentication)
- Back-up Authentication Server (MAC-based authentication)
- Primary Authentication Server (EAP/802.1x authentication)
- Back-up Authentication Server (EAP/802.1x authentication)
- Primary Accounting Server
- Back-up Accounting Server

The back-up servers are optional, but when configured, the AP will communicate with the back-up server if the primary server is off-line. After the AP has switched to the backup server, it will periodically check the status of the primary RADIUS server every five (5) minutes. Once the primary RADIUS server is again online, the AP automatically reverts from the backup RADIUS server back to the primary RADIUS server. All subsequent requests are then sent to the primary RADIUS server.

You can view monitoring statistics for each of the configured RADIUS servers.

## RADIUS Servers per Authentication Mode and per VLAN

The user can configure separate RADIUS authentication servers for each authentication mode and for each SSID (VLAN). For example:

- The user can configure separate RADIUS servers for RADIUS MAC authentication and 802.1x authentication
- The user can configure separate RADIUS servers for each VLAN: VLAN1 could support only WEP clients, whereas VLAN2 could support 802.1x and WEP clients.

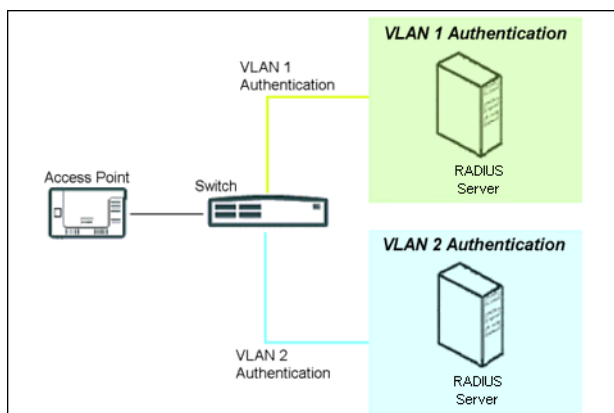


Figure 4-42 RADIUS Servers per VLAN

This figure shows a network with separate authentication servers for each authentication type and for each VLAN. The clients in VLAN 1 are authenticated using the authentication servers configured for VLAN 1. The type of authentication server used depends on whether the authentication is done for an 802.1x client or a non-802.1x client. The clients in VLAN 2 are authenticated using a different set of authentication servers configured for authenticating users in VLAN 2.

Authentication servers for each VLAN are configured as part of the configuration options for that VLAN. RADIUS profiles are independent of VLANs. The user can define any profile to be the default and associate all VLANs to that profile. Four profiles are created by default, “MAC Authentication”, “EAP Authentication”, Accounting”, and “Management”.

### RADIUS Servers Enforcing VLAN Access Control

A RADIUS server can be used to enforce VLAN access control in two ways:

- Authorize the SSID the client uses to connect to the AP. The SSID determines the VLAN that the client gets assigned to.
- Assigning the user to a VLAN by specifying the VLAN membership information of the user.

### Configuring Radius Profiles

A RADIUS server Profile consists of a Primary and a Secondary RADIUS server that get assigned to act as either MAC Authentication servers, 802.1x/EAP Authentication servers, or Accounting Servers in the VLAN Configuration. See [Configuring Security Profiles](#).

The RADIUS Profiles tab allows you to add new RADIUS profiles or modify or delete existing profiles.

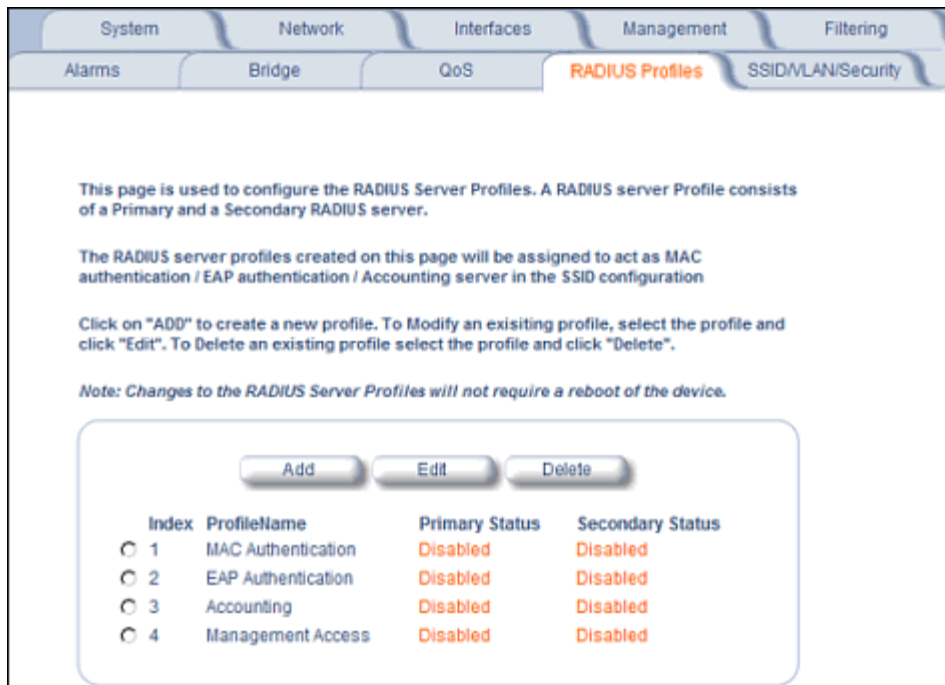


Figure 4-43 RADIUS Server Profiles

### Adding or Modifying a RADIUS Server Profile

Perform the following procedure to add a RADIUS server profile and to configure its parameters.

1. Click **Add** to create a new profile. To Modify an existing profile, select the profile and click Edit. To delete an existing profile, select the profile and click Delete. You cannot delete a RADIUS server profile if it is applied to an SSID.
2. Configure the following parameters for the RADIUS Server profile (see [Figure 4-44](#)):



**NOTE:** This page configures only the Primary RADIUS Server associated with the profile. After configuring these parameters, save them by clicking OK. Then, to configure the Secondary RADIUS Server, edit the profile from the main page.

Figure 4-44 Add RADIUS Server Profile

- **Server Profile Name:** the profile name. This is the name used to associated a VLAN to the profile. See [Configuring Security Profiles](#). The Server Profile Name is also used in the Configure > Management > Services page to specify the RADIUS profile to be used for RADIUS Based Management Access.
- **MAC Address Format Type:** This parameter should correspond to the format in which the clients' 12-digit MAC addresses are listed within the RADIUS server and the way passwords are sent to the RADIUS server. Available options are:
  - Dash delimited/SS: MAC addresses are formatted with a dash between each pair of digits (xx-yy-zz-aa-bb), and the password sent to the RADIUS server is the shared secret (configured below).
  - Colon delimited/SS: MAC addresses are formatted with a colon between each pair of digits (xx:yy:zz:aa:bb:cc) and the password sent to the RADIUS server is the shared secret (configured below).
  - Single dash delimited/SS: MAC addresses are formatted with a dash between the sixth and seventh digits (xxyyzz-aabbcc) and the password sent to the RADIUS server is the shared secret (configured below).
  - No delimiters/SS: MAC addresses are formatted with no characters or spaces between pairs of hexadecimal digits (xxyyzaabbcc) and the password sent to the RADIUS server is the shared secret (configured below).
  - Dash delimited/MAC: MAC addresses are formatted with a dash between each pair of digits (xx-yy-zz-aa-bb), and the password sent to the RADIUS server is the MAC address of the client.



- Colon delimited/MAC: MAC addresses are formatted with a colon between each pair of digits (xx:yy:zz:aa:bb:cc) and the password sent to the RADIUS server is the MAC address of the client.
  - Single dash delimited/MAC: MAC addresses are formatted with a dash between the sixth and seventh digits (xxyyzz-aabbcc) and the password sent to the RADIUS server is the MAC address of the client.
  - No delimiters/MAC: MAC addresses are formatted with no characters or spaces between pairs of hexadecimal digits (xxyyzzaaabbcc) and the password sent to the RADIUS server is the MAC address of the client.
  - **Accounting update interval:** Enter the time interval (in minutes) for sending Accounting Update messages to the RADIUS server. A value of 0 (default) means that the AP will not send Accounting Update messages.
  - **Accounting inactivity timer:** Enter the accounting inactivity timer. This parameter supports a value from 1-60 minutes. The default is 5 minutes.
  - **Authorization lifetime:** Enter the time, in seconds, each client session may be active before being automatically re-authenticated. This parameter supports a value between 900 and 43200 seconds. The default is 0 (disabled).
  - **Server Addressing Format:** select IP Address or Name. If you want to identify RADIUS servers by name, you must configure the AP as a DNS Client. See [DNS Client](#) for details.
  - **Server Name/IP Address:** Enter the server's name or IP address.
  - **Destination Port:** Enter the port number which the AP and the server will use to communicate. By default, RADIUS servers communicate on port 1812.
  - **Server VLAN ID:** Indicates the VLAN that uses this RADIUS server profile. If VLAN is disabled, this field will be grayed out.
  - **Shared Secret and Confirm Shared Secret:** Enter the password shared by the RADIUS server and the AP. The same password must also be configured on the RADIUS server. The default password is "public."
  - **Response Time (seconds):** Enter the maximum time, in seconds, that the AP should wait for the RADIUS server to respond to a request. The range is 1-10 seconds; the default is 3 seconds.
  - **Maximum Retransmissions (0-4):** Enter the maximum number of times an authentication request may be transmitted. The range is 0 to 4, the default is 3.
  - **Server Status:** Select Enable from the drop-down box to enable the RADIUS Server Profile.
3. Click **OK**.
  4. Select the Profile and click **Edit** to configure the Secondary RADIUS Server, if required.

## MAC Access Control Via RADIUS Authentication

If you want to control wireless access to the network and if your network includes a RADIUS Server, you can store the list of MAC addresses on the RADIUS server rather than configure each AP individually. You can define a RADIUS Profile that specifies the IP Address of the server that contains a central list of MAC Address values identifying the authorized stations that may access the wireless network. You must specify information for at least the primary RADIUS server. The back-up RADIUS server is optional.

**NOTE:** Each VLAN can be configured to use a separate RADIUS server (and backup server) for MAC authentication. MAC access control can be separately enabled for each VLAN.

**NOTE:** Contact your RADIUS server manufacturer if you have problems configuring the server or have problems using RADIUS authentication.

## 802.1x Authentication using RADIUS

You must configure a primary EAP/802.1x Authentication server to use 802.1x security. A back-up server is optional.

**NOTE:** Each VLAN can be configured to use a separate RADIUS server (and backup server) for 802.1x authentication. 802.1x authentication ("EAP authentication") can be separately enabled for each VLAN.

## RADIUS Accounting

Using an external RADIUS server, the AP can track and record the length of client sessions on the access point by sending RADIUS accounting messages per RFC2866. When a wireless client is successfully authenticated, RADIUS accounting is initiated by sending an “Accounting Start” request to the RADIUS server. When the wireless client session ends, an “Accounting Stop” request is sent to the RADIUS server.

**NOTE:** Each VLAN can be configured to use a separate RADIUS accounting server (and backup accounting server).

### Session Length

Accounting sessions continue when a client reauthenticates to the same AP. Sessions are terminated when:

- A client disassociates.
- A client does not transmit any data to the AP for a fixed amount of time.
- A client is detected on a different interface.
- Idle-Timeout or Session-Timeout attributes are configured in the Radius server.

If the client roams from one AP to another, one session is terminated and a new session is begun.

**NOTE:** This feature requires RADIUS authentication using MAC Access Control or 802.1x. Wireless clients configured in the Access Point's static MAC Access Control list are not tracked.

### Authentication and Accounting Attributes

Additionally, the AP supports a number of Authentication and Accounting Attributes defined in RFC2865, RFC2866, RFC2869, and RFC3580.

#### Authentication Attributes

- State: Received in Access-Accept Packet by the AP during Authentication and sent back as-is during Re-Authentication.
- Class: Received in Access-Accept Packet by the AP during Authentication and back as in Accounting Packets.
- Session-Timeout
  - If the RADIUS server does not send a Session-Timeout, the AP will set the subscriber expiration time to 0, which means indefinite access.
  - The Termination Action attribute defines how the Session-Timeout attribute will be interpreted. If the Termination Action is DEFAULT, then the session is terminated on expiration of the Session-Timeout time interval. If Termination Action is RADIUS-Request, then re-authentication is done on expiration on the session.
  - If the RADIUS server sends a Session-Timeout, the value specified by the Session-Timeout attribute will take precedence over the configured Authorization Lifetime value.
- Termination-Action
  - Valid values are: Default (0), RADIUS-Request (1). When the value is “default,” the Termination-Action attribute sends an accounting stop message and then reauthenticates. If the value is “RADIUS-Request,” the Termination-Action attribute reauthenticates without sending an accounting stop.
- Idle Timeout
  - The AP internally maintains the Idle-Timeout attribute obtained for each of the users during their authentication process, and uses this time interval in place of accounting inactivity time for timing out clients.
- Calling Station Id
  - MAC address of the client being authenticated.
- Called Station Id
  - The AP sends the MAC address of its own wireless interface with which the client getting authenticated is getting associated, appended with the SSID. If VLAN is enabled, the SSID and corresponding VLAN ID get appended.
- Acct-Interim-Interval

- Obtained during the Authentication process and used for determining the time interval for sending Accounting Update messages.
- This attribute value takes precedence over the value of the Accounting Update Interval.

**Accounting Attributes**

- Acct-Delay-Time
  - Indicates how many seconds the AP has been trying to send a particular packet related to a particular user. This time can be used at the server to determine the approximate time of the event generating this accounting request.
- Acct-Session-Id
  - Unique accounting ID that aids in tracking client accounting records. This attribute is sent in Start and Stop RADIUS accounting messages, and contains the client MAC address appended with the unique session ID.
- Acct-Session-Time
  - Acct-Session-Time is calculated the following way (for each transmitted/retransmitted Acct-Stop):  
Acct-Session-Time = time of last sent packet - subscriber login time.
- Acct-Input-Octets
  - Number of octets (bytes) received by subscriber.
- Acct-Output-Octets
  - Number of octets (bytes) sent by subscriber.
- Acct-Input-Packets
  - Number of packets received by subscriber.
- Acct-Output-Packets
  - Number of packets sent by subscriber.
- Acct-Terminate Cause
  - Indicates how the session was terminated.
- Vendor Specific Attributes

---

## SSID/VLAN/Security

The AP provides several security features to protect your network from unauthorized access. This section gives an overview of VLANs and then discusses the SSID/VLAN/Security configuration options in the AP:

- [VLAN Overview](#)
- [Management VLAN](#)
- [Security Profile](#)
- [MAC Access](#)
- [Wireless](#)

The AP also provides Broadcast Unique Beacon/Closed System and Rogue Scan to protect your network from unauthorized access. See the [Wireless](#) and [Rogue Scan](#) sections for more information.

### VLAN Overview

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to clients) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

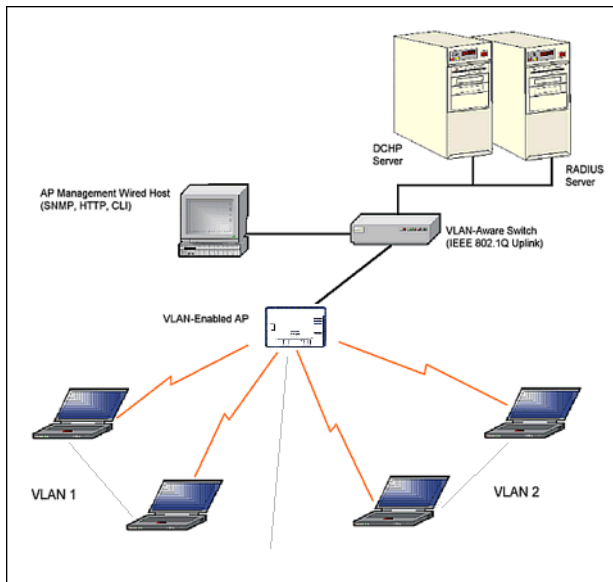
VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

AP devices are fully VLAN-ready; however, by default VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
  - Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own VLAN
  - Clients roam without compromising security

VLAN tagged data is collected and distributed through an AP's wireless interface(s) based on Network Name (SSID). An Ethernet port on the access point connects a wireless cell or network to a wired backbone. The access points communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses for the VLAN(s). Resources like servers and printers may be present, and a hub may include multiple APs, extending the network over a larger area.



**Figure 4-45 Components of a Typical VLAN**

### VLAN Workgroups and Traffic Management

Access Points that are not VLAN-capable typically transmit broadcast and multicast traffic to all wireless Network Interface Cards (NICs). This process wastes wireless bandwidth and degrades throughput performance. In comparison, a VLAN-capable AP is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 16 SSIDs per radio, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup; for example, one VLAN could be used for an EMPLOYEE workgroup and the other for a GUEST workgroup.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup could be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

### Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup.

The AP can segment users into a maximum of 16 different workgroups, based on an SSID/VLAN grouping (also referred as a VLAN Workgroup or a Sub-network).

The primary scenarios for using VLAN workgroups are as follows:

1. VLAN disabled: Your network does not use VLANs, and you cannot configure the AP to use multiple SSIDs.
2. VLAN enabled, each VLAN workgroup uses a different VLAN ID Tag.
3. VLAN enabled, a mixture of Tagged and Untagged workgroups exist.
4. VLAN enabled, all VLANs untagged: VLAN is enabled in order to use SSID. (Note that typical use of SSIDs assumes actual use of VLANs.)

**NOTE:** VLAN must be enabled to configure security per SSID.

## Management VLAN

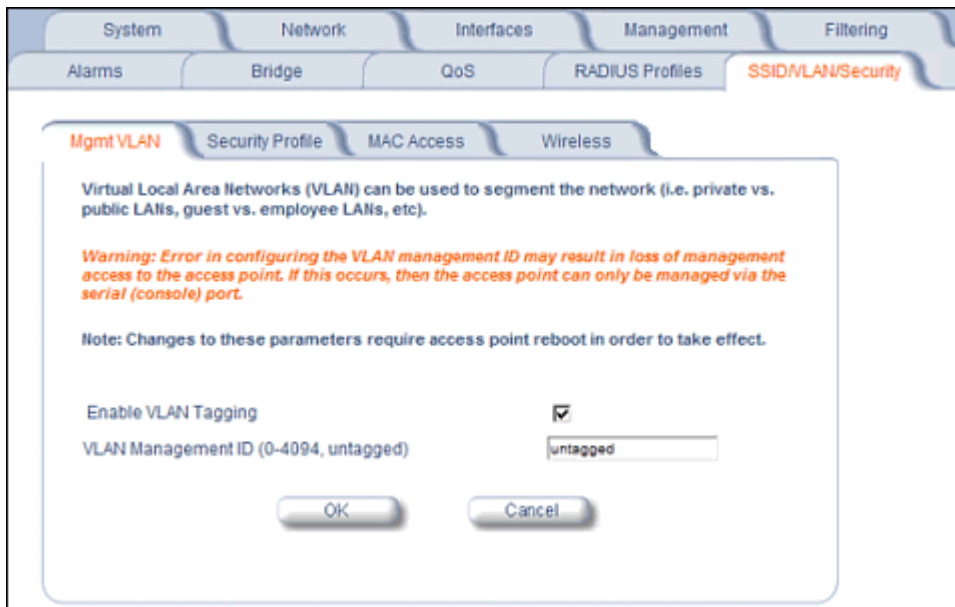


Figure 4-46 Mgmt VLAN

## VLAN Tagging Management

### Control Access to the AP

Management access to the AP can easily be secured by making management stations or hosts and the AP itself members of a common VLAN. Simply configure a non-zero management VLAN ID and enable VLAN to restrict management of the AP to members of the same VLAN.

**CAUTION:** If a non-zero management VLAN ID is configured then management access to the AP is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the AP.

**NOTE:** When VLAN is enabled, ensure that all devices in the network share the same VLAN ID.

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Set the VLAN Management ID to a value of between 1 and 4094. (A value of -1 disables VLAN Tagging).
3. Place a check mark in the **Enable VLAN Tagging** box.

### Provide Access to a Wireless Host in the Same Workgroup

The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN User ID, then those wireless clients who are members of that VLAN will have AP management access.

**CAUTION:** *Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.*

**NOTE:** *When VLAN is enabled, ensure that all devices in the network share the same VLAN ID.*

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Set the **VLAN Management ID** to use the same VLAN ID as one of the configured SSIDs.
3. Place a check mark in the **Enable VLAN Tagging** box.

#### **Disable VLAN Tagging**

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Remove the check mark from the **Enable VLAN Tagging** box (to disable all VLAN functionality) or set the **VLAN Management ID** to -1 (to disable VLAN Tagging only).

**NOTE:** *If you disable VLAN Tagging, you will be unable to configure security per SSID.*

## Security Profile

See the following sections:

- [Security Features](#)
- [Authentication Protocol Hierarchy](#)
- [VLANs and Security Profiles](#)
- [Configuring Security Profiles](#)

## Security Features

The AP supports the following security features:

- **WEP Encryption:** The original encryption technique specified by the IEEE 802.11 standard.
- **802.1x Authentication:** An IEEE standard for client authentication.
- **Wi-Fi Protected Access (WPA/802.11i [WPA2]):** A new standard that provides improved encryption security over WEP.

**NOTE:** *The AP does not support shared key 802.11 MAC level authentication. Clients with this MAC level feature must disable it.*

### **WEP Encryption**

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

### **802.1x Authentication**

IEEE 802.1x is a standard that provides a means to authenticate and authorize network devices attached to a LAN port. A port in the context of IEEE 802.1x is a point of attachment to the LAN, either a physical Ethernet connection or a wireless link to an Access Point. 802.1x requires a RADIUS server and uses the Extensible Authentication Protocol (EAP) as a standards-based authentication framework, and supports automatic key distribution for enhanced security. The EAP-based authentication framework can easily be upgraded to keep pace with future EAP types.

Popular EAP types include:

- EAP-Message Digest 5 (MD5): Username/Password-based authentication; does not support automatic key distribution
- EAP-Transport Layer Security (TLS): Certificate-based authentication (a certificate is required on the server and each client); supports automatic key distribution
- EAP-Tunneled Transport Layer Security (TTLS): Certificate-based authentication (a certificate is required on the server; a client's username/password is tunneled to the server over a secure connection); supports automatic key distribution
- PEAP - Protected EAP with MS-CHAP: Secure username/password-based authentication; supports automatic key distribution

Different servers support different EAP types and each EAP type provides different features. See the documentation that came with your RADIUS server to determine which EAP types it supports.

**NOTE:** The AP supports the following EAP types when Security Mode is set to 802.1x, WPA, or 802.11i (WPA2): EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, and EAP-SIM.

#### Authentication Process

There are three main components in the authentication process. The standard refers to them as:

1. Supplicant (client PC)
2. Authenticator (Access Point)
3. Authentication server (RADIUS server)

When the Security Mode is set to 802.1x Station, WPA Station, or 802.11i Station you need to configure your RADIUS server for authentication purposes.

Prior to successful authentication, an unauthenticated client PC cannot send any data traffic through the AP device to other systems on the LAN. The AP inhibits all data traffic from a particular client PC until the client PC is authenticated. Regardless of its authentication status, a client PC can always exchange 802.1x messages in the clear with the AP (the client begins encrypting data after it has been authenticated).

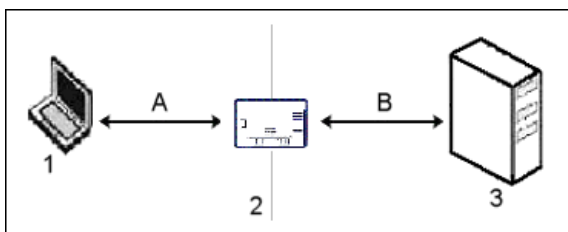


Figure 4-47 RADIUS Authentication Illustrated

The AP acts as a pass-through device to facilitate communications between the client PC and the RADIUS server. The AP (2) and the client (1) exchange 802.1x messages using an EAPOL (EAP Over LAN) protocol (A). Messages sent from the client station are encapsulated by the AP and transmitted to the RADIUS (3) server using EAP extensions (B).

Upon receiving a reply EAP packet from the RADIUS, the message is typically forwarded to the client, after translating it back to the EAPOL format. Negotiations take place between the client and the RADIUS server. After the client has been successfully authenticated, the client receives an Encryption Key from the AP (if the EAP type supports automatic key distribution). The client uses this key to encrypt data after it has been authenticated.

For 802.11a and 802.11b/g clients that communicate with an AP, each client receives its own unique encryption key; this is known as Per User Per Session Encryption Keys.



### **Wi-Fi Protected Access (WPA/802.11i [WPA2])**

Wi-Fi Protected Access (WPA) is a security standard designed by the Wi-Fi Alliance in conjunction with the Institute of Electrical and Electronics Engineers (IEEE). The AP supports 802.11i (WPA2), based on the IEEE 802.11i security standard.

WPA is a replacement for Wired Equivalent Privacy (WEP), the encryption technique specified by the original 802.11 standard. WEP has several vulnerabilities that have been widely publicized. WPA addresses these weaknesses and provides a stronger security system to protect wireless networks.

WPA provides the following new security measures not available with WEP:

- Improved packet encryption using the Temporal Key Integrity Protocol (TKIP) and the Michael Message Integrity Check (MIC).
- Per-user, per-session dynamic encryption keys:
  - Each client uses a different key to encrypt and decrypt unicast packets exchanged with the AP
  - A client's key is different for every session; it changes each time the client associates with an AP
  - The AP uses a single global key to encrypt broadcast packets that are sent to all clients simultaneously
  - Encryption keys change periodically based on the **Re-keying Interval** parameter
  - WPA uses 128-bit encryption keys
- Dynamic Key distribution
  - The AP generates and maintains the keys for its clients
  - The AP securely delivers the appropriate keys to its clients
- Client/server mutual authentication
  - 802.1x
  - Pre-shared key (for networks that do not have an 802.1x solution implemented)

The AP supports the following WPA security modes:

- **WPA:** The AP uses 802.1x to authenticate clients and TKIP for encryption. You should only use an EAP that supports mutual authentication and session key generation, such as EAP-TLS, EAP-TTLS, and PEAP. See [802.1x Authentication](#) for details.
- **WPA-PSK (Pre-Shared Key):** For networks that do not have 802.1x implemented, you can configure the AP to authenticate clients based on a Pre-Shared Key. This is a shared secret that is manually configured on the AP and each of its clients. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the TKIP Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).
- **802.11i** (also known as WPA2): The AP provides security to clients according to the 802.11i draft standard, using 802.1x authentication, a CCMP cipher based on AES, and re-keying.
- **802.11i-PSK** (also known as WPA2 PSK): The AP uses a CCMP cipher based on AES, and encrypts frames to clients based on a Pre-Shared Key. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).

**NOTE:** For more information on WPA, see the Wi-Fi Alliance Web site at <http://www.wi-fi.org>.

### **Authentication Protocol Hierarchy**

There is a hierarchy of authentication protocols defined for the AP. The hierarchy is as follows, from highest to lowest:

- 802.1x authentication (including 802.1x, WPA, WPA-PSK, 802.11i, 802.11i-PSK)
- MAC Access Control via RADIUS Authentication
- MAC Access Control through individual APs' MAC Access Control Lists

If you have both 802.1x and MAC Access Control authentication enabled, the 802.1x authentication takes precedence because it is higher in the authentication protocol hierarchy. This is required in order to propagate the WEP/TKIP/AES keys to the clients in such cases. If you disable 802.1x on the AP, you will see the effects of MAC authentication.

In addition, setting MAC Access Control status to **Strict** will cause *both* MAC ACL settings and 802.1x settings to be applied.

For example, assume that the MAC Access Control List contains MAC addresses to block, and that WPA-PSK is configured to allow access to clients with the appropriate PSK Passphrase.

- If the MAC ACL status is set to **Enable**, WPA-PSK will take precedence, and clients in the MAC ACL with the correct PSK passphrase will be *allowed*. Only the WPA-PSK setting is taken into consideration.
- If the MAC ACL status is set to **Strict**, then clients in the MAC ACL will be blocked even if they have the correct PSK passphrase. Clients will only be allowed if they have the correct passphrase *and* are NOT listed in the MAC ACL. In this way, both MAC and WPA-PSK settings are taken into consideration.

### VLANS and Security Profiles

The AP allows you to segment wireless networks into multiple sub-networks based on Network Name (SSID) and VLAN membership. A Network Name (SSID) identifies a wireless network. Clients associate with Access Points that share an SSID. During installation, the Setup Wizard prompts you to configure a Primary Network Name for each wireless interface.

After initial setup and once VLAN is enabled, the AP can be configured to support up to 16 SSIDs to segment wireless networks based on VLAN membership.

Each VLAN can be associated to a Security Profile and RADIUS Server Profiles. A Security Profile defines the allowed wireless clients, and authentication and encryption types. See the following sections for configuration details.

### Configuring Security Profiles

Security policies can be configured and applied on the AP as a whole, or on a per VLAN basis. When VLAN is disabled on the AP, the user can configure a security profile for each interface of the AP. When VLANs are enabled and Security per SSID is enabled, the user can configure a security profile for each VLAN.

The user defines a security policy by specifying one or more values for the following parameters:

- Wireless STA types (WPA station, 802.11i (WPA2) station, 802.1x station, WEP station, WPA-PSK, and 802.11i-PSK) that can associate to the AP.
- Authentication mechanisms (802.1x, RADIUS MAC authentication) that are used to authenticate clients for each type of station.
- Cipher Suites (CCMP, TKIP, WEP, None) used for encapsulating the wireless data for each type of station.

Up to 16 security profiles can be configured.

1. Click **Configure** > **SSID/VLAN/Security** > **Security Profile**.

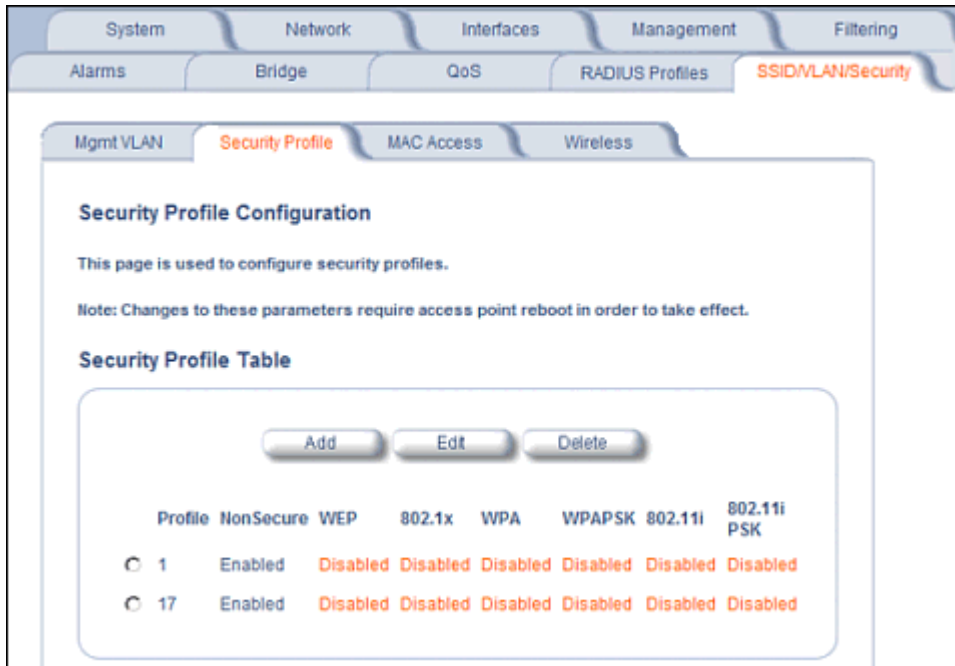


Figure 4-48 Security Profile Configuration

2. Click **Add** in the Security Profile Table to create a new entry. To modify an existing profile, select the profile and click **Edit**. To delete an existing profile, select the profile and click **Delete**. You cannot delete a Security Profile used in an SSID. Also, the first Security Profile cannot be deleted.
3. Configure one or more types of wireless stations (security modes) that are allowed access to the AP under the security profile. The WEP/PSK parameters are separately configurable for each security mode. To enable a security mode in the profile (Non Secure Station, WEP Station, 802.1x Station, WPA Station, WPA-PSK Station, 802.11i (WPA2) Station, 802.11i-PSK Station), check the box next to the mode. See [Figure 4-49](#).

If the security mode selected in a profile is WEP, WPA-PSK, or 802.11i-PSK, then you must configure the WEP or Pre-Shared Keys.

**NOTE:** If an 802.1x client that has already been authenticated attempts to switch to WEP, or if a WEP client that has already been connected attempts to switch to 802.1x, the AP will not allow the client to switch immediately. If this happens, either reboot the AP or disable the client/roam to a new AP for five minutes, and then attempt to reconnect to the AP. If the client is still unable to connect after waiting five minutes, reboot the AP.

4. Configure the parameters as follows for each enabled security mode. See [Figure 4-49](#).
  - **Non Secure Station:**
    - Authentication Mode: None. The AP allows access to Stations without authentication.
      - Non secure station should be used only with WEP or 802.1x security mode.
    - Cipher: None
  - **WEP Station:**
    - Authentication Mode: None
    - Cipher: WEP
    - Encryption Key 0, Encryption Key 1, Encryption Key 2, Encryption Key 3

**NOTE:** When VLAN tagging is enabled, only Key 0 can be configured.

    - Encryption Key Length: 64, 128, or 152 Bits.