



# Motorola Solutions WiNG 5.5.3 ACCESS POINT SYSTEM REFERENCE GUIDE





# **MOTOROLA SOLUTIONS WING 5.5.3 ACCESS POINT SYSTEM REFERENCE GUIDE**

MN000874A01

Revision A

June 2014

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Motorola Solutions. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Motorola Solutions grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Motorola Solutions. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Motorola Solutions. The user agrees to maintain Motorola Solution’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Motorola Solutions reserves the right to make changes to any software or product to improve reliability, function, or design.

Motorola Solutions does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Motorola Solutions, Inc., intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Motorola Solutions products

# TABLE OF CONTENTS

## About this Guide

## Chapter 1, Overview

1.1 About the Motorola Solutions WiNG 5 Software .....	1-3
--	-----

## Chapter 2, Web User Interface Features

2.1 Accessing the Web UI .....	2-2
2.1.1 Browser and System Requirements .....	2-2
2.1.2 Connecting to the Web UI .....	2-2
2.2 Icon Glossary .....	2-4
2.2.1 Global Icons .....	2-4
2.2.2 Dialog Box Icons .....	2-5
2.2.3 Table Icons .....	2-5
2.2.4 Status Icons .....	2-6
2.2.5 Configurable Objects .....	2-6
2.2.6 Configuration Objects .....	2-9
2.2.7 Configuration Operation Icons .....	2-10
2.2.8 Access Type Icons .....	2-10
2.2.9 Administrative Role Icons .....	2-11
2.2.10 Device Icons .....	2-11

## Chapter 3, Quick Start

3.1 Using the WiNG Initial Setup Wizard .....	3-2
3.1.1 Typical Setup Wizard .....	3-5
3.1.1.1 Virtual Controller AP Mode .....	3-8
3.1.1.2 Standalone Mode .....	3-9
3.1.1.3 Network Topology Selection .....	3-10
3.1.1.4 LAN Configuration .....	3-11
3.1.1.5 WAN Configuration .....	3-13

---

3.1.1.6	Wireless LAN Setup .....	3-15
3.1.1.7	Summary And Commit Screen .....	3-19
3.1.1.8	Adopt to a controller .....	3-20
3.1.2	Advanced Setup Wizard .....	3-21
3.1.2.1	Network Topology Selection .....	3-24
3.1.2.2	LAN Configuration .....	3-25
3.1.2.3	WAN Configuration .....	3-27
3.1.2.4	Radio Configuration .....	3-29
3.1.2.5	Wireless LAN Setup .....	3-31
3.1.2.6	System Information .....	3-33
3.1.2.7	Summary And Commit Screen .....	3-34
3.1.2.8	Adopt to a controller .....	3-35
3.2	Using WiNG Express Quick Configuration .....	3-36

## Chapter 4, Dashboard

4.1	Dashboard .....	4-2
4.1.1	Dashboard Conventions .....	4-2
4.1.1.1	Health .....	4-3
4.1.1.2	Inventory .....	4-7
4.2	Network View .....	4-10
4.2.1	Network View Display Options .....	4-11
4.2.2	Device Specific Information .....	4-12

## Chapter 5, Device Configuration

5.1	RF Domain Configuration .....	5-2
5.1.1	RF Domain Sensor Configuration .....	5-4
5.1.2	RF Client Name Configuration .....	5-5
5.1.3	RF Domain Alias Configuration .....	5-5
5.1.3.1	Network Basic Alias .....	5-7
5.1.3.2	Network Group Alias .....	5-10
5.1.3.3	Network Service Alias .....	5-12
5.2	System Profile Configuration .....	5-14
5.2.1	General Profile Configuration .....	5-15
5.2.2	Profile Radio Power .....	5-16
5.2.3	Profile Adoption (Auto Provisioning) Configuration .....	5-18
5.2.4	Profile Wired 802.1X Configuration .....	5-20
5.2.5	Profile Interface Configuration .....	5-21
5.2.5.1	Ethernet Port Configuration .....	5-22
5.2.5.2	Virtual Interface Configuration .....	5-31
5.2.5.3	Port Channel Configuration .....	5-34
5.2.5.4	Access Point Radio Configuration .....	5-41
5.2.5.5	WAN Backhaul Configuration .....	5-53
5.2.5.6	PPPoE Configuration .....	5-56
5.2.6	Profile Network Configuration .....	5-59
5.2.6.1	DNS Configuration .....	5-60

5.2.6.2	ARP	5-61
5.2.6.3	L2TPv3 Profile Configuration	5-62
5.2.6.4	IGMP Snooping	5-71
5.2.6.5	Quality of Service (QoS)	5-73
5.2.6.6	Spanning Tree Configuration	5-74
5.2.6.7	Routing	5-77
5.2.6.8	Dynamic Routing (OSPF)	5-79
5.2.6.9	Forwarding Database	5-86
5.2.6.10	Bridge VLAN	5-87
5.2.6.11	Cisco Discovery Protocol Configuration	5-92
5.2.6.12	Link Layer Discovery Protocol Configuration	5-93
5.2.6.13	Miscellaneous Network Configuration	5-94
5.2.6.14	Alias	5-95
5.2.6.15	Profile Network Configuration and Deployment Considerations	5-103
5.2.7	Profile Security Configuration	5-104
5.2.7.1	Defining Profile VPN Settings	5-104
5.2.7.2	Auto IPsec Tunnel	5-120
5.2.7.3	Defining Profile Security Settings	5-121
5.2.7.4	Setting the Certificate Revocation List (CRL) Configuration	5-122
5.2.7.5	Setting the Profile's NAT Configuration	5-123
5.2.7.6	Setting the Profile's Bridge NAT Configuration	5-132
5.2.7.7	Profile Security Configuration and Deployment Considerations	5-134
5.2.8	Virtual Router Redundancy Protocol (VRRP) Configuration	5-135
5.2.9	Profile Critical Resources	5-139
5.2.10	Profile Services Configuration	5-142
5.2.10.1	Profile Services Configuration and Deployment Considerations	5-143
5.2.11	Profile Management Configuration	5-144
5.2.11.1	Upgrading AP6532 Firmware from 5.1	5-149
5.2.11.2	Profile Management Configuration and Deployment Considerations	5-149
5.2.12	Mesh Point Configuration	5-150
5.2.12.1	Vehicle Mounted Modem (VMM) Deployment Consideration	5-158
5.2.13	Advanced Profile Configuration	5-159
5.2.13.1	Advanced Profile Client Load Balancing	5-160
5.2.13.2	Configuring MINT Protocol	5-164
5.2.13.3	Advanced Profile Miscellaneous Configuration	5-169
5.2.14	Environmental Sensor Configuration	5-170
5.3	Managing Virtual Controllers	5-173
5.4	Overriding a Device Configuration	5-175
5.4.1	Basic Configuration	5-175
5.4.2	Certificate Management	5-177
5.4.2.1	Manage Certificates	5-179
5.4.3	RF Domain Overrides	5-192
5.4.4	Wired 802.1X Overrides	5-194
5.4.5	Device Overrides	5-195
5.4.5.1	Radio Power Overrides	5-197
5.4.5.2	Adoption Overrides	5-199
5.4.5.3	Profile Interface Override Configuration	5-202

---

5.4.5.4	Overriding the Network Configuration .....	5-236
5.4.5.5	Overriding a Security Configuration .....	5-281
5.4.5.6	Overriding the Virtual Router Redundancy Protocol (VRRP) Configuration .....	5-304
5.4.5.7	Profile Critical Resources .....	5-309
5.4.5.8	Overriding a Services Configuration .....	5-312
5.4.5.9	Overriding a Management Configuration .....	5-313
5.4.5.10	Overriding Mesh Point Configuration .....	5-317
5.4.5.11	Overriding an Advanced Configuration .....	5-326
5.4.5.12	Overriding Environmental Sensor Configuration .....	5-336
5.5	Managing an Event Policy .....	5-338

## Chapter 6, Wireless Configuration

6.1	Wireless LANs .....	6-3
6.1.1	Basic WLAN Configuration .....	6-5
6.1.1.1	WLAN Basic Configuration Deployment Considerations .....	6-7
6.1.2	Configuring WLAN Security .....	6-7
6.1.2.1	802.1x EAP, EAP-PSK and EAP MAC .....	6-8
6.1.2.2	MAC Authentication .....	6-10
6.1.2.3	PSK / None .....	6-11
6.1.2.4	Captive Portal .....	6-11
6.1.2.5	Passpoint Policy .....	6-12
6.1.2.6	MAC Registration .....	6-12
6.1.2.7	External Controller .....	6-13
6.1.2.8	WPA/WPA2-TKIP .....	6-13
6.1.2.9	WPA2-CCMP .....	6-16
6.1.2.10	WEP 64 .....	6-19
6.1.2.11	WEP 128 and KeyGuard .....	6-21
6.1.3	Configuring WLAN Firewall Support .....	6-23
6.1.4	Configuring Client Settings .....	6-31
6.1.5	Configuring WLAN Accounting Settings .....	6-33
6.1.6	Configuring Service Monitoring Settings .....	6-35
6.1.7	Configuring Client Load Balancing .....	6-37
6.1.8	Configuring Advanced WLAN Settings .....	6-38
6.1.9	Configuring Auto Shutdown Settings .....	6-44
6.2	WLAN QoS Policy .....	6-46
6.2.1	Configuring QoS WMM Settings .....	6-48
6.2.2	Configuring a WLAN's QoS Rate Limit Settings .....	6-52
6.2.3	Configuring Multimedia Optimizations .....	6-57
6.2.3.1	WLAN QoS Deployment Considerations .....	6-59
6.3	Radio QoS Policy .....	6-60
6.3.1	Configuring a Radio's QoS Policy .....	6-61
6.4	Association ACL .....	6-71
6.4.1	Association ACL Deployment Considerations .....	6-73
6.5	SMART RF .....	6-74
6.5.1	Smart RF Configuration and Deployment Considerations .....	6-84
6.6	MeshConnex Policy .....	6-85

6.7 Mesh QoS Policy .....	6-91
6.8 Passpoint Policy .....	6-98

## Chapter 7, Network Configuration

7.1 Policy Based Routing (PBR) .....	7-2
7.2 L2TP V3 Configuration .....	7-8
7.3 AAA Policy .....	7-12
7.4 AAA TACACS Policy .....	7-22
7.5 Alias .....	7-34
7.5.1 Network Basic Alias .....	7-34
7.5.2 Network Group Alias .....	7-37
7.5.3 Network Service Alias .....	7-40
7.6 Network Deployment Considerations .....	7-42

## Chapter 8, Security Configuration

8.1 Wireless Firewall .....	8-2
8.1.1 Defining a Firewall Configuration .....	8-2
8.2 Configuring IP Firewall Rules .....	8-13
8.3 Device Fingerprinting .....	8-18
8.4 Configuring MAC Firewall Rules .....	8-25
8.5 Wireless IPS (WIPS) .....	8-28
8.6 Device Categorization .....	8-37
8.7 Security Deployment Considerations .....	8-39

## Chapter 9, Security Configuration

9.1 Configuring Captive Portal Policies .....	9-2
9.1.1 Configuring a Captive Portal Policy .....	9-2
9.2 Setting the DNS Whitelist Configuration .....	9-14
9.3 Setting the DHCP Server Configuration .....	9-15
9.3.1 Defining DHCP Pools .....	9-15
9.3.2 Defining DHCP Server Global Settings .....	9-23
9.3.3 DHCP Class Policy Configuration .....	9-25
9.4 Setting the Bonjour Gateway Configuration .....	9-28
9.4.1 Configuring the Bonjour Discovery Policy .....	9-28
9.4.2 Configuring the Bonjour Forwarding Policy .....	9-30
9.5 Setting the RADIUS Configuration .....	9-33
9.5.1 Creating RADIUS Groups .....	9-33
9.5.1.1 Creating RADIUS Groups .....	9-36
9.5.2 Defining User Pools .....	9-38
9.5.3 Configuring the RADIUS Server .....	9-41
9.6 Services Deployment Considerations .....	9-51

## Chapter 10, Security Configuration

10.1 Creating Administrators and Roles .....	10-2
--	------

---

10.2	Setting the Access Control Configuration .....	10-5
10.3	Setting the Authentication Configuration .....	10-8
10.4	Setting the SNMP Configuration .....	10-10
10.5	SNMP Trap Configuration .....	10-12
10.6	Management Access Deployment Considerations .....	10-13

## Chapter 11, Diagnostics

11.1	Fault Management .....	11-2
11.2	Crash Files .....	11-6
11.3	Advanced .....	11-7
11.3.1	UI Debugging .....	11-7
11.3.1.1	Schema Browser .....	11-8
11.3.2	View UI Logs .....	11-9
11.3.3	View Sessions .....	11-10

## Chapter 12, Security Configuration

12.1	Devices .....	12-2
12.1.1	Managing Firmware and Configuration Files .....	12-2
12.1.1.1	Managing Running Configuration .....	12-3
12.1.1.2	Managing Startup Configuration .....	12-6
12.1.1.3	Managing Crash Dump Files .....	12-9
12.1.2	Rebooting the Device .....	12-10
12.1.3	Locating a Device .....	12-11
12.1.4	Upgrading Device Firmware .....	12-12
12.1.5	Viewing Device Summary Information .....	12-14
12.1.6	Adopted Device Upgrades .....	12-16
12.1.7	File Management .....	12-23
12.1.8	Adopted Device Restart .....	12-29
12.1.9	Captive Portal Pages .....	12-30
12.1.10	Re-elect Controller .....	12-35
12.2	Certificates .....	12-37
12.2.1	Certificate Management .....	12-37
12.2.2	RSA Key Management .....	12-42
12.2.3	Certificate Creation .....	12-47
12.2.4	Generating a Certificate Signing Request (CSR) .....	12-49
12.3	Smart RF .....	12-52
12.3.1	Managing Smart RF for a RF Domain .....	12-52
12.4	Operations Deployment Considerations .....	12-55

## Chapter 13, Statistics

13.1	System Statistics .....	13-2
13.1.1	Health .....	13-2
13.1.2	Inventory .....	13-4
13.1.3	Adopted Devices .....	13-5

13.1.4	Pending Adoptions .....	13-7
13.1.5	Offline Devices .....	13-8
13.1.6	Device Upgrade .....	13-9
13.1.7	Licenses .....	13-10
13.2	RF Domain Statistics .....	13-14
13.2.1	Health .....	13-14
13.2.2	Inventory .....	13-17
13.2.3	Devices .....	13-19
13.2.4	AP Detection .....	13-20
13.2.5	Wireless Clients .....	13-21
13.2.6	Device Upgrade .....	13-22
13.2.7	Wireless LANs .....	13-24
13.2.8	Radios .....	13-25
13.2.8.1	Status .....	13-25
13.2.8.2	RF Statistics .....	13-27
13.2.8.3	Traffic Statistics .....	13-28
13.2.9	Mesh .....	13-29
13.2.10	Mesh Point .....	13-30
13.2.11	SMART RF .....	13-45
13.2.12	WIPS .....	13-50
13.2.12.1	WIPS Client Blacklist .....	13-50
13.2.12.2	WIPS Events .....	13-51
13.2.13	Captive Portal .....	13-52
13.3	Access Point Statistics .....	13-54
13.3.1	Health .....	13-55
13.3.2	Device .....	13-57
13.3.3	Device Upgrade .....	13-59
13.3.4	Adoption .....	13-60
13.3.4.1	Adopted APs .....	13-61
13.3.4.2	AP Adoption History .....	13-62
13.3.4.3	AP Self Adoption History .....	13-63
13.3.4.4	Pending Adoptions .....	13-63
13.3.5	AP Detection .....	13-64
13.3.6	Wireless Clients .....	13-66
13.3.7	Wireless LANs .....	13-67
13.3.8	Policy Based Routing .....	13-69
13.3.9	Radios .....	13-70
13.3.9.1	Status .....	13-71
13.3.9.2	RF Statistics .....	13-72
13.3.9.3	Traffic Statistics .....	13-73
13.3.10	Mesh .....	13-74
13.3.11	Interfaces .....	13-75
13.3.11.1	General Interface Details .....	13-76
13.3.11.2	Network Graph .....	13-78
13.3.12	RTLS .....	13-79
13.3.13	PPPoE .....	13-81
13.3.14	OSPF .....	13-82

---

13.3.14.1	OSPF Summary	13-83
13.3.14.2	OSPF Neighbors	13-85
13.3.14.3	OSPF Area Details	13-86
13.3.14.4	OSPF Route Statistics	13-88
13.3.14.5	OSPF Interface	13-91
13.3.14.6	OSPF State	13-92
13.3.15	L2TPv3 Tunnels	13-93
13.3.16	VRRP	13-95
13.3.17	Critical Resources	13-96
13.3.18	LDAP Agent Status	13-97
13.3.19	GRE Tunnels	13-98
13.3.20	Dot1x	13-99
13.3.21	Network	13-101
13.3.21.1	ARP Entries	13-101
13.3.21.2	Route Entries	13-102
13.3.21.3	Bridge	13-103
13.3.21.4	IGMP	13-104
13.3.21.5	DHCP Options	13-106
13.3.21.6	Cisco Discovery Protocol	13-108
13.3.21.7	Link Layer Discovery Protocol	13-109
13.3.22	DHCP Server	13-110
13.3.22.1	DHCP Bindings	13-112
13.3.22.2	DHCP Networks	13-113
13.3.23	Firewall	13-114
13.3.23.1	Packet Flows	13-115
13.3.23.2	Denial of Service	13-116
13.3.23.3	IP Firewall Rules	13-117
13.3.23.4	MAC Firewall Rules	13-118
13.3.23.5	NAT Translations	13-119
13.3.23.6	DHCP Snooping	13-120
13.3.24	VPN	13-122
13.3.24.1	IKESA	13-122
13.3.24.2	IPSec	13-123
13.3.25	Certificates	13-124
13.3.25.1	Trustpoints	13-124
13.3.25.2	RSA Keys	13-126
13.3.26	WIPS	13-127
13.3.26.1	WIPS Client Blacklist	13-127
13.3.26.2	WIPS Events	13-128
13.3.27	Sensor Servers	13-129
13.3.28	Bonjour Services	13-130
13.3.29	Captive Portal	13-131
13.3.30	Network Time	13-133
13.3.30.1	NTP Status	13-133
13.3.30.2	NTP Association	13-134
13.3.31	Load Balancing	13-135
13.3.32	Environmental Sensors (AP8132 Models Only)	13-137

---

13.4 Wireless Client Statistics .....	13-141
13.4.1 Health .....	13-141
13.4.2 Details .....	13-144
13.4.3 Traffic .....	13-148
13.4.4 WMM TSPEC .....	13-150
13.4.5 Association History .....	13-151
13.4.6 Graph .....	13-152

## Appendix A, Using WiNG Express

A.1 Dashboard .....	A-2
A.2 Monitor .....	A-4
A.2.1 Radios .....	A-5
A.2.2 WLANs .....	A-8
A.2.3 Clients .....	A-11
A.3 Configuration .....	A-14
A.3.1 Basic .....	A-15
A.3.2 LAN .....	A-17
A.3.3 WAN .....	A-19
A.3.4 Wireless .....	A-21
A.3.5 Security .....	A-24
A.3.5.1 Firewall .....	A-24
A.3.5.2 WIPS .....	A-26
A.3.6 Services .....	A-29
A.3.7 Management .....	A-30
A.4 Access Points .....	A-33
A.5 Event History .....	A-37

## Appendix B, Customer Support

## Appendix C, Publicly Available Software

C.1 General Information .....	C-1
C.2 Open Source Software Used .....	C-2
C.3 OSS Licenses .....	C-11
C.3.1 Apache License, Version 2.0 .....	C-11
C.3.2 The BSD License .....	C-13
C.3.3 Creative Commons Attribution-ShareAlike License, version 3.0 .....	C-13
C.3.4 DropBear License .....	C-18
C.3.5 GNU General Public License, version 2 .....	C-19
C.3.6 GNU Lesser General Public License 2.1 .....	C-23
C.3.7 GNU General Public License, version 3 .....	C-28
C.3.8 ISC License .....	C-36
C.3.9 GNU Lesser General Public License, version 3.0 .....	C-36
C.3.10 GNU General Public License 2.0 .....	C-38
C.3.11 GNU Lesser General Public License, version 2.0 .....	C-43

C.3.12 GNU Lesser General Public License, version 2.1 .....	C-48
C.3.13 MIT License .....	C-53
C.3.14 Mozilla Public License, version 2 .....	C-54
C.3.15 The Open LDAP Public License .....	C-58
C.3.16 OpenSSL License .....	C-58
C.3.17 WU-FTPD Software License .....	C-59
C.3.18 zlib License .....	C-60

---

# ABOUT THIS GUIDE

This manual supports the following access points:

- Access Points – AP300, AP621, AP622, AP650, AP6511, AP6511E, AP6521, AP6521E, AP6522, AP6522E, AP6522M, AP6532, AP6562, AP7131, AP7161, AP7181, AP7522, AP7522E, AP7532, AP7522E, AP8122, AP8132, AP8222, AP8232 and ES6510.



**NOTE:** In this guide, AP7131, AP7161, and AP7181 are collectively represented as AP71XX. Similarly, AP8122 and AP8132 are collectively represented as AP81XX. Also, the APs AP8222 and AP8232 are collectively represented as AP82XX. AP7522 and AP7532 are collectively represented as AP75XX. AP6511, AP6521, AP6522, AP6532, AP6562 are collectively represented as AP65XX.



**NOTE:** ES6510 is an *Ethernet Switch* managed by a wireless controller such as RFS4000/RFS6000/RFS7000/NX4500/NX4524/NX6500/NX6524/NX7500/NX9000/NX9500/NX9510. ES6510 does not have radios and does not provide WLAN support.



**NOTE:** Access points with ‘E’ appended to their names exclusively support WiNG Express.

---

---

This section is organized into the following:

- [Document Convention](#)
- [Notational Conventions](#)
- [Motorola Solutions Enterprise Mobility Support Center](#)
- [Motorola Solutions End-User Software License Agreement](#)

## Document Convention

The following conventions are used in this document to draw your attention to important information:



**NOTE:** Indicates tips or special requirements.

---

---



**CAUTION:** Indicates conditions that can cause equipment damage or data loss.

---

---



**WARNING!** Indicates a condition or procedure that could result in personal injury or equipment damage.

---

---



**Switch Note:** Indicates caveats unique to a RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500 or NX9510 model controller or service platform.

---

---

## Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (•) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

## Motorola Solutions Enterprise Mobility Support Center

If you have a problem with your equipment, contact Motorola Solutions Enterprise Mobility Support for your region.

Contact information is available by visiting the URL:

[http://www.motorolasolutions.com/Business/XP-EN/Pages/Contact\\_Us](http://www.motorolasolutions.com/Business/XP-EN/Pages/Contact_Us)

### **Customer Support Web Site**

Motorola Solutions' Support Central Web site, accessed via the Symbol-branded products link under Support for Business, provides information and online assistance including developer tools, software downloads, product manuals and online repair requests. Product support can be found at:

<https://portal.motorolasolutions.com/Support/US-EN>

When contacting Enterprise Mobility support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Motorola Solutions responds to calls by e-mail, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola Solutions business partner, contact that business partner for support.

### **Product Manuals**

<https://portal.motorolasolutions.com/Support/US-EN/Wireless+Networks>

### **Product Sales and Product Information**

Motorola Solutions, Inc.  
One Motorola Plaza  
Holtsville, New York 11742-1300

Tel: 1-631-738-2400 or 1-800-722-6234

Fax: 1-631-738-5990

### **General Information**

For general information, contact Motorola Solutions at:

Telephone (North America): 1-800-722-6234

Telephone (International): +1-631-738-5200

Website: <http://www.motorolasolutions.com>

---

## Motorola Solutions End-User Software License Agreement

THIS MOTOROLA SOLUTIONS END-USER SOFTWARE LICENSE AGREEMENT ("END-USER LICENSE AGREEMENT") IS BETWEEN MOTOROLA SOLUTIONS INC. (HEREIN "MOTOROLA SOLUTIONS") AND END-USER CUSTOMER TO WHOM MOTOROLA SOLUTIONS' PROPRIETARY SOFTWARE OR MOTOROLA SOLUTIONS PRODUCTS CONTAINING EMBEDDED, PRE-LOADED, OR INSTALLED SOFTWARE ("PRODUCTS") IS MADE AVAILABLE. THIS END-USER LICENSE AGREEMENT CONTAINS THE TERMS AND CONDITIONS OF THE LICENSE MOTOROLA SOLUTIONS IS PROVIDING TO END-USER CUSTOMER, AND END-USER CUSTOMER'S USE OF THE SOFTWARE AND DOCUMENTATION. BY USING, DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU OR THE ENTITY THAT YOU REPRESENT ("END-USER CUSTOMER") ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS END-USER LICENSE AGREEMENT.

### 1. DEFINITIONS

"Documentation" means product and software documentation that specifies technical and performance features and capabilities, and the user, operation and training manuals for the Software (including all physical or electronic media upon which such information is provided).

"Open Source Software" means software with either freely obtainable source code license for modification, or permission for free distribution.

"Open Source Software License" means the terms or conditions under which the Open Source Software is licensed.

"Software" (i) means proprietary software in object code format, and adaptations, translations, decompilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Motorola Solutions; and (iii) may contain items of software owned by a third party supplier. The term "Software" does not include any third party software provided under separate license or third party software not licensable under the terms of this Agreement. To the extent, if any, that there is a separate license agreement packaged with, or provided electronically with, a particular Product that becomes effective on an act of acceptance by the end user, then that agreement supersedes this End-User License Agreement as to the end use of that particular Product.

### 2. GRANT OF LICENSE

2.1 Subject to the provisions of this End-User License Agreement, Motorola Solutions grants to End-User Customer a personal, limited, non-transferable (except as provided in Section 4), and non-exclusive license under Motorola Solutions' copyrights and confidential information embodied in the Software to use the Software, in object code form, and the Documentation solely in connection with End-User Customer's use of the Products. This End-User License Agreement does not grant any rights to source code.

2.2 If the Software licensed under this End-User License Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not this End-User License Agreement. If there is a conflict between the terms and conditions of this End-User License Agreement and the terms and conditions of the Open Source Software Licenses governing End-User Customer's use of the Open Source Software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this End-User License Agreement. If requested by End-User Customer, Motorola Solutions will use commercially reasonable efforts to: (i) determine whether any Open source Software is provided under this End-User License Agreement; (ii) identify the Open Source Software and provide End-User Customer a copy of the applicable Open Source Software License (or specify where that license may be found); and, (iii) provide End-User Customer a copy of the Open Source Software source code, without charge, if it is publicly available (although distribution fees may be applicable).

### 3. LIMITATIONS ON USE

3.1 End-User Customer may use the Software only for End-User Customer's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited and will be deemed a breach of this End-User License Agreement. Without limiting the general nature of these restrictions, End-User Customer will

not make the Software available for use by third parties on a “time sharing,” “application service provider,” or “service bureau” basis or for any other similar commercial rental or sharing arrangement.

3.2 End-User Customer will not, and will not allow or enable any third party to: (i) reverse engineer, disassemble, peel components, decompile, reprogram or otherwise reduce the Software or any portion to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software with other software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party, grant any sublicense or other rights in the Software or Documentation to any third party, or take any action that would cause the Software or Documentation to be placed in the public domain; (iv) remove, or in any way alter or obscure, any copyright notice or other notice of Motorola Solutions’ proprietary rights; (v) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by any third party or on any machine except as expressly authorized by this Agreement; or (vi) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software solely by activating a machine containing the Software. End-User Customer may make one copy of Software to be used solely for archival, back-up, or disaster recovery purposes; provided that End-User Customer may not operate that copy of the Software at the same time as the original Software is being operated. End-User Customer may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

3.3 Unless otherwise authorized by Motorola Solutions in writing, End-User Customer will not, and will not enable or allow any third party to: (i) install a licensed copy of the Software on more than one unit of a Product; or (ii) copy onto or transfer Software installed in one unit of a Product onto another device.

3.4 If End-User Customer is purchasing Products that require a site license, End-User Customer must purchase a copy of the applicable Software for each site at which End-User Customer uses such Software. End-User Customer may make one additional copy for each computer owned or controlled by End-User Customer at each such site. End-User Customer may temporarily use the Software on portable or laptop computers at other sites. End-User Customer must provide a written list of all sites where End-User Customer uses or intends to use the Software.

#### 4. TRANSFERS

4.1 End-User Customer will not transfer the Software or Documentation to any third party without Motorola Solutions’ prior written consent. Motorola Solutions’ consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this End-User License Agreement.

#### 5. OWNERSHIP AND TITLE

5.1 Motorola Solutions, its licensors, and its suppliers retain all of their proprietary rights in any form in and to the Software and Documentation, including, but not limited to, all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation. No rights are granted to End-User Customer under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to End-User Customer in this End-User License Agreement. All intellectual property developed, originated, or prepared by Motorola Solutions in connection with providing the Software, Products, Documentation or related services remains vested exclusively in Motorola Solutions, and End-User Customer will not have any shared development or other intellectual property rights.

#### 6. CONFIDENTIALITY

6.1 End-User Customer acknowledges that the Software contains valuable proprietary information and trade secrets and that unauthorized dissemination, distribution, modification, reverse engineering, disassembly or other improper use of the Software will result in irreparable harm to Motorola Solutions for which monetary damages would be inadequate. Accordingly, End-User Customer will limit access to the Software to those of its employees and agents who need to use the Software for End-User Customer’s internal business.

#### 7. MAINTENANCE AND SUPPORT

7.1 No maintenance or support is provided under this End-User License Agreement. Maintenance or support, if available, will be provided under a separate Motorola Solutions Software maintenance and support agreement.

## 8. LIMITED WARRANTY AND LIMITATION OF LIABILITY

8.1 Unless otherwise specified in the applicable warranty statement, the Documentation or in any other media at the time of shipment of the Software by Motorola Solutions, and for the warranty period specified therein, for the first 120 days after initial shipment of the Software to the End-User Customer, Motorola Solutions warrants that the Software, when installed and/or used properly, will be free from reproducible defects that materially vary from its published specifications. Motorola Solutions does not warrant that End-User Customer's use of the Software or the Products will be uninterrupted or error-free or that the Software or the Products will meet End-User Customer's particular requirements.

8.2 MOTOROLA SOLUTIONS' TOTAL LIABILITY, AND END-USER CUSTOMER'S SOLE REMEDY, FOR ANY BREACH OF THIS WARRANTY WILL BE LIMITED TO, AT MOTOROLA SOLUTIONS' OPTION, REPAIR OR REPLACEMENT OF THE SOFTWARE OR PAYMENT OF END-USER CUSTOMER'S ACTUAL DAMAGES UP TO THE AMOUNT PAID TO MOTOROLA SOLUTIONS FOR THE SOFTWARE OR THE INDIVIDUAL PRODUCT IN WHICH THE SOFTWARE IS EMBEDDED OR FOR WHICH IT WAS PROVIDED. THIS WARRANTY EXTENDS ONLY TO THE FIRST END-USER CUSTOMER; SUBSEQUENT TRANSFEREES MUST ACCEPT THE SOFTWARE "AS IS" AND WITH NO WARRANTIES OF ANY KIND. MOTOROLA SOLUTIONS DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

8.3 IN NO EVENT WILL MOTOROLA SOLUTIONS BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF USE, TIME OR DATA, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS, OR SAVINGS, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIMITATIONS IN THIS PARAGRAPH WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

## 9. TERM AND TERMINATION

9.1 Any use of the Software, including but not limited to use on the Products, will constitute End-User Customer's agreement to this End-User License Agreement. End-User Customer's right to use the Software will continue for the life of the Products with which or for which the Software and Documentation have been provided by Motorola Solutions, unless End-User Customer breaches this End-User License Agreement, in which case this End-User License Agreement and End-User Customer's right to use the Software and Documentation may be terminated immediately by Motorola Solutions. In addition, if Motorola Solutions reasonably believes that End-User Customer intends to breach this End-User License Agreement Motorola Solutions may, by notice to End-User Customer, terminate End-User Customer's right to use the Software.

9.2 Upon termination, Motorola Solutions will be entitled to immediate injunctive relief without proving damages and, unless End-User Customer is a sovereign government entity, Motorola Solutions will have the right to repossess all copies of the Software in End-User Customer's possession. Within thirty (30) days after termination of End-User Customer's right to use the Software, End-User Customer must certify in writing to Motorola Solutions that all copies of such Software have been returned to Motorola Solutions or destroyed.

## 10. UNITED STATES GOVERNMENT LICENSING PROVISIONS

10.1 This Section applies if End-User Customer is the United States Government or a United States Government agency. End-User Customer's use, duplication or disclosure of the Software and Documentation under Motorola Solutions' copyrights or trade secret rights is subject to the restrictions set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless they are being provided to the Department of Defense. If the Software and Documentation are being provided to the Department of Defense, End-User Customer's use, duplication, or disclosure of the Software and Documentation is subject to the restricted rights set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. The Software and Documentation may or may not include a Restricted Rights notice, or other notice referring to this End-User License Agreement. The provisions of this End-User License Agreement will continue to apply, but only to the extent that they are consistent with the rights provided to the End-User Customer under the provisions of the FAR and DFARS mentioned above, as applicable to the particular procuring agency and procurement transaction.

## 11. GENERAL

- 11.1 Copyright Notices. The existence of a copyright notice on the Software will not be construed as an admission or presumption that public disclosure of the Software or any trade secrets associated with the Software has occurred.
- 11.2 Compliance with Laws. End-User Customer acknowledges that the Software is subject to the laws and regulations of the United States and End-User Customer will comply with all applicable laws and regulations, including export laws and regulations of the United States. End-User Customer will not, without the prior authorization of Motorola Solutions and the appropriate governmental authority of the United States, in any form export or re-export, sell or resell, ship or reship, or divert, through direct or indirect means, any item or technical data or direct or indirect products sold or otherwise furnished to any person within any territory for which the United States Government or any of its agencies at the time of the action, requires an export license or other governmental approval. Violation of this provision is a material breach of this Agreement.
- 11.3 Third Party Beneficiaries. This End-User License Agreement is entered into solely for the benefit of Motorola Solutions and End-User Customer. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this End-User License Agreement. Notwithstanding the foregoing, any licensor or supplier of third party software included in the Software will be a direct and intended third party beneficiary of this End-User License Agreement.
- 11.4 Waiver. No waiver of a right or remedy of a Party will constitute a waiver of another right or remedy of that Party.
- 11.5 Assignments. Motorola Solutions may assign any of its rights or sub-contract any of its obligations under this End-User License Agreement or encumber or sell any of its rights in any Software, without prior notice to or consent of End-User Customer.
- 11.6 Causes of Action. End-User Customer must bring any action under this End-User License Agreement within one year after the cause of action arises except that warranty claims must be brought within the applicable warranty period.
- 11.7 Entire Agreement and Amendment. This End-User License Agreement contains the parties' entire agreement regarding End-User Customer's use of the Software and may be amended only in a writing signed by both parties, except that Motorola Solutions may modify this End-User License Agreement as necessary to comply with applicable laws and regulations.
- 11.8 Governing Law. This End-User License Agreement is governed by the laws of the State of Delaware in the United States to the extent that they apply and otherwise by the internal substantive laws of the country to which the Software is shipped if End-User Customer is a sovereign governmental entity. The terms of the U.N. Convention on Contracts for the International Sale of Goods do not apply. In the event that the Uniform Computer Information Transaction Act, any version of this Act, or a substantially similar law (collectively "UCITA") becomes applicable to a Party's performance under this Agreement, UCITA does not govern any aspect of this End-User License Agreement or any license granted under this End-User License Agreement, or any of the parties' rights or obligations under this End-User License Agreement. The governing law will be that in effect prior to the applicability of UCITA.
- 11.9 Dispute Resolution. Unless End-User Customer is a sovereign governmental entity, any dispute arising from or in connection with this End-User License Agreement shall be submitted to the sole and exclusive forum of the state and federal courts sitting in New Castle County, Delaware (the "Delaware Courts"), and each Party irrevocably submits to the jurisdiction of the Delaware Courts for the litigation of such disputes. Each Party hereby irrevocably waives, and agrees not to assert in any suit, action or proceeding brought in the Delaware Courts, any claim or defense that the Party is not subject to the jurisdiction of the Delaware Courts, that the Delaware Courts are an inconvenient forum, or that the Delaware Courts are an improper venue.



# CHAPTER 1

## OVERVIEW

Motorola Solutions' family of access points enable high performance with secure and resilient wireless voice and data services to remote locations with the scalability required to meet the needs of large distributed enterprises.

The unique WiNG 5 software enables the access point to function as a Standalone "thick" access point, or a Virtual Controller AP capable of adopting and managing up to 24 access points of the same model. For a complete list of access points supporting WiNG 5 software, see [About this Guide on page 1](#).



**NOTE:** ES6510 is an *Ethernet Switch* managed by a wireless controller such as RFS4000/RFS6000/RFS7000/NX4500/NX4524/NX6500/NX6524/NX7500/NX9000/NX9500/NX9510s. ES6510 does not have radios and does not provide WLAN support.

---

When deploying an access point as a pure Virtual Controller AP, with no RFS Series controllers available anywhere on the network, the access point itself is a controller supporting other access points of the same model. The Virtual Controller AP can:

- Provide firmware upgrades for connected access point
- Aggregate statistics for the group of access points the Virtual Controller is managing
- Be the single point of configuration for that deployment location



**NOTE:** The recommended way to administer a network populated by numerous access points is to configure them directly from the Virtual Controller AP. If a single access point configuration requires an update from the Virtual Controller AP's assigned profile configuration, the administrator should apply a Device Override to change just that access point's configuration. For more information on applying an override to an access point's Virtual Controller AP assigned configuration and profile, see [Device Overrides on page 5-195](#).

---

The WiNG 5 architecture is a solution designed for 802.11n networking. It leverages the best aspects of independent and dependent architectures to create a smart network that meets the connectivity, quality and security needs of each user and their applications, based on the availability of network resources including wired networks. By distributing intelligence and control amongst access points, a WiNG 5 network can route directly via the best path, as determined by factors including the user, location, the application and available wireless and wired resources. WiNG 5 extends the differentiation Motorola Solutions offer to the next level, by making available services and security at every point in the network. managed traffic flow

---

is optimized to prevent wired congestion and wireless congestion. Traffic flows dynamically, based on user and application, and finds alternate routes to work around network choke points.



**NOTE:** This guide describes the installation and use of the WiNG 5 software designed specifically for access points that support this release and ES6510 model ethernet switch. It does not describe the version of the WiNG 5 software designed for use with the RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX7500, NX9000, NX9500 and NX9510. For information on using WiNG 5 in a controller managed network, go to:

<https://portal.motorolasolutions.com/Support/US-EN/Wireless+Networks>

For a complete list of supported access points, see [About this Guide on page 1](#).

---

---

WiNG Express is a minimal version of the WiNG 5 user interface for use on AP6511, AP6521, AP6522 and AP75XX access points. WiNG Express presents a minimum set of configuration options for each of the above access points enabling quick deployment with a large set of default values.

## 1.1 About the Motorola Solutions WiNG 5 Software

The WiNG 5 architecture is a solution designed for 802.11n networking. It leverages the best aspects of independent and dependent architectures to create a smart network that meets the connectivity, quality and security needs of each user and their applications, based on the availability of network resources including wired networks. By distributing intelligence and control amongst access points, a WiNG 5 network can route directly via the best path, as determined by factors including the user, location, the application and available wireless and wired resources. WiNG 5 extends the differentiation Motorola Solutions offer to the next level, by making available services and security at every point in the network. Access point managed traffic flow is optimized to prevent wired congestion and wireless congestion. Traffic flows dynamically, based on user and application, and finds alternate routes to work around network choke points.

With this latest WiNG 5 release, the network can use access points to adapt to the dynamic circumstances of their deployment environment. The WiNG 5 architecture provides a customized site-specific deployment, supporting the best path and routes based on the user, location, application and the best route available (both wireless and wired). A WiNG 5 access point managed network assures end-to-end quality, reliability and security without latency and performance degradation. A WiNG 5 access point managed network supports rapid application delivery, mixed-media application optimization and quality assurance.

Deploying a new WiNG 5 access point managed network does not require the replacement of existing Motorola Solutions access points. WiNG 5 enables the simultaneous use of existing architectures from Motorola Solutions and other vendors, even if those other architectures are centralized models. A wireless network administrator can retain and optimize legacy infrastructure while evolving to WiNG 5 as needed.

By distributing intelligence and control amongst access points, a WiNG 5 network can route data directly using the best path. As a result, the additional load placed on the wired network from 802.11n support is significantly reduced, as traffic does not require an unnecessary backhaul.

Within a WiNG 5 network, up to 80% of the network traffic can remain on the wireless mesh, and never touch the wired network, so the 802.11n load impact on the wired network is negligible. In addition, latency and associated costs are reduced while reliability and scalability are increased. A WiNG 5 network enables the creation of dynamic wireless traffic flows, so bottlenecks can be avoided, and the destination is reached without latency or performance degradation. This behavior delivers a significantly better quality of experience for the end user.

The same distributed intelligence enables more resilience and survivability, since access points keep users connected and traffic flowing with full QoS, security and mobility even if a connection is interrupted due to a wired network or backhaul problem.

When the network is fully operational, sources of interference or unbalanced wireless network loading can be automatically corrected by the access point's Smart RF functionality. Smart RF senses interference or potential client connectivity problems and makes the required changes to the channel and access point radio power while minimizing the impact to latency sensitive applications like VoIP. Using Smart RF, the network can continuously adjust power and channel assignments for self-recovery if an access point radio fails or a coverage hole is detected.

Additionally, integrated access point sensors, in conjunction with AirDefense Network Assurance, alerts administrators of interference and network coverage problems, which shortens response times and boosts overall reliability and availability of the access point managed network.

Network traffic optimization protects the network from broadcast storms and minimizes congestion on the wired network. The access point managed network provides VLAN load balancing, WAN traffic shaping and optimizations in *dynamic host configuration protocol* (DHCP) responses and *Internet group management protocol* (IGMP) snooping for multicast traffic flows in wired and wireless networks. Thus, users benefit from an extremely reliable network that adapts to meet their needs and delivers mixed-media applications.

Firmware and configuration updates are supported from one access point to another, over the air or wire, and can be centrally managed by an access point in Virtual Controller AP mode. Controllers no longer need to push firmware and configurations to individual access point, thus reducing unnecessary network congestion.



# CHAPTER 2

## WEB USER INTERFACE FEATURES

The access point's resident user interface contains a set of features specifically designed to enable either Virtual Controller AP, Standalone AP or Adopt to Controller functionality. In Virtual Controller AP mode, an access point can manage up to 24 other access points of the same model and share data amongst managed access points. In Standalone mode, an access point functions as an autonomous, non adopted, access point servicing wireless clients. If adopted to controller, an access point is reliant on its connected controller for its configuration and management.

For information on how to access and use the access point's Web UI, see:

- [Accessing the Web UI](#)
- [Icon Glossary](#)

## 2.1 Accessing the Web UI

The access point uses a *Graphical User Interface* (GUI) which can be accessed using any supported Web browser on a client connected to the subnet the Web UI is configured on.

### 2.1.1 Browser and System Requirements

To access the GUI, a browser supporting Flash Player 11 is recommended. The system accessing the GUI should have a minimum of 1 GB of RAM for the UI to display and function properly. The Web UI is based on Flex, and does not use Java as the underlying UI framework. Motorola Solutions recommends using a resolution of 1280 x 1024 pixels for using the GUI.

The following browsers have been validated with the Web UI:

- Firefox 3.0 or higher
- Internet Explorer 7 or higher
- Google Chrome 2.0 or higher
- Safari 3 and higher
- Opera 9.5 and higher

### 2.1.2 Connecting to the Web UI

1. Connect one end of an Ethernet cable to an access point LAN port and connect the other end to a computer with a working Web browser.
2. Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet/network mask of 255.255.255.0.



**NOTE:** The access point's IP address is optimally provided using DHCP. A zero config IP address can also be derived if DHCP resources are unavailable. Using zero config, the last two octets in the IP address are the decimal equivalent of the last two bytes in the access point's hardcoded MAC address.

For example:

MAC address - 00:C0:23:00:F0:0A  
Zero-config IP address - 169.254.240.10

---

---

3. To derive the access point's IP address using its MAC address:
4. Open the Windows calculator by selecting **Start > All Programs > Accessories > Calculator**. This menu path may vary slightly depending on your version of Windows.
5. With the Calculator displayed, select **View > Scientific**. Select the **Hex** radio button.
6. Enter a hex byte of the access point's MAC address. For example, *F0*.
7. Select the **Dec** radio button. The calculator converts *F0* into *240*. Repeat this process for the last access point MAC address octet.
8. Once obtained, point the Web browser to the access point's IP address. The following login screen displays:



**Figure 2-1** Access Point Web UI Login screen

9. Enter the default username *admin* in the **Username** field.
10. Enter the default password *motorola* in the **Password** field.
11. Select the **Login** button to load the management interface.

If this is the first time the management interface has been accessed, the first screen to display will prompt for a change of the default access point password. Then, a dialogue displays to start the initial setup wizard. For more information on using the initial setup wizard see [Using the WiNG Initial Setup Wizard on page 3-2](#).

## 2.2 Icon Glossary

The access point interface utilizes a number of icons designed to interact with the system, gather information from managed devices and obtain status. This chapter is a compendium of the icons used, and is organized as follows:

- [Global Icons](#)
- [Dialog Box Icons](#)
- [Table Icons](#)
- [Status Icons](#)
- [Configurable Objects](#)
- [Configuration Objects](#)
- [Configuration Operation Icons](#)
- [Access Type Icons](#)
- [Administrative Role Icons](#)
- [Device Icons](#)

### 2.2.1 Global Icons

#### ► [Icon Glossary](#)

This section lists global icons available throughout the interface.



*Logout* – Select this icon to log out of the system. This icon is always available and is located at the top right-hand corner of the UI.



*Add* – Select this icon to add a row in a table. When this icon is selected, a new row is created in the table, or a dialog box opens where you can enter values for that particular list.



*Delete* – Select this icon to remove a row from a table. When this icon is clicked, the selected row is immediately deleted.



*More Information* – Select this icon to display a pop-up with supplementary information that may be available for an item.



*Trash* – Select this icon to remove a row from a table. When this icon is clicked, the selected row is immediately deleted.



*Create new policy*— Select this icon to create a new policy. Policies define different configuration parameters that can be applied to device configurations, and device profiles.



*Edit policy*— Select this icon to edit an existing configuration item or policy. To edit a policy, select the policy and this icon.

## 2.2.2 Dialog Box Icons

### ► [Icon Glossary](#)

These icons indicate the current state of various controls in a dialog. These icons enables you to gather, at a glance, the status of all the controls in a dialog. The absence of any of these icons next to a control indicates the value in that control has not been modified from its last saved configuration.



*Entry Updated*— Indicates a value has been modified from its last saved configuration.



*Entry Update*— States that an override has been applied to a device's profile configuration.



*Mandatory Field*— Indicates the control's value is a mandatory configuration item. You will not be allowed to proceed further without providing all mandatory values in the dialog or the screen.



*Error in Entry*— Indicates there is an error in a supplied value. A small red popup provides a likely cause of the error.

## 2.2.3 Table Icons

### ► [Icon Glossary](#)

The following two override icons are status indicators for transactions that need to be committed.



*Table Row Overridden*— Indicates a change (profile configuration override) has been made to a table row, and the change will not be implemented until saved. This icon represents a change from this device's profile assigned configuration.



*Table Row Added*— Indicates a new row has been added to a table, and the change will not be implemented until saved. This icon represents a change from this device's profile assigned configuration.

## 2.2.4 Status Icons

### ► [Icon Glossary](#)

These icons define device status, operations on the wireless controller, or any other action that requires a status being returned to the user.



*Fatal Error* – States there is an error causing a managed device to stop functioning.



*Error* – Indicates an error exists requiring intervention. An action has failed, but the error is not system wide.



*Warning* – States a particular action has completed, but some errors were detected that did not stop the process from completing. Intervention might still be required to resolve subsequent warnings.



*Success* – Indicates everything is well within the network or a process has completed successfully without error.



*Information* – This icon always precedes information displayed to the user. This may either be a message displaying progress for a particular process, or may just be a message from the system.

## 2.2.5 Configurable Objects

### ► [Icon Glossary](#)

These icons define configurable items within the UI.



*Device Configuration* – Represents a configuration file applicable to a device category.



*Auto Provisioning Policy* – Represents a provisioning policy. Provisioning policies are a set of configuration parameters that define how Access Points and wireless clients are adopted and their management configuration supplied.



*Wireless LANs* – States an action impacting a WLAN has occurred.



*WLAN QoS Policy* – States a *Quality of Service* (QoS) policy configuration has been impacted.



*Radio QoS Policy* – Indicates a QoS policy configuration has been impacted.



*AAA Policy* – Indicates an *Authentication, Authorization and Accounting* (AAA) policy has been impacted. AAA policies define RADIUS authentication and accounting parameters.



*Association ACL* – Indicates an *Association Access Control List* (ACL) configuration has been impacted. An ACL is a set of configuration parameters used to set access to managed resources. The association ACL configures the parameters for controlling device associations.



*Smart RF Policy* – States a Smart RF policy has been impacted. Smart RF enables neighboring APs to take over for an AP that suddenly becomes unavailable. This is accomplished by increasing the power of radios on nearby APs to cover the hole created by the non-functioning AP.



*Profile* – States a device profile configuration has been impacted. A profile is a collection of configuration parameters used to configure a device or a feature.



*Bridging Policy* – Indicates a bridging policy configuration has been impacted. A bridging policy defines which VLANs are bridged and how local VLANs are bridged between the wired and wireless sides of the network.



*RF Domain* – States an RF Domain configuration has been impacted. RF Domain implement location based security restrictions applicable to all VLANs in a particular physical location.



*Firewall Policy* – Indicates a Firewall policy has been impacted. Firewalls provide a barrier that prevent unauthorized access to secure resources while allowing authorized access to external and internal resources.



*IP Firewall Rules* – Indicates an IP Firewall rule has been applied. An IP based firewall rule implements firewall restrictions based on the IP address in a received packet.



*MAC Firewall Rules* – States a MAC based Firewall Rule has been applied. A MAC based firewall rule implements firewall restrictions based on the MAC address in a received packet.



*Wireless Client Role* – Indicates a wireless client role has been applied to a managed client. The role could be either sensor or client.



*WIPS Policy* – States the conditions of a WIPS policy have been invoked. WIPS prevents unauthorized access to the network by checking for (and removing) rogue APs and wireless clients.



*Advanced WIPS Policy* – States the conditions of an advanced WIPS policy have been invoked. WIPS prevents unauthorized access to the system by checking for and removing rogue access points and wireless clients.



*Device Categorization* – Indicates a device categorization policy is being applied. This is used by the intrusion prevention system to categorize APs or wireless clients as either neighbors or sanctioned devices. This enables these devices to bypass the intrusion prevention system.



*Captive Portal* – States a captive portal is being applied. Captive portal is used to provide temporary controller, service platform, or access point access to requesting wireless clients.



*DNS Whitelist* – A DNS whitelist is used in conjunction with captive portal to provide captive portal services to wireless clients.



*DHCP Server Policy* – Indicates a DHCP server policy is being applied. DHCP provides IP addresses to wireless clients. A DHCP server policy configures how DHCP provides these IP addresses.



*RADIUS Group* – Indicates the configuration of RADIUS Group is being defined and applied. A RADIUS group is a collection of RADIUS users with the same set of permissions.



*RADIUS User Pools* – States a RADIUS user pool is being applied. RADIUS user pools are a set of IP addresses that can be assigned to an authenticated RADIUS user.



*RADIUS Server Policy* – Indicates a RADIUS server policy is being applied. RADIUS server policy is a set of configuration attributes used when a RADIUS server is configured for AAA.



*Smart Caching Policy* – Smart Caching enables NX4500 and NX6500 series service platforms to temporarily store frequently accessed Web content on network infrastructure devices.



*Management Policy* – Indicates a management policy is being applied. Management policies are used to configure access control, authentication, traps and administrator permissions.



*MeshConnex Policy* – Indicates a mesh connex policy is being applied. MeshConnex is a hybrid proactive/on-demand path selection protocol to form efficient mesh paths.



*Mesh QoS Policy*— Indicates a mesh quality of service policy is being applied. This policy ensures that each mesh point in the network receives a fair share of overall bandwidth for its use.



*Virtual Controller APs*— Indicates an AP is configured as a Virtual Controller access point. A Virtual Controller access point can manage up to 24 access points of similar type deployed in a network.

## 2.2.6 Configuration Objects

### ► [Icon Glossary](#)

Configuration icons are used to define the following:



*Configuration*— Indicates an item capable of being configured by the access point's interface.



*View Events / Event History*— Defines a list of events. Select this icon to view events or view the event history.



*Core Snapshots*— Indicates a core snapshot has been generated. A core snapshot is a file that records the status of all the processes and memory when a process fails.



*Panic Snapshots*— Indicates a panic snapshot has been generated. A panic snapshot is a file that records the status of all the processes and memory when a failure occurs.



*UI Debugging*— Select this icon/link to view current NETCONF messages.



*View UI Logs*— Select this icon/link to view the different logs generated by the user interface, FLEX and the error logs.

## 2.2.7 Configuration Operation Icons

### ► [Icon Glossary](#)

The following icons are used to define configuration operations:



*Revert* – When selected, any unsaved changes are reverted back to their last saved configuration.



*Commit* – When selected, all changes made to the configuration are written to the access point. Once committed, changes cannot be reverted.



*Commit and Save* – When selected, changes are saved to the access point's configuration.

## 2.2.8 Access Type Icons

### ► [Icon Glossary](#)

The following icons display a user access type:



*Web UI* – Defines a Web UI access permission. A user with this permission is permitted to access an associated device's Web UI.



*Telnet* – Defines a TELNET access permission. A user with this permission is permitted to access an access point using TELNET.



*SSH* – Indicates a SSH access permission. A user with this permission is permitted to access an access point using SSH.



*Console* – Indicates a console access permission. A user with this permission is permitted to access the access point using the device's serial console.

## 2.2.9 Administrative Role Icons

### ► [Icon Glossary](#)

The following icons identify the different administrative roles allowed on the system:



*Superuser* – Indicates superuser privileges. A superuser has complete access to all configuration aspects of the access point to which they are connected.



*System* – Indicates system user privileges. A system user is allowed to configure some general settings like boot parameters, licenses, auto install, image upgrades etc.



*Network* – Indicates network user privileges. A network user is allowed to configure all wired and wireless parameters, like IP configuration, VLANs, L2/L3 security, WLANs, radios etc.



*Security* – Indicates security user privileges. A security level user is allowed to configure all security related parameters.



*Monitor* – Indicates a monitor role. This role provides no configuration privileges. A user with this role can view all system configuration but cannot modify them.



*Help Desk* – Indicates help desk privileges. A help desk user is allowed to use troubleshooting tools like sniffers, execute service commands, view or retrieve logs and reboot an access point.



*Web User* – Indicates a Web user privilege. A Web user is allowed accessing the access point's Web user interface.

## 2.2.10 Device Icons

### ► [Icon Glossary](#)

The following icons indicate the different device types managed by the system:



*System* – This icon indicates the entire WiNG supported system and all of its members including wireless controller, service platforms, and access points that may be interacting at any one time.



*Cluster* – This icon indicates a cluster. A cluster is a set of access points that work collectively to provide redundancy and load sharing amongst its members.



*Service Platform* – This icon indicates an NX45xx, NX65xx, NX7500 or NX9000 series service platform that's part of the managed network



*RF Domain* - This icon indicates a RF Domain. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, a building or a site. Each RF Domain also contains policies that can determine a Smart RF or WIPS configuration.



*Access Point* – This icon indicates any access point that is a part of the network.



*Wireless Client* – This icon indicates any wireless client connected within the access point managed network.

# CHAPTER 3

## QUICK START

Access points can utilize an initial setup wizard to streamline the process of initially accessing the wireless network. The wizard defines the access point's operational mode, deployment location, basic security, network and WLAN settings. For instructions on how to use the initial setup wizard, see [Using the WiNG Initial Setup Wizard on page 3-2](#).

This section describes, in detail, the initial setup steps for the AP SKUs running the standard WiNG build as well for those SKUs running the WiNG Express build. For more information see:

- [Using the WiNG Initial Setup Wizard](#)
- [Using WiNG Express Quick Configuration](#)

## 3.1 Using the WiNG Initial Setup Wizard

### ► Quick Start

Once the access point is installed and powered on, complete the following steps to get the access point up and running and access management functions:

1. Point the Web browser to the access point's IP address. The following login screen displays:



**Figure 3-1** Web UI Login screen

2. Enter the default username **admin** in the **Username** field.
3. Enter the default password **motorola** in the **Password** field.
4. Select the **Login** button to load the management interface.

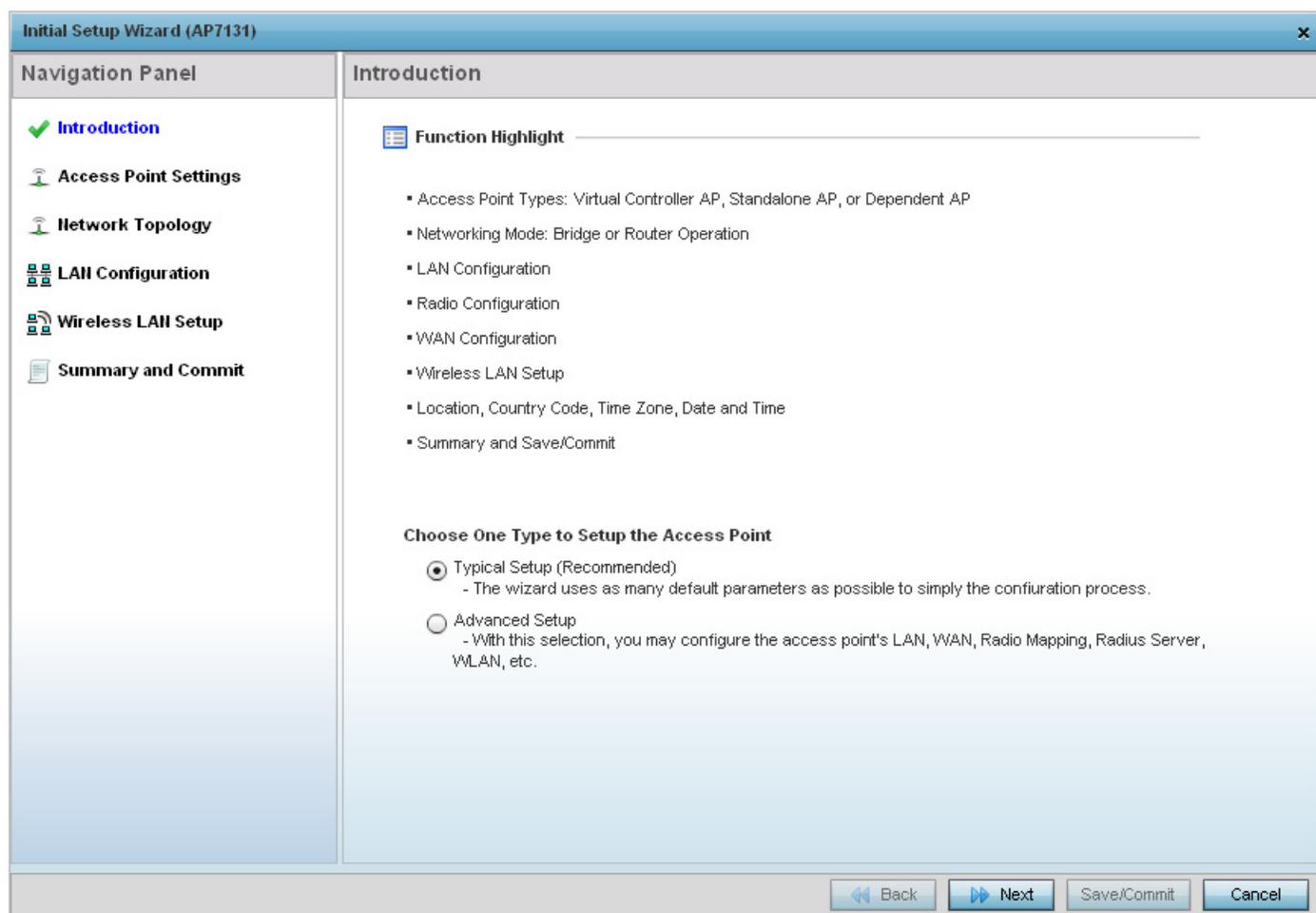


**NOTE:** When logging in for the first time, you are prompted to change the password to enhance device security in subsequent logins.



**NOTE:** If you get disconnected when running the wizard, you can connect again with the access point's actual IP address (once obtained) and resume the wizard.

5. If this is the first time the access point's management interface has been accessed, the **Initial Setup Wizard** automatically displays.
-



**Figure 3-2** Initial Setup Wizard



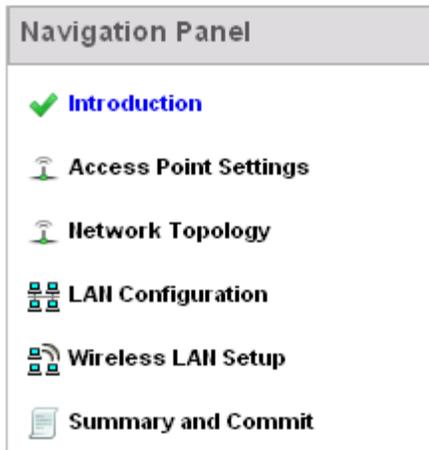
**NOTE:** The Initial Setup Wizard displays the same pages and content for each access point model supported. The only difference being the number of radios configurable by model, as an AP7131 model can support up to three radios, AP6522, AP6532, AP6562, AP7522, AP7532, AP8122, AP8132, AP8222, AP8232, AP7161 and AP7181 models support two radios and AP6511 and AP6521 models support a single radio.

The **Introduction** screen displays the various actions that can be performed using the wizard under the **Function Highlight** field.

Use the **Choose One type to Setup the Access Point** field options to select the type of wizard to run. The **Typical Setup** is the recommended wizard. This wizard uses the default parameters for most of the configuration parameters and sets up a working network with the least amount of manual configuration.

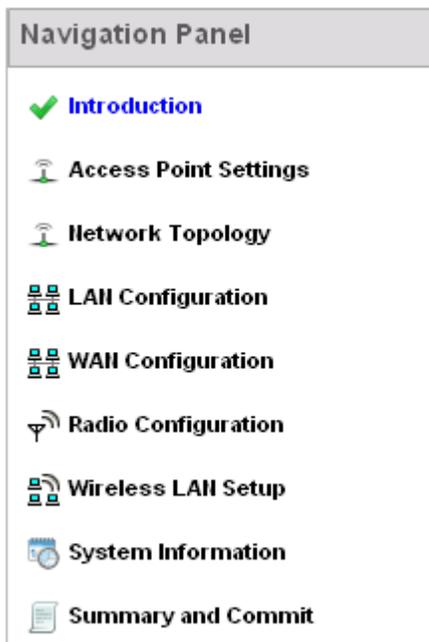
The **Advanced Setup** wizard is for administrators who prefer more control over the different configuration parameters. A few more configuration screens are available for customization when the **Advanced Setup** wizard is used.

The first page of the *Initial Setup Wizard* displays the **Navigation Panel** and **Function Highlights** for the configuration activities comprising the access point's initial setup. This page also displays options to select the typical or advanced mode for the wizard.



**Figure 3-3** Initial Setup Wizard - Navigation Panel - Typical Setup Wizard

A green check mark to the left of an item in the **Navigation Panel** defines the listed task as having its minimum required configuration parameters set correctly. A red X defines the task as still requiring at least one parameter be defined correctly. [Figure 3-3](#) displays the navigation panel for the **Typical Setup Wizard**.



**Figure 3-4** Initial Setup Wizard - Navigation Panel - Advanced Setup Wizard

[Figure 3-4](#) displays the navigation panel for the **Advanced Setup Wizard**.



**NOTE:** Note the difference in the number of steps between the Typical Setup and Advanced Setup Wizards.

---

6. Select **Save/Commit** within each page to save the updates made to that page's configuration. Select **Next** to proceed to the next page listed in the **Navigation Panel**. Select **Back** to revert to the previous screen without saving your updates.
- 
- 



**NOTE:** While you can navigate to any page in the navigation panel, you cannot complete the *Initial Setup Wizard* until each task in the *Navigation Panel* has a green check mark.

---

---

The following sections describe the two different wizards and their parameters. The available wizards are:

- [Typical Setup Wizard](#)
- [Advanced Setup Wizard](#)

### 3.1.1 Typical Setup Wizard

#### ▶ [Using the WiNG Initial Setup Wizard](#)

The **Typical Setup** is the recommended wizard. This wizard uses default parameters for most of the configuration parameters and creates a working network with the fewest steps.

The **Typical Setup** wizard consists of the following:

- [Network Topology Selection](#)
- [LAN Configuration](#)
- [WAN Configuration](#)
- [Wireless LAN Setup](#)
- [Summary And Commit Screen](#)

To configure the access point using the **Typical Setup Wizard**:

1. Select **Typical Setup** from the **Choose One type to Setup the Access Point** field.
2. Select **Next**.

The *Initial Setup Wizard* displays the *Access Point Settings* screen to define the access point's Standalone versus Virtual Controller AP functionality. This screen also enables selection of the country of operation for the access point.

---

**Access Point Settings**

**Access Point Type Selection**

Virtual Controller AP - When more than one access point is deployed, a single access point can function as a Virtual Controller AP and manage Dependent mode access points. The Virtual Controller AP can adopt and configure other like APs in a 24-cell deployment.

Standalone AP - Select this option to deploy this access point as an autonomous "fat" access point. A standalone AP isn't managed by a Virtual Controller AP, or adopted by a controller.

Country

◀ Back   Next ▶   Save/Commit   Cancel

**Figure 3-5** Initial Setup Wizard - Access Point Settings screen for Typical Setup Wizard

3. Select an **Access Point Type** from the following options:
  - *Virtual Controller AP* - When more than one access points are deployed, a single access point can function as a Virtual Controller AP. Up to 24 access points can be connected to, and managed by a single Virtual Controller AP. These connected access points must be the same model as the Virtual Controller AP. For more information, see [Virtual Controller AP Mode on page 3-8](#).
  - *Standalone AP* - Select this option to deploy this access point as an autonomous access point. A standalone AP is not managed by a Virtual Controller AP, or adopted by a RFS series wireless controller. For more information, see [Standalone Mode on page 3-9](#).



**NOTE:** If designating the access point as a Standalone AP, Motorola Solutions recommends the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

- *Adopted to Controller* - Select this option when deploying the access point as a controller managed (Dependent mode) access point. Selecting this option closes the Initial AP Setup Wizard. An adopted access point obtains its configuration from a profile stored on its managing controller. Any manual configuration changes are overwritten by the controller upon reboot. For more information on configuring the access point in the *Adopted to Controller* mode, see [Adopt to a controller on page 3-35](#).



**NOTE:** The option **Adopted to Controller** is only available for the *Advanced Setup Wizard*.

- 
- 
4. Select the **Country Code** where the access point is deployed. Selecting a proper country of operation is a very critical task while configuring the access point as it defines the correct channels of operations and ensures compliance to the regulations for the selected country. This field is only available for the *Typical Setup Wizard*.



**NOTE:** The professional installer should refer to the Motorola Solutions WiNG Access Point System Reference Guide available at

<https://portal.motorolasolutions.com/Support/US-EN/Wireless+Networks>

for detailed information on how to set the access point's transmit power, antenna gain and channel in respect to the deployment country's unique regulatory requirements.

- 
- 
5. Select the **Next** button to start configuring the access point in the selected mode.

### 3.1.1.1 Virtual Controller AP Mode

▶ *Using the WiNG Initial Setup Wizard*

When more than one access point is deployed, a single access point can function as a Virtual Controller AP. Up to 24 access points can be connected to, and managed by a single Virtual Controller AP of the same access point model. These connected access points must be of the same model as the Virtual Controller AP.

To designate an access point as a Virtual Controller AP:

1. From the *Access Point Settings* screen, select **Virtual Controller AP**.
2. Select **Next**.

The remainder of a Virtual Controller AP configuration is the same as a Standalone Access Point.

### 3.1.1.2 Standalone Mode

▶ *Using the WiNG Initial Setup Wizard*

In the *Standalone* mode, the access point is not adopted to a wireless controller. Select this option to deploy this access point as an autonomous fat access point.



**CAUTION:** If designating the access point as a Standalone AP, Motorola Solutions recommends the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

---

---

To configure the access point to work in the *Standalone* mode:

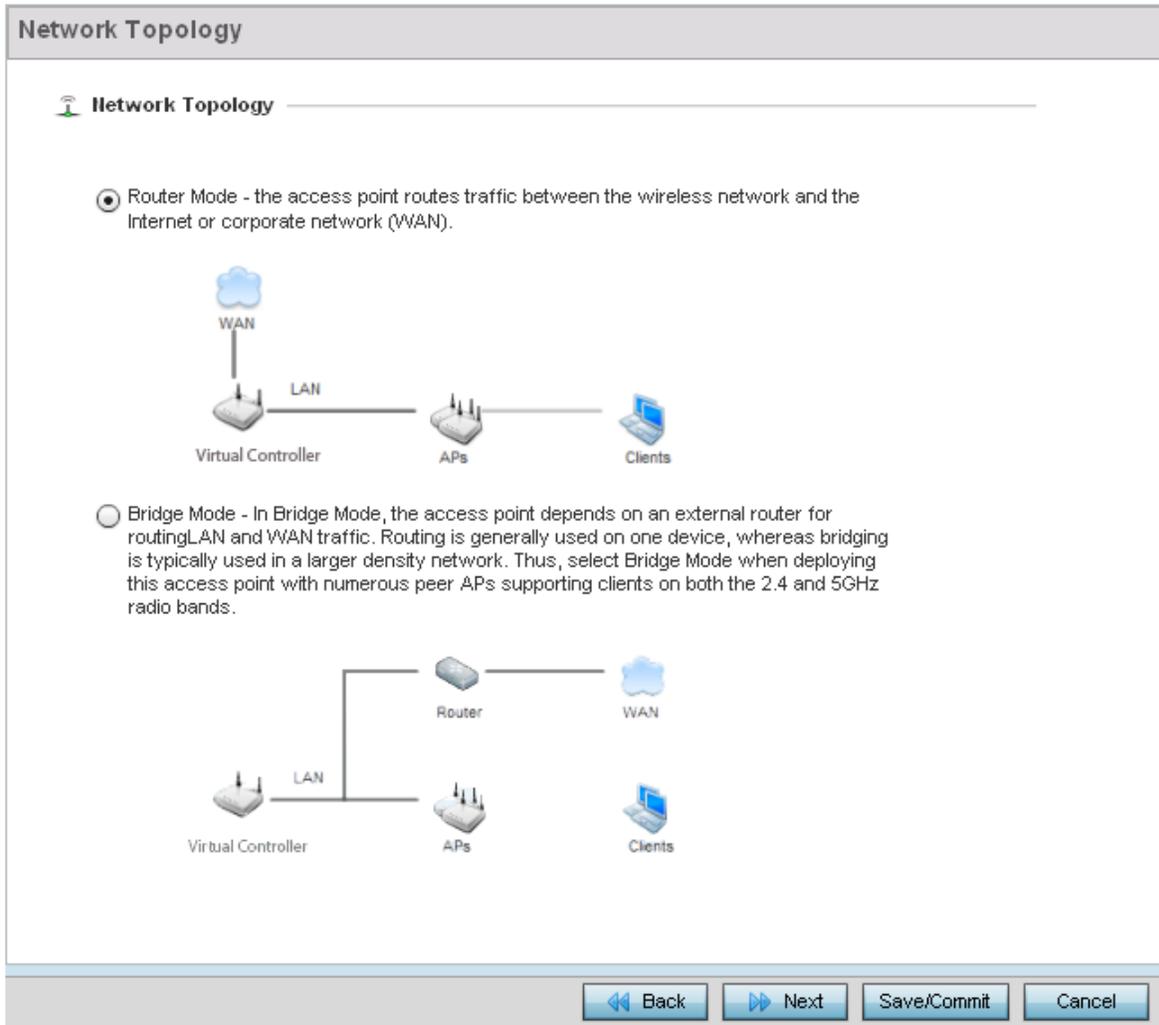
1. From the *Access Point Settings* screen, select **Standalone AP**.
2. Select **Next**.

The remainder of a Standalone AP configuration is the same as a Virtual Controller Access Point.

### 3.1.1.3 Network Topology Selection

#### ► *Typical Setup Wizard*

Use the *Network Topology* screen to define how the access point manages network traffic. The available modes are:



**Figure 3-6** *Initial Setup Wizard - Network Topology screen for Typical Setup Wizard*

- **Router Mode** - In Router Mode, the access point routes traffic between the *local network* (LAN) and the Internet or *external network* (WAN). Router mode is recommended in a deployment supported by just a single access point.
- **Bridge Mode** - In Bridge Mode, the access point depends on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger density network. Select *Bridge Mode* when deploying this access point with numerous peer access points supporting clients on both the 2.4 GHz and 5.0 GHz radio bands.



**NOTE:** When *Bridge Mode* is selected, WAN configuration cannot be performed and the *Initial Setup Wizard* does not display the WAN configuration screen.

1. Select **Next**. The *Typical Setup Wizard* displays the **LAN Configuration** screen to set the access point's LAN interface configuration. For more information, see [LAN Configuration on page 3-11](#).

### 3.1.1.4 LAN Configuration

#### ▶ Typical Setup Wizard

Use the *LAN Configuration* screen to set the access point's DHCP and LAN network address configuration.

**LAN Configuration**

**LAN Configuration**

Please configure interface settings for LAN (VLAN 1) which will be used by wireless clients

Use DHCP [What is this?](#)

Static IP Address/Subnet [What is this?](#) 192.168.13.23 / 24 \*

**DHCP Server**

Use on-board DHCP server to assign IP addresses to wireless clients

Range 192.168.0.100 -- 192.168.0.200

Default Gateway 192.168.0.1

**Domain Name Server (DNS)**

DNS Forwarding

Primary DNS . . . Secondary DNS . . .

Back Next Save/Commit Cancel

**Figure 3-7** Initial Setup Wizard - LAN Configuration screen for Typical Setup Wizard

- Set the following DHCP and Static IP Address/Subnet information:
  - Use DHCP** - Select the option to enable an automatic network address configuration using DHCP server.
  - Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's LAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **DHCP Server** and **Domain Name Server (DNS)** resources, as those fields will become enabled on the bottom portion of the screen.
    - Use on-board DHCP server to assign IP addresses to wireless clients** - Select the check box to enable the access point's DHCP server to provide IP and DNS information to clients on the LAN interface.
    - Range** - Enter a starting and ending IP Address range for client assignments on the access point's LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.
    - Default Gateway** - Define a default gateway address for use with the default gateway. This is a required parameter.
    - DNS Forwarding** - Select this option to allow a DNS server to translate domain names into IP addresses. If this

option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.

- **Primary DNS** - Enter an IP Address for the main Domain Name Server providing DNS services for the access point's LAN interface.
  - **Secondary DNS** - Enter an IP Address for the backup Domain Name Server providing DNS services for the access point's LAN interface
2. Select **Next**. The *Typical Setup Wizard* displays the *Wireless LAN Setup* screen to set the access point's Wireless LAN interface configuration. For more information see [Wireless LAN Setup on page 3-15](#).

If *Router Mode* is selected as the **Network Topology**, the *Typical Setup Wizard* displays the WAN configuration screen. For more information, see [WAN Configuration on page 3-13](#).

---

### 3.1.1.5 WAN Configuration

► [Typical Setup Wizard](#)



**NOTE:** This option is only available when *Router Mode* is selected in the **Network Topology** screen.

Use the **WAN Setting** screen to define network address settings for the WAN interface. The WAN interface connects the access point to a wired local area network or backhaul.

**Figure 3-8** Initial Setup Wizard - WAN Configuration screen of the Typical Setup Wizard

- Set the following WAN parameters:
  - Use DHCP** - Select the radio control to enable an automatic network address configuration using external DHCP servers. An automatic IP address is configured to the access point's WAN port using DHCP servers located on the WAN side of the network.
  - Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's WAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define **Default Gateway** information, as the field will become enabled on the bottom portion of the screen. The provided IP address is assigned to the WAN interface of the access point. The **Default Gateway** is a router that serves as a access to other networks.
  - Select the port that is connected to the WAN** – Select the port connected to the WAN.

- **Enable NAT on the WAN Interface** – Select the option to enable *Network Address Translation* on the selected GE interface.
2. Select **Next**. The *Typical Setup Wizard* displays the **Wireless LAN Setup** screen to set the access point's wireless LAN configuration. For more information, see [Wireless LAN Setup on page 3-15](#).

### 3.1.1.6 Wireless LAN Setup

#### ▶ *Typical Setup Wizard*

A *Wireless Local Area Network* (WLAN) is a data-communications system and local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

Up to two (2) WLANs can be configured for the access point using the wizard.

The screenshot shows the 'Wireless LAN Setup' wizard interface. At the top, there are two tabs: 'WLAN 1' (selected) and 'WLAN 2'. Below the tabs, the 'WLAN 1 Configuration' section is visible. It includes a text input field for 'SSID' containing 'WLA\_01', with a 'What is this?' link and a red asterisk icon to its right. Below the SSID field, there are three radio button options for 'WLAN Type':
 

- No Authentication and No Encryption (with a 'What is this?' link)
- Captive Portal Authentication and No Encryption (with a 'What is this?' link)
- PSK authentication, WPA2 encryption (with a 'What is this?' link)

 At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Save/Commit', and 'Cancel'.

**Figure 3-9** Initial Setup Wizard - Wireless LAN Setup screen for Typical Setup Wizard

1. Set the following WLAN1 configuration parameters:
  - **SSID** – Configure the SSID for the WLAN.
  - **WLAN Type** – Configure the encryption and authentication to use with this WLAN.
    - **No Authentication and No Encryption** – Configures a network without any authentication. This means any device can access the network. This option also configures the network without encryption. This means any data transmitted through the network is in plain text.

- **Captive Portal Authentication and No Encryption** – Configures a network that uses a RADIUS server to authenticate users before allowing them on to the network. Once on the network, no encryption is used for the data being transmitted through the network. Select this option to use a Web page (either internally or externally hosted) to authenticate users before access is granted to the network
    - **External RADIUS Server** – When this option is selected, provide the IP address of the external RADIUS server used for user authentication. Also provide the shared secret in the **RADIUS Shared Secret** field.
    - **Onboard RADIUS Server** – When this option is selected, a new screen is displayed where additional updates can be made. For more information on configuring the onboard RADIUS server, see [RADIUS Server Configuration on page 3-17](#).
  - **PSK authentication, WPA2 encryption** – Configures a network that uses PSK authentication and WPA2 encryption. Select this option to implement a pre-shared key that must be correctly shared between the access point and requesting clients using this WLAN
    - **WPA Key** – Provide a 64 character HEX key or 8-63 character ASCII key. Use the drop-down to specify the type of key being provided. Select *ASCII* or *HEX* to specify the key type being provided in the **WPA Key** field.
2. Select **Next**. The *Typical Setup Wizard* displays the **RADIUS Server Configuration** screen if required. For more information, see [RADIUS Server Configuration on page 3-17](#)

Otherwise, the *Typical Setup Wizard* displays the **Summary and Commit** screen. For more information, see [Summary And Commit Screen on page 3-19](#).



**Figure 3-11** Initial Setup Wizard - RADIUS Server Configuration - Add User screen for Typical Setup Wizard

- Use the **Add User** dialog to provide user information to add to the RADIUS server user database.
  - **Username** – Provide a user name to authenticate the user
  - **Password** – Provide a password to authenticate the user
  - **Confirm Password** – Confirm the password by entering the same password entered in the **Password** field
  - **Description** – Provide a description for the user created in the RADIUS server user database
- To create the user and continue with creating another user, select **Create**. To create the user and close this dialog, click **Create & Close**. To close the dialog and abandon the operation, select **Cancel**.

Use the **Modify User** button to modify the details for an existing user in the RADIUS user database. Select the user to modify details for and then click **Modify User**. The username for the user cannot be modified using this dialog.

Use the **Delete User** button to remove the details of an existing user from the RADIUS user database. Select the user to remove and then click **Delete User**. A confirmation dialog appears. Once confirmed, the user is removed from the RADIUS user database.

- Click **Next** The *Typical Setup Wizard* displays the **Summary and Commit** screen. For more information, see [Summary And Commit Screen on page 3-19](#).

### 3.1.1.7 Summary And Commit Screen

#### ▶ Typical Setup Wizard

The *Summary And Commit* screen displays a complete overview of the configurations made in the previous screens.

There is no user intervention or additional settings required. The *Summary and Commit* screen is an additional means of validating the configuration before it is deployed.

**Summary and Commit**

**Access Point Type Page**

Access Point Type    Standalone AP

**Networking Mode Page**

Networking Mode    Router Mode

**LAN Configuration Page**

LAN Configuration Type    Static IP Address/Subnet

VLAN ID for the LAN Interface    1

Static IP Address/Subnet    192.168.13.23/24

**WAN Configuration Page**

WAN Configuration Type    Use DHCP

Port to External    GE1 Port

**WLAN Configuration**

WLAN1 Configuration

◀ Back    ▶ Next    Save/Commit    Cancel

**Figure 3-12** Initial Setup Wizard - Summary And Commit Screen of the Typical Setup Wizard

If the configuration displays as intended, select the **Save/Commit** button to implement these settings to the access point's configuration. If additional changes are warranted based on the summary, either select the target page from the **Navigation Panel**, or use the **Back** button.

### 3.1.1.8 Adopt to a controller

► *Using the WiNG Initial Setup Wizard*

*Adopted to Controller* is the default behavior of the access point. When the access point is switched on for the first time, it looks for a wireless controller on the default subnet and that runs the same WiNG firmware version and automatically adopts to it. Use the *Initial Setup Wizard* to configure the preferred wireless controller that the access point must adopt to.

When *Adopted to Controller* is selected, further configuration settings are displayed in the same screen. Select the **Automatic controller discovery** option to enable the access point to be discovered and adopted using layer 2 settings.

If preferring layer 3 adoption, select the **Static Controller Configuration** option, and define the addresses of the preferred controllers. When using the static method, define whether the access point receives an IP address using DHCP or if IP resources are provided statically. Up to two (2) controllers can be defined. The access point will try to adopt to the controller defined in the Controller 1 field first. Should the controller not be found, then the access point tries to adopt to the controller defined in Controller 2 field.

When preferring layer 3 adoption, configure how an IP is assigned to this access point. Select **Use DHCP** to use DHCP to assign an IP address to this access point. If this access point requires a static IP to be assigned, select **Static IP Address/Subnet** and provide the appropriate IP address and net mask. For your convenience, the netmask is automatically set to 24. Also assign the **Default Gateway** to forward traffic.

**Adoption Settings**

Automatic controller discovery (L2, DHCP or DNS based)  
 Static Controller Configuration

**Controller 1**  \*      **Controller 2**

Use DHCP     Static IP Address/Subnet     \*

**Default Gateway**  \*

**Figure 3-13** *Initial Setup Wizard - Adoption Settings*

Select the **Save/Commit** button to save the current configuration. Select the **Cancel** button to exit the **Initial Setup Wizard** without making any changes. Select the **Back** button to go back to the previous screen of the *Initial Setup Wizard*.

### 3.1.2 Advanced Setup Wizard

► *Using the WiNG Initial Setup Wizard*

The **Advanced Setup** is the recommended wizard for users who want more control on how the access point is configured beyond minimum default settings. This wizard provides additional radio and system information settings.

The *Advanced Setup* wizard consists of the following:

- *Network Topology Selection*
- *LAN Configuration*
- *WAN Configuration*
- *Radio Configuration*
- *Wireless LAN Setup*
- *System Information*
- *Summary And Commit Screen*

To configure the access point using the *Advanced Setup Wizard*:

1. Select **Advanced Setup** from the **Choose One type to Setup the Access Point** field.
2. Select **Next**.

The *Advanced Setup Wizard* displays the **Access Point Settings** screen to define the access point's Standalone versus Virtual Controller AP versus functionality. This screen also enables selection of the country of operation.

**Access Point Settings**

**Access Point Type Selection**

- Virtual Controller AP - When more than one access point is deployed, a single access point can function as a Virtual Controller AP and manage Dependent mode access points. The Virtual Controller AP can adopt and configure other like APs in a 24-cell deployment.
- Standalone AP - Select this option to deploy this access point as an autonomous "fat" access point. A standalone AP isn't managed by a Virtual Controller AP, or adopted by a controller.
- Adopted to Controller - Select this option when you want the AP to adopt to a controller. The AP will discover L2 connected controllers automatically. It will also try to discover controllers over L3 using DHCP or DNS discovery mechanism. For this, no further configuration is required on the AP. Please see the System Reference Guide for details on how to setup your DHCP or DNS server to enable this. If the AP is not on the same L2 segment as the controller and your network is not setup for DHCP or DNS based discover, you can specify the controller IP manually below.

◀ Back    ▶ Next    Save/Commit    Cancel

**Figure 3-14** Initial Setup Wizard - Access Point Settings screen for Advanced Setup Wizard

3. Select an **Access Point Type** from the following options:

- *Virtual Controller AP* - When more than one access point is deployed, a single access point can function as a Virtual Controller AP. Up to 24 access points can be connected to, and managed by, a single Virtual Controller AP. These connected access points must be the same model as the Virtual Controller AP. For more information, see [Virtual Controller AP Mode on page 3-8](#).
- *Standalone AP* - Select this option to deploy this access point as an autonomous fat access point. A standalone AP is not managed by a Virtual Controller AP, or adopted by a RFS series wireless controller. For more information see [Standalone Mode on page 3-9](#).



**NOTE:** If designating the access point as a Standalone AP, Motorola Solutions recommends the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

- *Adopted to Controller* - Select this option when deploying the access point as a controller managed (Dependent mode) access point. Selecting this option closes the Initial AP Setup Wizard. An adopted access point obtains its configuration from a profile stored on its managing controller. Any manual configuration changes are overwritten by the controller upon reboot. For more information on configuring the access point in the *Adopted to Controller* mode, see [Adopt to a controller on page 3-35](#).

4. Select the **Next** button to start configuring the access point in the selected mode. If the **Access Point Type** is *Virtual Controller AP* or *Standard AP*, see [Network Topology Selection on page 3-24](#).

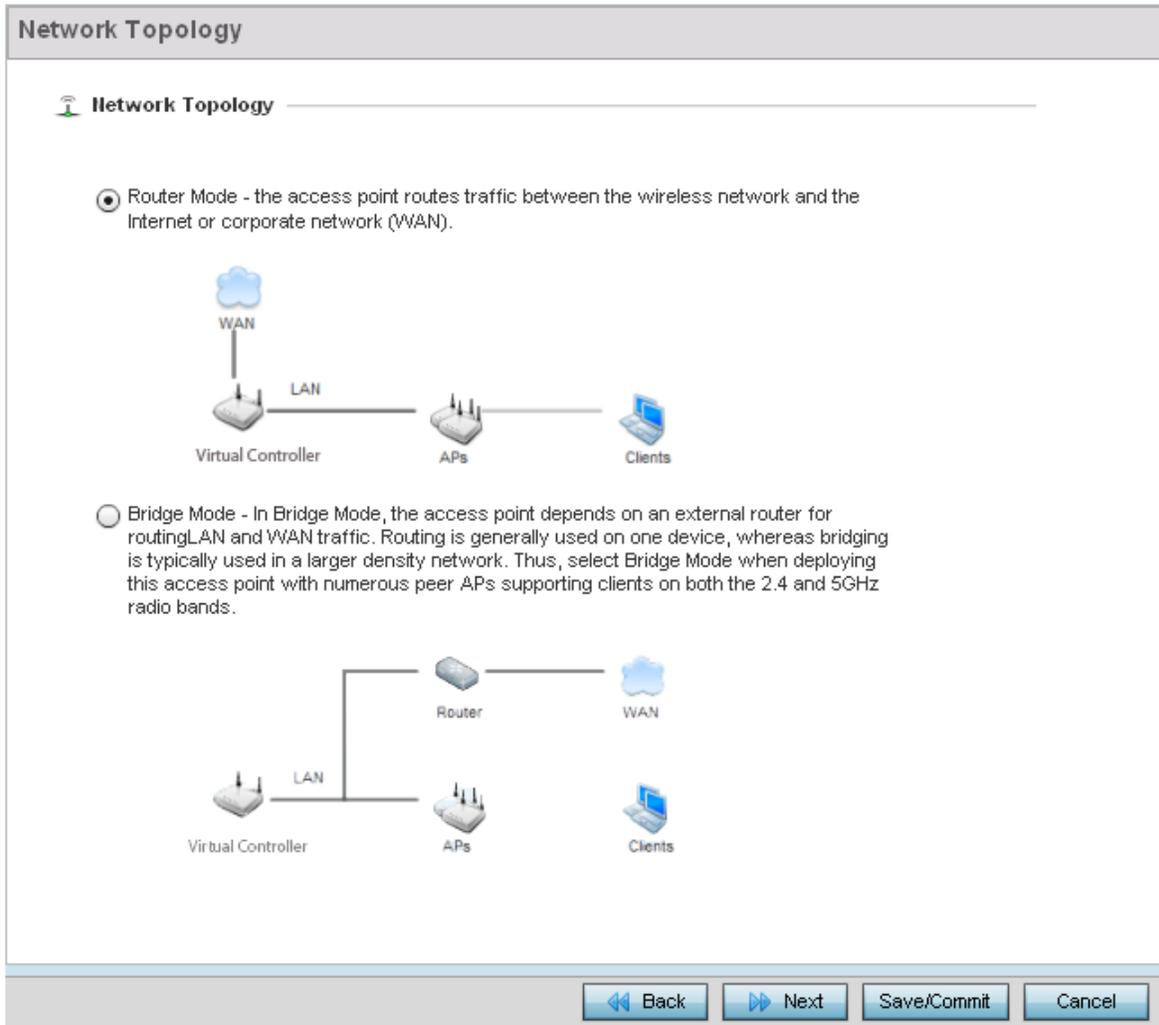
If the **Access Point Type** is *Adopted to Controller*, see [Adopt to a controller on page 3-35](#).

---

### 3.1.2.1 Network Topology Selection

► *Advanced Setup Wizard*

Use the *Network Topology* screen to define how the access point manages network traffic. The available modes are:



**Figure 3-15** *Initial Setup Wizard - Access Point Mode screen for Advanced Setup Wizard*

- **Router Mode** - In Router Mode, the access point routes traffic between the local network (LAN) and the Internet or external network (WAN). Router mode is recommended in a deployment supported by just a single access point.
- **Bridge Mode** - In Bridge Mode, the access point depends on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger density network. Select *Bridge Mode* when deploying this access point with numerous peer access points supporting clients on both the 2.4 GHz and 5.0 GHz radio bands.



**NOTE:** When *Bridge Mode* is selected, WAN configuration cannot be performed and the Initial Setup Wizard does not display the WAN configuration screen.

1. Select **Next**. The *Advanced Setup Wizard* displays the **LAN Configuration** screen to set the access point's LAN interface. For more information, see [LAN Configuration on page 3-25](#).

### 3.1.2.2 LAN Configuration

► [Advanced Setup Wizard](#)

Use the *LAN Configuration* screen to configure the parameters required for setting a *Local Area Network* (LAN) on the access point.

**Figure 3-16** Initial Setup Wizard - LAN Configuration screen for Advanced Setup Wizard

- Set the following DHCP and Static IP Address/Subnet information for the LAN interface:
  - Use DHCP** - Select the option to enable an automatic network address configuration using DHCP server.
  - Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's LAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **DHCP Server** and **Domain Name Server (DNS)** resources, as those fields will become enabled on the bottom portion of the screen.
    - Use on-board DHCP server to assign IP addresses to wireless clients** - Select the check box to enable the access point's DHCP server to provide IP and DNS information to clients on the LAN interface.
    - Range** - Enter a starting and ending IP Address range for client assignments on the access point's LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.
    - Default Gateway** - Define a default gateway address for use with the default gateway. This is a required parameter.

- **DNS Forwarding** - Select this option to allow a DNS server to translate domain names into IP addresses. If this option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.
  - **Primary DNS** - Enter an IP Address for the main Domain Name Server providing DNS services for the access point's LAN interface.
  - **Secondary DNS** - Enter an IP Address for the backup Domain Name Server providing DNS services for the access point's LAN interface
2. Select **Next**. The *Advanced Setup Wizard* displays the *Radio Configuration* screen to set the access point's radios. For more information, see [Radio Configuration on page 3-29](#).

If *Router Mode* is selected as the **Network Topology**, then the *Advanced Setup Wizard* displays the WAN configuration screen. For more information, see [WAN Configuration on page 3-13](#).

---

### 3.1.2.3 WAN Configuration

► [Advanced Setup Wizard](#)



**NOTE:** This option is only available when *Router Mode* is selected in the **Network Topology** screen of the *Advanced Setup Wizard*.

The *Advanced Setup Wizard* displays the **WAN Setting** screen to define DHCP and network address information for the WAN interface. The WAN interface is used to connect the access point to a wired local area network or backhaul.

**Figure 3-17** Initial Setup Wizard - WAN Configuration screen of the Advanced Setup Wizard

- Set the following WAN parameters:
  - Use DHCP** - Select the radio control to enable an automatic network address configuration using external DHCP servers. An automatic IP address is configured to the access point's WAN port using DHCP servers located on the WAN side of the network.
  - Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's WAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **Default Gateway** information as the field will become enabled on the bottom portion of the screen. The IP address defined in this field is assigned to the WAN interface. The **Default Gateway** is a router that serves as a access to other networks.
  - Select the port that's connected to the WAN** – Select the port that is connected to the WAN.

- **Enable NAT on the WAN Interface** – Select the option to enable *Network Address Translation* on the selected GE interface.
2. Select **Next**. The *Advanced Setup Wizard* displays the **Radio Configuration** screen to set the access point's radios. For more information, see [Radio Configuration on page 3-29](#).

### 3.1.2.4 Radio Configuration

► [Advanced Setup Wizard](#)

Use the **Radio Configuration** screen to define radio support for the 2.4 GHz radio band, 5.0 GHz radio band or set the radio as a dedicated sensor.



**NOTE:** The *Radio Configuration* screen displays separate configurable fields for each access point radio. Supported access point models can have from one to three (AP7131) radios. The **ADSP Sensor Server** field displays at the bottom of the screen only if one of the radios has been dedicated as a sensor.

**Radio Configuration**

**Radio 1**

Configure as a Data Radio [What is this?](#)

Power Level: smart (1 -- 23) Channel Mode: [ ]

Configure as a Sensor Radio [What is this?](#)

Disable the Radio Radio 1 will be disabled. Please make sure this is what you want to do.

**Radio 2**

Configure as a Data Radio

Power Level: smart (1 -- 23) Channel Mode: [ ]

Configure as a Sensor Radio [What is this?](#)

Disable the Radio Radio 2 will be disabled. Please make sure this is what you want to do.

Back Next Save/Commit Cancel

**Figure 3-18** Initial Setup Wizard - Radio Configuration screen of the Advanced Setup Wizard

- Set the following for each radio:
  - Configure as a Data Radio** - Select this option to dedicate this radio to WLAN client support in the selected 2.4 GHz or 5.0 GHz radio band.
  - Radio Frequency Band** - Select the 2.4 GHz or 5.0 GHz radio band to use with the radio when selected as a Data Radio. The selected band is used for WLAN client support. Consider selecting one radio for 2.4 GHz and another for 5.0 GHz support (if using a dual or three radio model) when supporting clients in both the 802.11b and 802.11n bands.
  - Power Level** - Use the spinner control to select a 1 - 23 dBm minimum power level to assign to this radio in selected

2.4 GHz or 5.0 GHz band. 1 dBm is the default setting.

- **Channel Mode** - Select either *Random*, *Best* or *Static*. Select *Random* for use with a 802.11a/n radio. To comply with *Dynamic Frequency Selection* (DFS) requirements in the European Union, the 802.11a/n radio uses a randomly selected channel each time the access point is powered on. Select *Best* to enable the access point to scan non-overlapping channels and listen for beacons from other access points. After the channels are scanned, it will select the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level. When *Constantly Monitor* is selected, the access point will continuously scan the network for excessive noise and sources of interference. Select *Static* to assign the access point a permanent channel and scan for noise and interference only when initialized.
- **Configure as a Sensor Radio** - Select this option to dedicate the radio to sensor support exclusively. When functioning as a sensor, the radio scans in sensor mode across all channels within the 2.4 and 5.0 GHz bands to identify potential threats. If dedicating a radio as a sensor resource, a primary and secondary ADSP server must be specified as an ADSP management resource.



**NOTE:** If configuring an AP6511 or AP6521 model access point as a sensor, the access point will require a reboot before its sensor functionality is invoked. The reboot can take place at the completion of the Initial Setup Wizard.

- 
- 
- **Disable the Radio** - Select this option to disable this radio, thus prohibiting it from either providing WLAN or sensor support. Verify this course action with your network administrator before rendering the radio offline.
2. Select **Next**. The *Advanced Setup Wizard* displays the *Wireless LAN Setup* screen to set the access point's Wireless LAN interface configuration. For more information, see [Wireless LAN Setup on page 3-31](#).

### 3.1.2.5 Wireless LAN Setup

#### ▶ *Advanced Setup Wizard*

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

Use the *Wireless LAN Setup* screen to configure the WLAN parameters. Up to two (2) WLANs can be configured for the access point.

The screenshot shows the 'Wireless LAN Setting' window. At the top, there are tabs for 'WLAN 1' and 'WLAN 2'. Below the tabs, the 'WLAN 1 Configuration' section is active. It features a text input field for 'SSID' containing 'WLA\_01', with a 'What is this?' link and a red asterisk to its right. Underneath, the 'WLAN Type' section has four radio button options: 'No Authentication and No Encryption' (selected), 'Captive Portal Authentication and No Encryption', 'PSK authentication, WPA2 encryption', and 'EAP Authentication and WPA2 Encryption'. Each option has a 'What is this?' link. At the bottom of the window, there are four buttons: 'Back', 'Next', 'Save/Commit', and 'Cancel'.

**Figure 3-19** Initial Setup Wizard - WAN Configuration screen for Advanced Setup Wizard

1. Set the following WLAN1 Configuration parameters:
  - **SSID** – Configure the SSID for the WLAN.
  - **WLAN Type** – Configure the encryption and authentication to use with this WLAN.
    - **No Authentication and No Encryption** – Configures a network without any authentication. This means any device can access the network. This option also configures the network without encryption. This means any data transmitted through the network is in plain text.
    - **Captive Portal Authentication and No Encryption** – Configures a network using a RADIUS server to authenticate

users before allowing them on to the network. Once on the network, no encryption is used for the data transmitted through the network. Select this option to use a Web page (either internally or externally hosted) to authenticate users before access is granted to the network.

- **External RADIUS Server** – When selected, provide the IP address of the external RADIUS server used for user authentication. Also enter the shared secret in the **RADIUS Shared Secret** field.
  - **Onboard RADIUS Server** – When selected, a new screen displays where further configuration can be performed. For more information, see [RADIUS Server Configuration on page 3-17](#).
  - **PSK authentication, WPA2 encryption** – Configures a network that uses PSK authentication and WPA2 encryption. Select this option to implement a pre-shared key that must be correctly shared between the access point and requesting clients on the WLAN.
    - **WPA Key** – Provide a 64 character HEX key or 8-63 character ASCII key. Use the drop-down to specify the type of key provided. Select ASCII or HEX to specify the key type provided in the **WPA Key** field.
  - **EAP Authentication and WPA2 Encryption** – Configures a network that uses EAP authentication and WPA2 encryption. Select this option to authenticate clients within this WLAN through the exchange and verification of certificates.
    - **External RADIUS Server** – When selected, provide the IP address of the external RADIUS server used for user authentication. Also provide the shared secret in the **RADIUS Shared Secret** field.
    - **Onboard RADIUS Server** – When selected, a new screen is displayed where further configuration can be performed. For more information, see [RADIUS Server Configuration on page 3-17](#).
2. Select **Next**. The *Advanced Setup Wizard* displays the *RADIUS Server Configuration* screen if required. This screen is only displayed when **Onboard RADIUS Server** is selected for either **Captive Portal Authentication And No Encryption** or for **EAP Authentication and WPA2 Encryption** fields. For more information, see [RADIUS Server Configuration on page 3-17](#).

Otherwise, the *Advanced Setup Wizard* displays the *System Information* screen. For more information, see [System Information on page 3-33](#).

### 3.1.2.6 System Information

▶ [Advanced Setup Wizard](#)

Use the *System Information* screen to define the device's location, contact information for an administrator, and the country where this access point is deployed.

**System Information**

**Country and Time Zone**

The System should be configured with the correct identifying information and a new administrator password to prevent unauthorized access. The country code is especially important in order to ensure regulatory compliance.

Location:       Contact:

Country: **United States-us** \*

Time Zone: **(GMT-05:00) America/New\_York**

Navigation:

**Figure 3-20** Initial Setup Wizard - System Information screen for the Advanced Setup Wizard

- **Location** - Provide the location of the access point.
  - **Contact** - Specify the contact information for the administrator. The credentials provided should accurately reflect the individual responding to service queries.
  - **Country** - Select the country where the access point is deployed. The access point prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. This is a required parameter.
  - **Time Zone** - Set the time zone where the access point is deployed. This is a required parameter. The setting should be complimentary with the selected deployment country.
1. Select **Next**. The *Advanced Setup Wizard* displays the *Summary and Commit* screen to summarize the screens (pages) and settings updated using the Initial AP Setup Wizard. For more information, see [Summary And Commit Screen on page 3-34](#).

### 3.1.2.7 Summary And Commit Screen

► *Advanced Setup Wizard*

The *Summary And Commit* screen displays an overview of the updates made using the *Advanced Setup Wizard*.

There is no user intervention or additional settings required. This screen is an additional means of validating the configuration before it is deployed. However, if a screen displays settings not intended as part of the initial configuration, the screen can be selected from within the **Navigation Panel** and its settings modified accordingly.

**Summary and Commit**

**Access Point Type Page**

Access Point Type    Standalone AP

**Networking Mode Page**

Networking Mode    Router Mode

**LAN Configuration Page**

LAN Configuration Type    Static IP Address/Subnet

VLAN ID for the LAN Interface    1

Static IP Address/Subnet    192.168.13.23/24

**WAN Configuration Page**

WAN Configuration Type    Use DHCP

Port to External    GE1 Port

**Radio Configuration Page**

Radio 1    Configure as a Data Radio

◀ Back    ▶ Next    Save/Commit    Cancel

**Figure 3-21** *Initial Setup Wizard - Summary and Commit screen for the Advanced Setup Wizard*

If the configuration displays as intended, select **Save/Commit** to implement these settings to the access point. If additional changes are warranted, either select the target page from the *Navigational Panel*, or use the **Back** button.

### 3.1.2.8 Adopt to a controller

#### ▶ *Advanced Setup Wizard*

When the access point is powered on for the first time, it looks for a wireless controller on the default subnet running the same firmware version and automatically adopts to it.

When *Adopted to Controller* is selected, further configuration settings are displayed in the same screen. Select **Automatic controller discovery** to enable the access point to be discovered and adopted using layer 2 settings.

If preferring layer 3 adoption, select **Static Controller Configuration**, and define the addresses of the preferred controllers. When using the static method, define whether the access point receives an IP address using DHCP or if IP resources are provided statically. Up to two (2) controllers can be defined. The access point will try to adopt to the controller defined in the **Controller 1** field first. Should the controller not be found, the access point tries to adopt to the controller defined in **Controller 2** field.

When preferring layer 3 adoption, configure how an IP is assigned to this access point. Select **Use DHCP** to use DHCP to assign an IP address to this access point. If this access point requires a static IP, select **Static IP Address/Subnet** and provide the appropriate IP address and net mask. For your convenience, the netmask is automatically set to 24. Also assign the **Default Gateway** for forwarding traffic.

**Adoption Settings**

Automatic controller discovery (L2, DHCP or DNS based)  
 Static Controller Configuration

**Controller 1**  \*      **Controller 2**

Use DHCP       Static IP Address/Subnet       \*

**Default Gateway**  \*

**Figure 3-22** *Initial Setup Wizard - Adoption Settings*



**NOTE:** The best way to administer a network populated by numerous access points is to configure them directly from their managing controller or Virtual Controller AP. If an access point's configuration requires an exception from the wireless controller or Virtual Controller AP's assigned profile configuration, the administrator should apply a Device Override to change just that access point's configuration.

1. Select the **Save/Commit** button to save the current configuration. Select the **Cancel** button to exit the *Initial Setup Wizard* without making any changes. Select the **Back** button to go back to the previous screen of the *Initial Setup Wizard*.

## 3.2 Using WiNG Express Quick Configuration

### ► Quick Start



**NOTE:** This section describes the configuration of the following APs running WiNG Express.

- AP6511E, AP6521E, AP6522E
- AP6562E
- AP7522E, AP7532E

The above access points can also run standard WiNG. For more information on configuring standard WiNG, see *Using the WiNG Initial Setup Wizard on page 3-2*. For a complete list of access points supporting WiNG 5, see *About this Guide on page 1*.

For an access point running WiNG Express, both the WiNG Express UI and an *over the air* (OTA) provisioning configuration are required for a basic setup and network connection. For a non WiNG Express SKUs there is no OTA support, and the access point utilizes just the UI for its basic setup.



**NOTE:** For information on using WiNG Express beyond this initial setup, refer to the *Motorola Solutions WiNG Express Users Guide* to familiarize yourself with the WiNG Express Access Point operating system. The guide is available at <https://portal.motorolasolutions.com/Support/US-EN>.

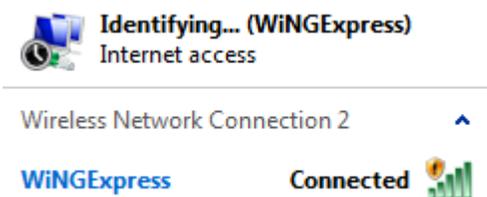
To provide the access point a basic configuration and access WiNG Express management functions:

1. Power up the access point.

The access point can be powered using an appropriately rated power adapter, POE injector or POE switch resource.

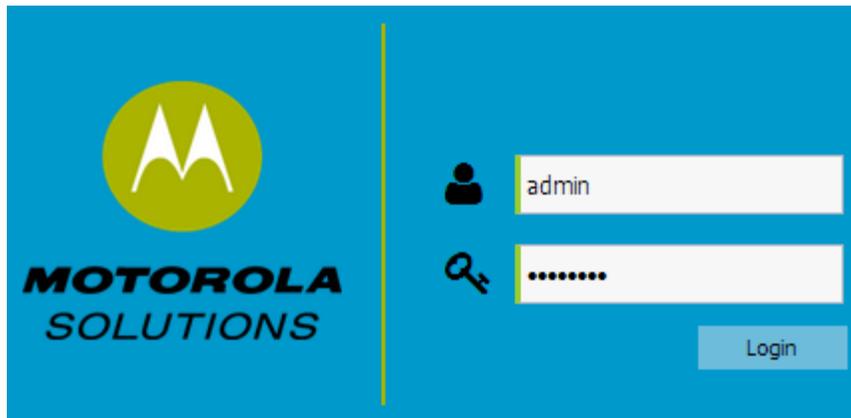
2. Connect to the access point.

By default, an access point running WiNG Express is preconfigured to broadcast with an SSID *WiNGExpress*. Connect to the WiNG Express SSID. For Windows systems, locate the SSID by selecting the network icon on the bottom right corner of the screen. For MAC systems, locate the SSID by selecting the network icon on the top right corner of the screen.



**Figure 3-23** WiNG Express SSID

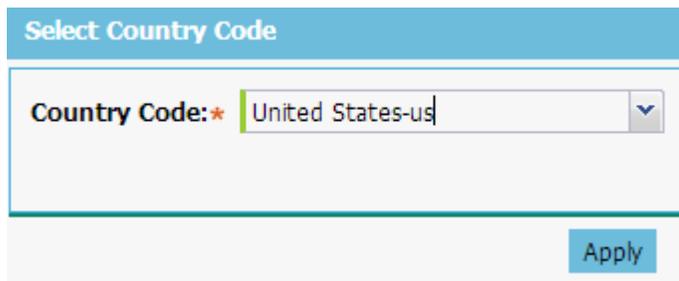
3. Open a browser (Chrome, Firefox or Internet Explorer) and enter <http://express.motorolasolutions.com>. The login screen displays.



**Figure 3-24** WiNG Express Login screen

4. Enter the default username *admin* in the **Username** field.
5. Enter the default password *motorola* in the **Password** field.
6. Select the **Login** button to load the management interface.

If this is the first time the WiNG Express interface has been accessed, a screen displays prompting for the access point's country code.



**Figure 3-25** WiNG Express - Select Country Code screen

7. Select the **Country Code** specific to this access point's deployment location.

Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. Select **Apply** to implement the selected Country Code. SKUs only support certain countries (for example: a US SKU only includes US, Guam, Puerto Rico, American Samoa, US Virgin Islands and Mariana Island).

The access point automatically displays a **Dashboard** where users can assess network health and conduct a diagnostic review of access point performance.



**NOTE** At some point in the access point's initial setup, the default password should be changed to enhance the security of the access point and WiNG Express managed network. Refer to the **Configuration > Management** screen to change the default password to a more secure password.

---



---

8. Expand the **Configuration** menu item and select **Basic**.

Basic Configuration Settings

AP Name:★ AN-08-15E54C

Country Code:★ Select a Country

Virtual Controller:

Timezone: Select a Timezone

Date & Time: 05/12/2014 Hour: 1 Mins: 34  AM  PM

NTP Server: . . .

Apply Discard

**Figure 3-26** WiNG Express - Basic Configuration Settings screen

9. Set the following **Basic Configuration Settings** for the access point.

<b>AP Name</b>	Provide a name to be used as this access point's WiNG Express network identifier. If setting this access point as a Virtual Controller, each access point managed by this Virtual Controller lists this access point's <i>AP Name</i> as its own. This is a required parameter.
<b>Country Code</b>	If country code was not set when the access point was initially powered on, set the country now to ensure the access point's legal operation. The access point's wireless capabilities are disabled until the country code is set. This is a required parameter.
<b>Virtual Controller</b>	Select this option to define this access point as a Virtual Controller capable of managing and provisioning up to 24 access points of the same model. If selecting this access point as a Virtual Controller, those access point managed by this Virtual Controller will list this access point's <i>AP Name</i> as its own. Only one access point can be designated as a Virtual Controller.
<b>Timezone</b>	Use the drop-down menu to specify the geographic timezone where the access point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.
<b>Date &amp; Time</b>	Set the date, hour and minute for the access point's current system time. Specify whether the current time is in the <i>AM</i> or <i>PM</i> .
<b>NTP Server</b>	Optionally provide the IP address of a NTP server resource. <i>Network Time Protocol</i> (NTP) manages time and/or network clock synchronization within the WiNG Express network. NTP is a client/server implementation. Access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

10. Select **Apply** to implement the updates.
11. Expand the **Configuration** menu item and select **WAN**.

WAN Settings

Enable:

Port: ge1

Interface: vlan1

DHCP Client  Static IP  PPPoE Settings

Static IP/Mask:\*

Primary DNS:

Secondary DNS:

Default Gateway:

**Figure 3-27** WiNG Express - Configuration - WAN Settings screen

12. Refer to the **WAN Settings** field and set the following:

<b>Enable</b>	Select Enable to allow a connection between the access point and a larger network or outside world through the WAN port. Disable this option to effectively isolate the access point's WAN connection. No connections to a larger network or the Internet will be possible. Clients cannot communicate beyond the configured subnets.
<b>Port</b>	The default <i>Gigabit Ethernet</i> (GE) port GE1 is used when connecting to the WAN. Supported access point models have different physical port configurations.
<b>Interface</b>	The default interface is VLAN1.
<b>DHCP Client</b>	Select this option to enable DHCP for the access point WAN connection. <sup>1</sup> This is useful, if the target network or <i>Internet Service Provider</i> (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are <i>IP address</i> , <i>network mask</i> , and <i>gateway</i> . Motorola Solutions recommends the WAN and LAN ports should not both be configured as DHCP clients.
<b>Static IP</b>	Select this option to bypass DHCP address allocation resources and manually set the IP address for the access point's WAN connection. Manually provide the access point's <i>Static IP/Mask</i> and <i>Default Gateway</i> .
<b>PPPoE Settings</b>	Optionally enable <i>Point-to-Point Protocol over Ethernet</i> (PPPoE) on the WAN network. If PPPoE is enabled, provide the required Auth Type, Login Name and Login Password. Server Name and Default Gateway are optional settings. PPP is a data-link protocol for dialup connections allowing an access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression as specified by the PPPoE protocol. PPPoE enables the access point to establish a point-to-point connection to an ISP over an existing Ethernet interface.
<b>Static IP / Mask</b>	Specify an IP address for the WAN connection if using static address assignment for the WAN port. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1. Additionally, specify a Mask for the access point's WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the access point connects to a larger network.

**Primary/  
Secondary DNS/  
Default Gateway**

If using a static IP or DHCP, enter the Primary and Secondary DNS server resource's numerical IP address and Default Gateway.



**NOTE:** If segmenting traffic between the access point's WAN and LAN, you'll need to create a VLAN. Complete steps 14 and 15 to define the required VLAN. Otherwise, proceed to step 16.

13. Select **Apply** to implement the updates.

14. Expand the **Configuration** menu item and select **Access Points**. Each **AP Name** displays as a link that can be selected to update the configuration of that specific access point. Select a target AP Name link from amongst those displayed in the Access Points screen.

**Edit -> AN-08-15E54C**

**Basic Settings**

AP Name : \* AN-08-15E54C

Location : SEQUOIA-CONF

Version : 5.5.3.0-027D

Model : AP-7532-67030-US

UP Time : 0 days, 01 hours 08 minutes

**LAN IP Interface Settings**

+ Add | Delete

<input checked="" type="checkbox"/>	Interface (1-4094)	Description	Static IP
	VLAN *		0.0.0.0/24

Update Cancel

**Figure 3-28** WiNG Express - Access Point Edit screen

Refer to the **LAN IP Interface Settings** field, and add a VLAN and Static IP as required for enabling DHCP (within the *Configuration > Services* screen) for client IP address requests and ensuring routable traffic.

15. Select **Apply** to commit the updates to the selected access point's configuration.

16. Expand the **Configuration** menu item and select **Wireless**.

The Wireless screen displays fields where *Radio Settings* and *Wireless LAN* settings can be defined. Motorola Solutions recommends default radio settings remain as is for the access point's basic setup. For information on using WiNG Express beyond this initial setup, refer to the *Motorola Solutions WiNG Express Users Guide*. The guide is available at <https://portal.motorolasolutions.com/Support/US-EN>.

In respect to the **Radio Settings**, the professional installer should be aware of the following:

**Figure 3-29** WiNG Express - Wireless Screen - Radio Settings



**NOTE:** The above example includes a field for setting the antenna gain. This setting is only available for external antenna model access points and does not display for internal antenna model access points.

- The **Channels** available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
- Selecting *Smart* as the **Power** setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
- For external antenna model access points, configure the **Antenna Gain** based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the access point and the antenna.

In respect to the **Wireless LAN** settings, the professional installer should be aware WiNG Express access points ship with a default WLAN (WiNGExpress). However, this WLAN does not provide adequate authentication to protect from unauthorized user access. Motorola Solutions recommends an additional WLAN configuration be created and validated before deleting default WLAN.

Wireless LAN

+ Add		Delete		Row Count: 1			
	Name	Enable	SSID	VLAN	Authentication Type	2.4GHz	5GHz
<input type="checkbox"/>	WiNGExpress	✓	WiNGExpress	2100	captive	✓	✗

**Figure 3-30** WiNG Express - Wireless Screen - Wireless LAN

17. To create a new WLAN, select **+ Add** from the upper, left-hand side of the **Wireless LAN** field.

**Figure 3-31** WiNG Express - Wireless LAN - Add screen

18. Set the following configuration attributes for the new WLAN:

<b>Name</b>	Provide a unique name for the WLAN as its WiNG Express network identifier. This is a required setting.
<b>Enable</b>	Select this setting to enable this WLAN within the WiNG Express managed access point network and to provide some measure of data protection not available in the default WLAN.
<b>SSID</b>	Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters. This is a required setting. Select <i>Client-To-Client Communication</i> to enable client interoperability within this WLAN. The default is disabled, meaning clients are not allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but if this setting is disabled on the other WLAN, clients are not permitted to interoperate at all.
<b>WLAN Type</b>	The screen displays with the <i>Open</i> option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended.  If selecting <i>Secure-PSK</i> , enter a WPA2 Key to password protect the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting <i>Show</i> to expose the key is not recommended.  If selecting <i>Secure-802.1x</i> , provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the access point's WLAN resources.  Selecting <i>Guest</i> displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express access point configuration.
<b>Band</b>	Select the 2.4 GHz and/or 5 GHz radio bands supports by the WiNG Express managed access point and its connected client traffic. If this access point is designated as a Virtual Controller AP, both radio bands should be enabled.

<b>VLAN</b>	Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Motorola Solutions recommends you do not use VLAN 1 with the WLAN configuration if the WAN port has been enabled.
<b>Description</b>	Optionally enter a WLAN description to further describe the WLAN's deployment objective within the WiNG Express managed network.

19. Select **Apply** to commit the updates to the access point's WLAN configuration.
20. Expand the **Configuration** menu item and select **Services**.

The screenshot shows the 'DHCP Settings' configuration page. At the top, there is a section for 'Enable DHCP Server' with a checked checkbox. Below this is a table management area with '+ Add' and 'Delete' buttons, and a 'Row Count: 0' indicator. The table has columns for 'Interface', 'IP', 'Start IP', and 'End IP'. At the bottom right of the page, there are 'Apply' and 'Discard' buttons.

**Figure 3-32** WiNG Express - Services screen

21. Select **Enable DHCP Server** to ensure the access point can provision IP addresses to requesting clients over the specified interface.



**NOTE:** A VLAN must be already configured and available to the DHCP server as a viable interface between the access point and requesting client. Refer to the *LAN IP Interface Settings* field (within the *Edit Access Point* screen), and add a VLAN.

Select **+ Add** and provide a starting and ending IP range of addresses that constitute a pool of addresses available to requesting clients.

22. Select **Apply** to commit the updates to the access point's DHCP configuration.
23. At this point, you are ready to connect to the WiNG Express managed network using the security restrictions applied to the newly created WLAN. Ensure the new secure WLAN has been enabled, and check whether a client is able to access the WiNG Express network.



**Figure 3-33** *WiNG Express Secure SSID*



**NOTE:** Only when the new WLAN configuration is validated as accessible should the existing WiNG Express default WLAN be deleted.

# CHAPTER 4

# DASHBOARD

The dashboard allows network administrators to review and troubleshoot the operation of the devices comprising the access point managed network. Use the dashboard to review the current network topology, assess the network's component health and diagnose problematic device behavior.

By default, the *Dashboard* screen displays the System Dashboard, which is the top level in the device hierarchy.

The dashboard provides the following tools and diagnostics:

- *Dashboard*
- *Network View*

## 4.1 Dashboard

### ► Dashboard

The *Dashboard* screen displays device information organized by device association and inter-connectivity between an access point and connected wireless clients.

To review dashboard information:

1. Select **Dashboard**. Expand the **System** menu item on the upper, left-hand, side of the UI and select either an access point or connected client.

The *Dashboard* screen displays the **Health** tab by default.

The screenshot shows the 'Dashboard - Health' tab for an access point. The page is divided into several sections:

- Access Point:** ap7131-11E6C4 (00-23-68-11-E6-C4)
- Health / Inventory:** Two tabs are visible, with 'Health' selected.
- Device Details:** A table listing various system parameters.
 

Hostname	ap7131-11E6C4
Device MAC	00-23-68-11-E6-C4
Type	AP71XX
Model Number	AP7131
RF Domain Name	default
Version	5.4.0.0-027B
Uptime	0 days, 01 hours 17 minutes
CPU	Cavium Networks Octeon CN30XX V0.2
RAM	87804 kB
System Clock	2012-03-11 00:30:03 UTC
- Radio Utilization:** A table showing transmission and reception statistics.
 

Parameter	Transmit	Receive
Total Bytes	0	0
Total Packets	0	0
Total Dropped	0	
- Client RF Quality Index:** A table showing the worst 5 clients based on their RF quality.
 

Worst 5	Client MAC	Retry Rate
- Radio RF Quality Index:** A table showing the status of the radio interfaces.
 

RF Quality Index	Radio Id	Radio Type
(Off)	ap7131-11E6C4:R2	5 GHz WLAN
(Off)	ap7131-11E6C4:R1	2.4 GHz WLAN
- Refresh:** A button at the bottom right of the dashboard.

Figure 4-1 Dashboard - Health tab

### 4.1.1 Dashboard Conventions

The *Dashboard* screen displays device information using the following conventions:

- **Health** – Displays the state of the access point managed network.
- **Inventory** – Displays the physical devices managed by the access point.

### 4.1.1.1 Health

▶ [Dashboard Conventions](#)

The **Health** tab displays performance and utilization data for the access point managed network.

Access Point ap7131-11E6C4 (00-23-68-11-E6-C4) ?

Health
Inventory

**Device Details**

Hostname	ap7131-11E6C4
Device MAC	00-23-68-11-E6-C4
Type	AP71XX
Model Number	AP7131
RF Domain Name	<u>default</u>
Version	5.4.0.0-027B
Uptime	0 days, 01 hours 17 minutes
CPU	Cavium Networks Octeon CN30XX V0.2
RAM	87804 kB
System Clock	2012-03-11 00:30:03 UTC

**Radio Utilization**

Parameter	Transmit	Receive
Total Bytes	0	0
Total Packets	0	0
Total Dropped	0	

**Client RF Quality Index**

Worst 5	Client MAC	Retry Rate

**Radio RF Quality Index**

RF Quality Index	Radio Id	Radio Type
(Off)	<u>ap7131-11E6C4:R2</u>	5 GHz WLAN
(Off)	<u>ap7131-11E6C4:R1</u>	2.4 GHz WLAN

Refresh

**Figure 4-2** Dashboard - Health tab

For more information see:

- [Device Details](#)
- [Radio RF Quality Index](#)
- [Radio Utilization Index](#)
- [Client RF Quality Index](#)

#### 4.1.1.1.1 Device Details

▶ [Health](#)

The **Device Details** field displays model and version information.

Device Details	
Hostname	ap7131-11E6C4
Device MAC	00-23-68-11-E6-C4
Primary IP	192.168.13.23
Type	 AP71XX
Model Number	AP7131
RF Domain Name	<u>default</u>
Version	5.5.0.0-055B
Uptime	0 days, 06 hours 54 minutes
CPU	Cavium Networks Octeon CN30XX V0.2
RAM	90176 kB
System Clock	2013-06-12 10:21:19 IST

**Figure 4-3** Dashboard - Health tab - Device Details field

The **Device Details** field displays the name assigned to the selected access point, factory encoded MAC address, primary IP address, model type, RF Domain, software version, uptime, CPU and RAM information and system clock. Use this data to determine whether a software upgrade is warranted, or if the system clock needs adjustment.

Periodically select **Refresh** (at the bottom of the screen) to update the data displayed.

#### 4.1.1.1.2 Radio RF Quality Index

##### ► Dashboard Conventions

The **Radio RF Quality Index** displays a RF quality table for the access point's single default RF Domain. It is a percentage of the overall effectiveness of the RF environment. It is a function of the data rate in both directions, the retry rate and the error rate.

Radio RF Quality Index		
RF Quality Index	Radio Id	Radio Type
 (Off)	<u>ap7131-11E6C4:R2</u>	5 GHz WLAN
 100 (Good)	<u>ap7131-11E6C4:R1</u>	2.4 GHz WLAN

**Figure 4-4** Dashboard - Health tab - Radio RF Quality Index field

RF Quality displays as the average quality index for the single RF Domain utilized by the access point. The table lists the bottom five (5) RF quality values for the RF Domain.

The quality is measured as:

- 0-20 – Very poor quality
- 20-40 – Poor quality
- 40-60 – Average quality
- 60-100 – Good quality

The access point's RF Domain allows an administrator to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. The RF Domain contains policies that can determine a Smart RF or WIPS configuration.

Use this diagnostic information to define measures to improve radio performance in respect to wireless client load and radio band.

Periodically select **Refresh** (at the bottom of the screen) to update the RF quality data.

#### 4.1.1.1.3 Radio Utilization Index

► *Dashboard Conventions*

The **Radio Utilization Index** displays how efficiently the RF medium is used by the access point. Traffic utilization is defined as the percentage of throughput relative to the maximum possible throughput.

Refer to the number of errors and dropped packets to assess radio performance relative to the number of packets both transmitted and received.

Periodically select **Refresh** (at the bottom of the screen) to update the radio utilization information displayed.

**Radio Utilization Index**

Utilization	Radio Id	Radio Type
✎ (Off)	<u>ap7131-11E6C4:R2</u>	5 GHz WLAN
✔ 100 (Good)	<u>ap7131-11E6C4:R1</u>	2.4 GHz WLAN

Parameter	Transmit	Receive
Total Bytes	3,090	2,660
Total Packets	6,090	442,660
Total Dropped	4,900	

**Figure 4-5** Dashboard - Health tab - Radio Utilization Index field

#### 4.1.1.1.4 Client RF Quality Index

► *Dashboard Conventions*

The **Client RF Quality Index** displays a list of the worst 5 performing clients managed by the selected access point.

**Client RF Quality Index**

Worst 5	Client MAC	Retry Rate
✘ 20 (Very Poor)	<u>AA-11-11-00-00-00</u>	3,452
✔ 90 (Good)	<u>AA-11-22-00-00-00</u>	52

**Figure 4-6** Dashboard - Health tab - Client RF Quality Index field

1. The **Client RF Quality Index** displays the following:

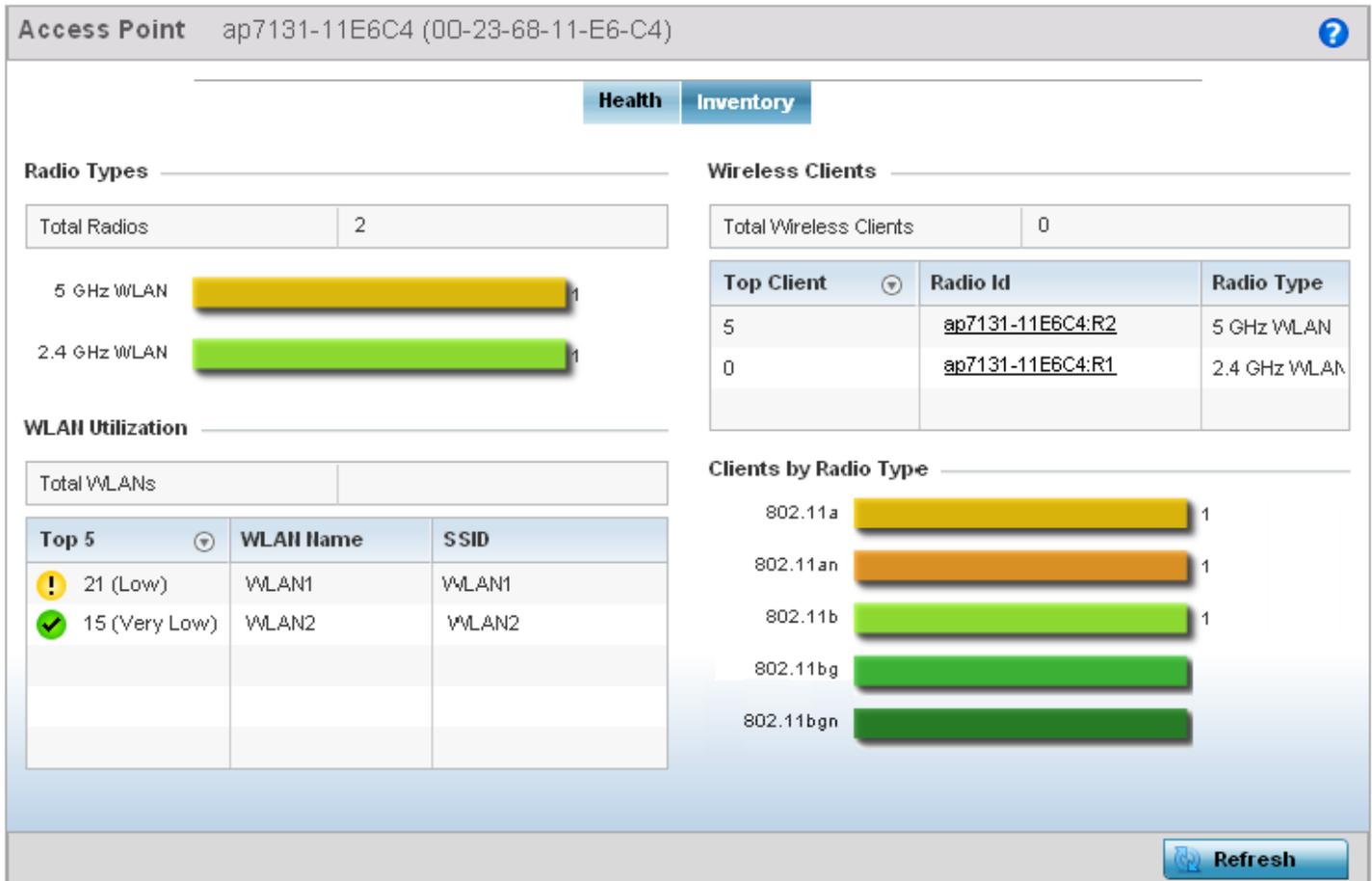
<b>Worst 5</b>	Lists the worst 5 performing client radios connected to the access point. The RF Quality Index measures the overall effectiveness of the RF environment as a percentage. Its a function of the connect rate in both directions, as well as the retry rate and the error rate. The quality is measured as: <ul style="list-style-type: none"><li>• <i>0-20</i> – Very poor quality</li><li>• <i>20-40</i> – Poor quality</li><li>• <i>40-60</i> – Average quality</li><li>• <i>60-100</i> – Good quality</li></ul>
<b>Client MAC</b>	Displays the factory encoded MAC address assigned to each connected radio listed. Use this information to assist in the identification of poorly performing radios.
<b>Retry Rate</b>	Lists the number of retries attempted to re-connect with the listed radio.

2. Periodically select **Refresh** (at the bottom of the screen) to update client RF quality.

### 4.1.1.2 Inventory

► [Dashboard Conventions](#)

The **Inventory** tab displays information relative to the devices managed by the selected access point. The Inventory screen affords a system administrator an overview of the number and state of managed devices. The screen contains links to display more granular data specific to a radio.



**Figure 4-7** Dashboard - Inventory tab

The Inventory tab is partitioned into the following fields:

- [Radio Types](#)
- [WLAN Utilization](#)
- [Wireless Clients](#)
- [Clients by Radio Type](#)

### 4.1.1.2.1 Radio Types

► [Inventory](#)

The **Radio Types** field displays the total number and types of radios managed by the selected access point.



**Figure 4-8** Dashboard - Inventory tab - Radio Types field

Refer to the **Total Radios** column to review the number of managed radios. Additionally, use the bar graphs to assess the number WLANs utilized by supported radio bands.

Periodically select **Refresh** (at the bottom of the screen) to update the radio information.

### 4.1.1.2.2 WLAN Utilization

► [Inventory](#)

The **WLAN Utilization** field displays the top 5 WLANs utilized by this access point in respect to client support. The index measures how efficiently the RF medium is utilized. It is defined as a percentage of the current throughput relative to the maximum throughput possible.

The quality is measured as:

- 0-20 – Very low utilization
- 20-40 – Low utilization
- 40-60 – Moderate utilization
- 60 and above – High utilization

WLAN Utilization			
Total WLANs			
Top 5		WLAN Name	SSID
!	21 (Low)	WLAN1	WLAN1
✓	15 (Very Low)	WLAN2	WLAN2

**Figure 4-9** Dashboard - Inventory tab - WLAN Utilization field

Periodically select **Refresh** (at the bottom of the screen) to update WLAN utilization information.

### 4.1.1.2.3 Wireless Clients

► [Inventory](#)

The **Wireless Clients** field displays information about the wireless clients managed by the selected access point.

**Wireless Clients**

Total Wireless Clients	5
------------------------	---

Top Client	Radio Id	Radio Type
5	<a href="#">ap7131-11E6C4:R2</a>	5 GHz WLAN
0	<a href="#">ap7131-11E6C4:R1</a>	2.4 GHz WLAN

**Figure 4-10** Dashboard - Inventory tab - Wireless Clients field

Information within the **Wireless Clients** field is presented in two tables. The first table lists the total number of wireless clients managed by this access point. The second table lists an ordered ranking of radios based on their supported client count. Use this information to assess if an access point managed radio is optimally deployed in respect to its radio type and intended client support requirements.

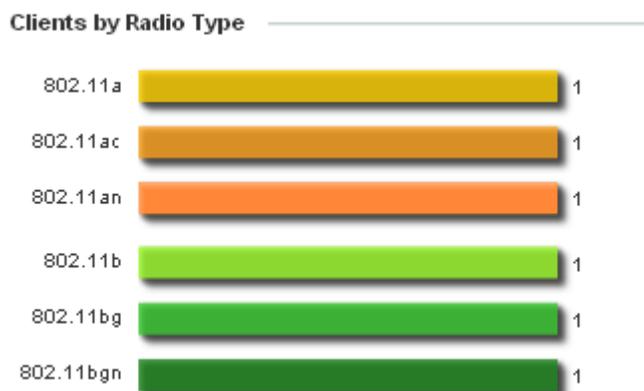


**NOTE:** AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 client connections to a single access point. AP6511 and AP6521 model access points (both single radio models) can support up to 128 client connections per access point.

#### 4.1.1.2.4 Clients by Radio Type

► [Inventory](#)

The **Clients by Radio Type** field displays a bar graph illustrating the number of connected clients currently operating on supported radio bands.



**Figure 4-11** Dashboard - Inventory tab - Clients by Radio Type field

For 5.0 GHz, clients are displayed supporting the *802.11a*, *802.11an* and *802.11ac* radio bands. For 2.4 GHz, clients are displayed supporting the *802.11b*, *802.11bg*, and *802.11bgn* radio bands. Use this information to determine if all the access point's client radio bands are optimally supported for the access point's radio coverage area.

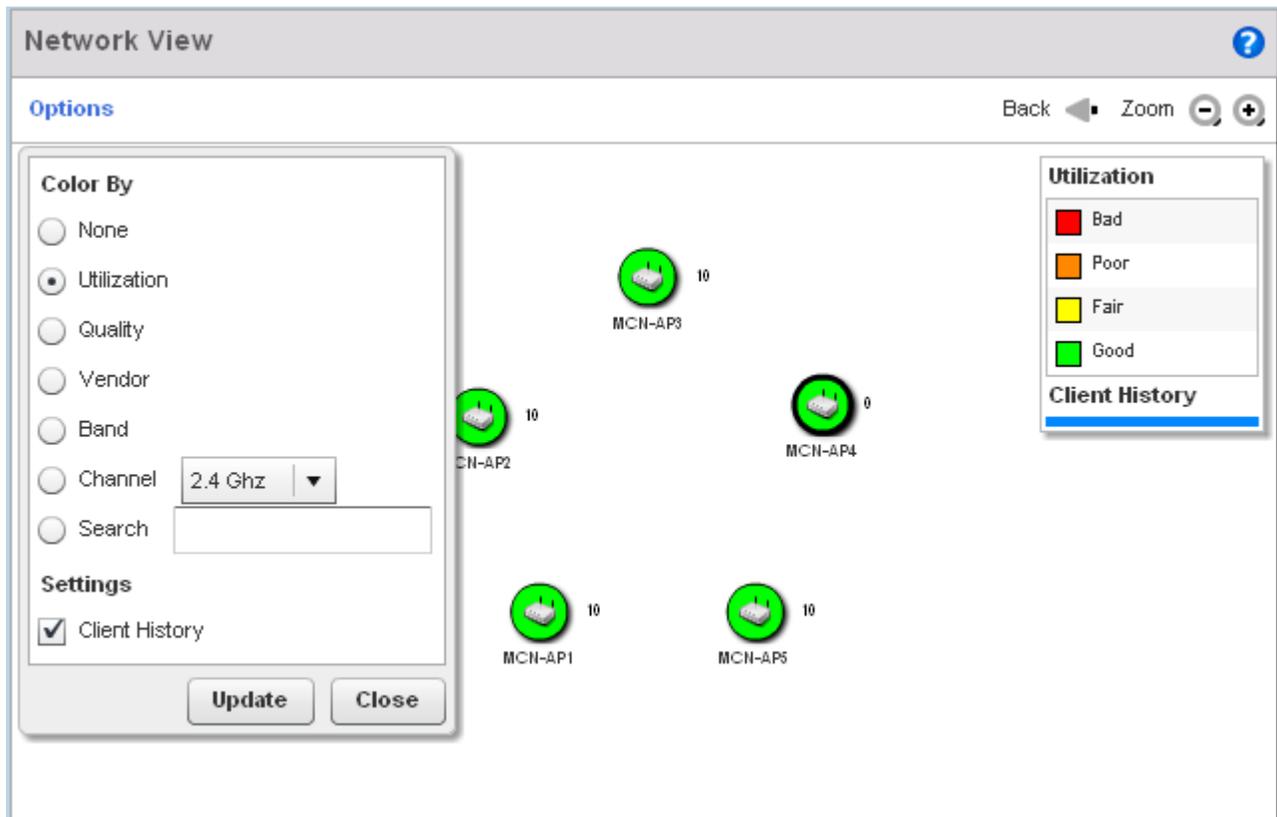
## 4.2 Network View

### ► Dashboard

The **Network View** displays device topology association between a selected access point, its RF Domain and its connected clients.

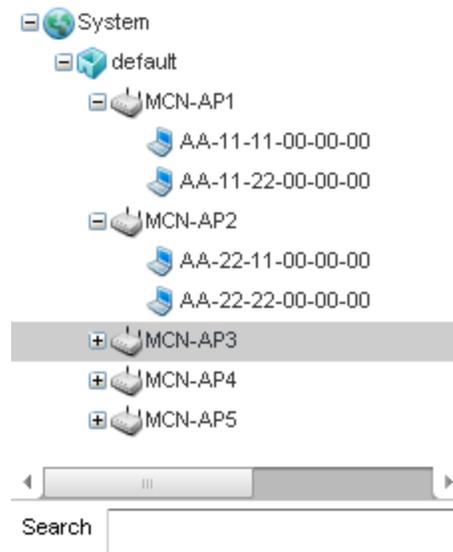
Access points and clients can be selected and viewed using various color schemes in respect to neighboring access points, connected devices and performance criteria. Display options can be utilized to review device performance and utilization, as well as the RF band, channel and vendor. For more information, see [Network View Display Options on page 4-11](#).

To review a device's Network Topology, select **Dashboard > Network View**.



**Figure 4-12** Network View Topology

The left-hand side of the *Network View* screen contains an expandable System Browser where access points can be selected and expanded to display connected clients. Navigate the System Browser to review device connections within the access point managed network. Many of these peer access points are available for connection to access points in Virtual Controller AP mode.

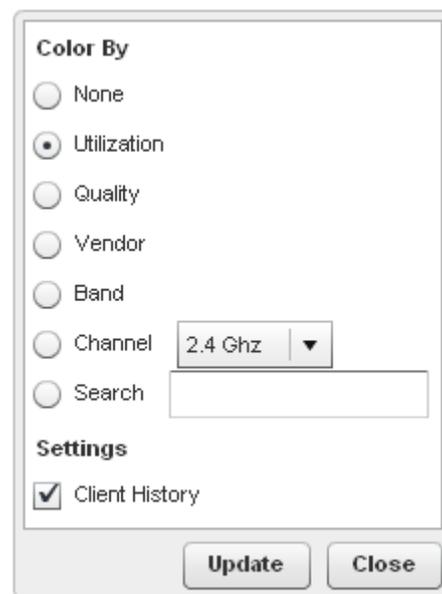


**Figure 4-13** Network View - System Browser

## 4.2.1 Network View Display Options

### ► Network View

1. Select the blue [Options](#) link right under the *Network View* banner to display a menu for different device interaction display options.



**Figure 4-14** Network View - Display Options

2. The following display filter options are available:

- *None* - Select this option to keep the Network View display as it currently appears, without any additional color or device interaction adjustments.
- *Utilization* – Select this option to filter based on the percentage of current throughput relative to maximum throughput. Utilization results include: *Red* (Bad Utilization), *Orange* (Poor Utilization), *Yellow* (Fair Utilization) and *Green* (Good Utilization).
- *Quality* – Select this option to filter based on the overall RF health. RF health is a ratio of connection rate, retry rates,

and error rates. Quality results include: *Red* (Bad Quality), *Orange* (Poor Quality), *Yellow* (Fair Quality) and *Green* (Good Quality).

- *Vendor* – Displays the device manufacturer.
  - *Band* – Select this option to filter based on the 2.4 or 5.0 GHz radio band of connected clients. Results include: *Yellow* (2.4 GHz radio band) and *Blue* (5.0 GHz radio band). Selecting Band is a good way to determine whether 2.4 and 5.0 GHz radios are optimally deployed in respect to the access point client loads on both bands.
  - *Channel* - Use the drop-down menu to filter whether device connections should be displayed in either the 2.4 or 5.0 GHz band.
  - *Search* - Enter search criteria in the provided text field and select the **Update** button to isolate located variables in blue within the Network View display.
3. Select the **Update** button to update the display with the changes made to the filter options. Select **Close** to close the options field and remove it from the Network View.

## 4.2.2 Device Specific Information

### ► Network View

A device specific information screen is available for individual devices selected from within the Network View (not the System Browser). The screen displays the name assigned to the device, its model, factory encoded MAC address, number of radios within the device, number of connected clients, as well as the highest and lowest reported quality, utilization and *Signal to Noise Ratio* (SNR). This information cannot be modified by the administrator.

MCN-AP3	
AP650 	
MAC Address	AA-33-00-00-00-00
Radio Count	2
Client Count	10
Highest Quality	70
Lowest Quality	10
Highest Utilization	55
Lowest Utilization	5
Highest SNR	40
Lowest SNR	12
<a href="#">Statistics</a>	

**Figure 4-15** Network View - Device Specific Information

Optionally select the [Statistics](#) link at the bottom of the display to open a screen where access point device data can be reviewed on a much more granular level. For more information, see [Health on page 4-3](#).

# CHAPTER 5

## DEVICE CONFIGURATION

Access points can either be assigned unique configurations to support a particular deployment objective or have an existing RF Domain or profile configuration modified (overridden) to support a requirement that deviates its configuration from the configuration shared by its peer access points.

Refer to the following to set an access point's sensor functionality, Virtual Controller AP designation, and license and certificate usage configuration:

- [RF Domain Configuration](#)
- [System Profile Configuration](#)
- [Managing Virtual Controllers](#)
- [Overriding a Device Configuration](#)
- [Managing an Event Policy](#)

An RF Domain allows an administrator to assign comparable configuration data to multiple access points deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these devices share, as their general client support roles are quite similar. However, access point configurations may need periodic refinement and overrides from their original RF Domain administered design. For more information, see [RF Domain Overrides on page 5-192](#).

Profiles enable administrators to assign a common set of configuration parameters and policies to access points of the same model. Profiles assign shared network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. To define a configuration profile for a specific access point model, refer to [System Profile Configuration on page 5-14](#).

However, device Profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could be applied an override from a configuration shared amongst numerous peer devices deployed within a particular site. For more information, see [Device Overrides on page 5-195](#).

## 5.1 RF Domain Configuration

### ► Device Configuration

An access point's configuration consists of numerous elements including a RF Domain, WLAN and device specific settings. RF Domains are used to assign regulatory, location and relevant policies to access points of the same model. For example, an AP6532 RF Domain can only be applied to another AP6532 model.

An access point RF Domain allows an administrator to assign configuration data to multiple access points deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these access points share, as their general client support roles are quite similar.

However, an access point's RF Domain configuration may need periodic refinement from its original RF Domain designation. Unlike a RFS series wireless controller, an access point supports just a single RF domain. Thus, administrators should be aware that overriding an access point's RF Domain configuration results in a separate configuration that must be managed in addition to the RF Domain configuration. Thus, a configuration should only be overridden when needed. For more information, see [RF Domain Overrides on page 5-192](#).

The access point's RF Domain can have a WIPS sensor configuration applied. For more information on defining a WIPS sensor configuration for use with the access point's RF Domain, see [RF Domain Sensor Configuration on page 5-4](#).

To set a RF Domain configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **RF Domains** from the options on left-hand side of the UI.

The RF Domain **Basic Configuration** tab displays by default with the access point RF Domain activated.

The screenshot shows the 'RF Domain' configuration window with the 'Basic Configuration' tab selected. The 'RF Domain Activated' status is shown at the top. The configuration is divided into several sections:

- Basic Configuration:**
  - Location: Blr
  - Contact: [Empty field]
  - Time Zone: (GMT+05:30) Asia/Calcutta
  - Country: India-In
  - Controller Managed: [Unchecked checkbox]
- Smart Scan:**
  - Enable Dynamic Channel: [Unchecked checkbox]
  - 2.4 GHz Channels: 1,2,3,4,... [Select]
  - 5 GHz Channels: 21,25,34,36,... [Select]
- Statistics:**
  - Update Interval: 0 (0,5-300 seconds)
  - Table with columns: Window Index, Sample Interval, Window Size, and a delete icon.
  - + Add Row button

At the bottom, there are buttons for 'Initial Setup Wizard', 'OK', and 'Reset'.

**Figure 5-1** RF Domain - Basic Configuration tab

4. Define the following **Basic Configuration** values for the access point RF Domain:

<b>Location</b>	Assign the physical location of the RF Domain. This name could be as specific as the floor of a building, or as generic as an entire site. The location defines the physical area where a common set of access point configurations are deployed and managed by the RF Domain policy.
<b>Contact</b>	Provide the name of the contact E-mail (or administrator) assigned to respond to events created by or impacting the RF Domain.
<b>Time Zone</b>	Set the geographic time zone for the RF Domain. The RF Domain can contain unique country codes and time zone information to access points deployed across different states or countries, thus making them ideal for managing device configurations across different geographical deployments.
<b>Country</b>	Define the two-digit country code set for the RF Domain. The country code must be set accurately to avoid the policy's illegal operation, as device radios transmit in specific channels unique to the country of operation.
<b>Controller Managed</b>	Select the option to indicate this RF Domain is managed by adopting controllers or service platforms. This option is disabled by default.

5. Refer to the **Smart Scan** field to define the channels for smart scan.

<b>Enable Dynamic Channel</b>	Select the option to enable dynamic channel scan.
<b>2.4 GHz Channels</b>	Use the <i>Select</i> drop-down menu to select channels to scan in the 2.4 GHz band. Selected channels are highlighted with a grey background. Unselected channels are highlighted with a white background. Multiple channels can be selected at the same time.
<b>5.0 GHz Channels</b>	Use the <i>Select</i> drop-down menu to select channels to scan in the 5.0 GHz band. Selected channels are highlighted with a grey background. Unselected channels are highlighted with a white background. Multiple channels can be selected at the same time.

6. Refer to the **Statistics** field to define how RF Domain statistics are updated.

<b>Update Interval</b>	Set a statistics update interval of 0 or 5-3600 seconds for updates retrieved from the access point.
------------------------	--

7. Select the **Add Row** button to add a new row to the **Statistics** update table.

<b>Window Index</b>	Use the spinner control to set a numerical index used as an identifier for each RF Domain statistic defined.
<b>Sample Interval</b>	Use the spinner control to define the interval (in seconds) used by the access point to capture windowed statistics supporting the RF Domain configuration. The default is 5 seconds.
<b>Window Size</b>	Use the spinner control to set the number of samples used by the controller to define RF Domain statistics. The default value is 3.

To delete a row in the **Statistics** update table, select the **Delete** icon next to the row in the table.

8. Use the **Initial Setup Wizard** to configure the device. For more information on using the **Initial Setup Wizard**, see [Using the WiNG Initial Setup Wizard on page 3-2](#).
9. Select **OK** to save the changes to the Basic Configuration, or select **Reset** to revert to the last saved configuration.

## 5.1.1 RF Domain Sensor Configuration

### ▶ RF Domain Configuration

The Motorola Solutions' *Wireless Intrusion Protection System* (WIPS) protects wireless client and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgement of a threat.

In addition to dedicated Motorola Solutions AirDefense sensors, an access point radio can function as a sensor and upload information to a dedicated WIPS server (external to the access point). Unique WIPS server configurations can be used to ensure a WIPS server configuration is available to support the unique data protection needs of a RF Domain.

WIPS is not supported on a WLAN basis, rather, sensor functionality is supported on the access point radio(s) available to each managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan in sensor mode across all legal channels within the 2.4 and 5.0 GHz band. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

To define a WIPS server configuration used with the access point's RF Domain:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **RF Domains** from the options on left-hand side of the UI.
4. Select the **Sensor Configuration** tab.

The screenshot displays the 'RF Domain' configuration page, specifically the 'Sensor Configuration' tab. At the top, there are navigation tabs: 'Basic Configuration', 'Sensor Configuration' (selected), 'Basic Alias', 'Network Group Alias', and 'Network Service Alias'. Below these is the 'Sensor Appliance Configuration' section, which contains a table with the following data:

Server Id	IP Address/Hostname	Port	
1	172.16.10.23	443	

Below the table is a '+ Add Row' button. At the bottom right of the configuration area are 'OK' and 'Reset' buttons.

**Figure 5-2** RF Domain - Sensor Configuration tab

5. Either select the **+ Add Row** button to create a new WIPS server configuration or highlight an existing Sensor Server Configuration and select the **Delete** icon to remove it.
6. Use the spinner control to assign a numerical **Server ID** to each WIPS server defined. The server with the lowest defined ID is the first reached by the access point. The default ID is 1.
7. Provide the numerical (non DNS) **IP Address** of each server used as a WIPS sensor server by the RF Domain.
8. Use the spinner control to specify the **Port** of each WIPS server. The default port is 443.

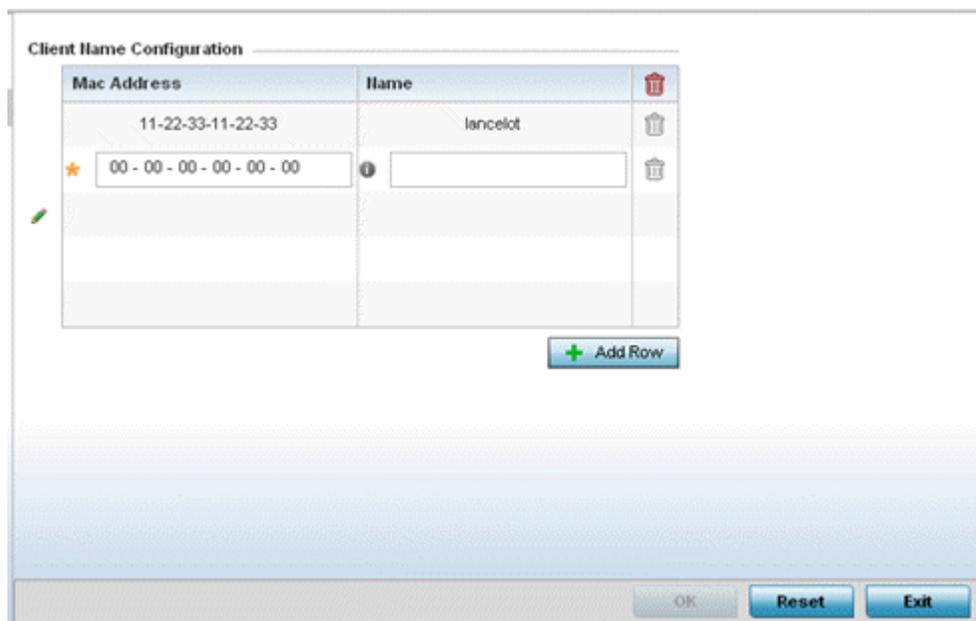
9. Select **OK** to save the changes to the AirDefense WIPS configuration, or select **Reset** to revert to the last saved configuration.

### 5.1.2 RF Client Name Configuration

The **Client Name Configuration** screen displays clients connected to RF Domain member access point adopted by networked controllers or service platforms. Use the screen to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

To define a client name configuration used with RF Domain member devices:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **RF Domains** from the options on left-hand side of the UI.
4. Select the **Client Name** tab.



**Figure 5-3** RF Domain Client Configuration screen

5. Either select the **+ Add Row** button to create a new client configuration or highlight an existing configuration and select the **Delete** icon to remove it.
6. Enter the client's factory coded MAC address.
7. Assign a **Name** to the RF Domain member access point's connected client to assist in its easy recognition.
8. Select **OK** to save the changes to the configuration, or select **Reset** to revert to the last saved configuration.

### 5.1.3 RF Domain Alias Configuration

#### ▶ RF Domain Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An *alias* enables an administrator to define a configuration item, such as a hostname, as an *alias* once and use the defined *alias* across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the *alias* used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration > Network > Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from **Configuration > Devices > System Profile > Network > Alias** screen. These aliases are available for use to a specific group of wireless controllers or access points. *Alias* values defined in this profile override alias values defined within global aliases.
- *RF Domain aliases* are defined from **Configuration > Devices > RF Domain > Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an *Network Alias* defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias works with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias can be classified as:

- *Network Basic Alias*
  - *Network Group Alias*
  - *Network Service Alias*
-

### 5.1.3.1 Network Basic Alias

#### ▶ RF Domain Configuration

A *basic alias* is a set of configurations that consist of *VLAN*, *Host*, *Network* and *Address Range* alias configurations. VLAN configuration is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

A basic alias configuration can contain multiple instances for each of the five (5) alias types.

To edit or delete a basic alias configuration:

1. Select **Configuration** tab from the Web user interface.
2. Select **Devices**.
3. Select **RF Domain**.
4. Select the **Basic Alias** tab.

The screenshot displays the 'RF Domain' configuration interface with the 'Basic Alias' tab selected. The interface includes a navigation bar with tabs for 'Basic Configuration', 'Sensor Configuration', 'Basic Alias', 'Network Group Alias', and 'Network Service Alias'. Below the navigation bar, there is an information icon and a note: 'Delete button is enabled only for entries created in this context.' The main area contains four tables, each with an information icon and an 'Add Row' button.

**Vlan Alias**

Name	Vlan	
\$TPLL	1	

**Host Alias**

Name	Host	
\$DNS_01	192.168.13.2	

**Address Range Alias**

Name	Start IP	End IP	
\$IP_Pool_01	192.168.13.10	192.168.13.20	

**Network Alias**

Name	Network	
\$Shop_01	192.168.14.0/24	

At the bottom of the screen, there are 'OK' and 'Reset' buttons.

Figure 5-4 RF Domain - Basic Alias screen

5. Select **+ Add Row** to define **VLAN Alias** settings:

Use the **VLAN Alias** field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

<b>Name</b>	If adding a new <i>VLAN Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>VLAN</b>	Use the spinner control to set a numeric VLAN from 1 - 4094.

A *VLAN alias* can be used to replace VLANs in the following locations:

- Bridge VLAN
  - IP Firewall Rules
  - L2TPv3
  - Switchport
  - Wireless LANs
6. Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

<b>Name</b>	If adding a new <i>Address Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Start IP</b>	Set a starting IP address used with a range of addresses utilized with the address range alias.
<b>End IP</b>	Set a ending IP address used with a range of addresses utilized with the address range alias.

An *address range alias* can be used to replace an IP address range in IP firewall rules.

7. Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	Set the IP address of the host machine.

A *host alias* can be used to replace hostnames in the following locations:

- IP Firewall Rules
- DHCP

8. Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	Provide a network address in the form of <i>host/mask</i> .

A *network alias* can be used to replace network declarations in the following locations:

- IP Firewall Rules
  - DHCP
9. Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.

<b>Name</b>	If adding a new <i>String Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	Provide a string value to use in the alias.

A *string alias* can be used to replace a domain name string in DHCP.

10. Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.



5. Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new Network Group Alias. **Copy** to copy an existing policy or **Rename** to rename an existing policy.

Name \$NGA\_01

Host

1.2.3.4  
2.3.4.5  
3.4.5.6

Network

192.168.13.0/24

Range

Start IP	End IP
1.2.3.4	4.3.2.1

+ Add Row

OK Reset Exit

**Figure 5-6** RF Domain - Network Group Alias Add screen

6. If adding a new **Network Group Alias**, provide it a name of up to 32 characters.



**NOTE:** The **Network Group Alias Name** always starts with a dollar sign (\$).

7. Define the following network group alias parameters:

<b>Host</b>	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
<b>Network</b>	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

8. Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

9. Select **OK** when completed to update the network group alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.1.3.3 Network Service Alias

#### ▶ RF Domain Configuration

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per *network service alias*.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

*Network Service Alias* can be used in the following location to substitute protocols and ports:

- IP Firewall Rules

To edit or delete a service alias configuration:

1. Select **Configuration** tab from the Web user interface.
2. Select **Devices**.
3. Select **RF Domain**.
4. Select the **Network Service Alias** tab.

The screenshot displays the 'RF Domain' configuration page, specifically the 'Network Service Alias' tab. At the top, there is a header 'RF Domain' with a help icon and a status indicator 'RF Domain Activated'. Below the header are several tabs: 'Basic Configuration', 'Sensor Configuration', 'Basic Alias', 'Network Group Alias', and 'Network Service Alias'. The 'Network Service Alias' tab is active, showing a table with a single entry. The table has a column labeled 'Name' and contains the value '\$NSA\_01'. At the bottom of the table, there is a search bar with the placeholder text 'Type to search in tables' and a 'Row Count: 1' indicator. Below the search bar are three buttons: 'Add', 'Edit', and 'Delete'.

**Figure 5-7** RF Domain - Network Service Alias screen

5. Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Service Alias**.

Name \$NSA\_01 ?

Entry

Protocol	Source Port(Low and High)	Destination Port(Low and High)	
* igmp	2	Enter R	
6	80-92	80	

+ Add Row

OK
Reset
Exit

**Figure 5-8** RF Domain - Network Service Alias Add screen

6. If adding a new **Network Service Alias**, provide it a name up to 32 characters.



**NOTE:** The **Network Service Alias Name** always starts with a dollar sign (\$).

7. Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

<b>Protocol</b>	Specify the protocol for which the alias has to be created. Use the drop-down menu to select the protocol ( <i>eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp</i> and <i>udp</i> ). Select <i>other</i> if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
<b>Source Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
<b>Destination Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

8. Select **OK** when completed to update the network service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

## 5.2 System Profile Configuration

### ► *Device Configuration*

An access point profile enables an administrator to assign a common set of configuration parameters and policies to access points of the same model. Profiles can be used to assign common or unique network, wireless and security parameters to across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. All WING 5 supported access point models supported a single profile that is either shared amongst multiple access point or not. The central benefit of a profile is its ability to update access points collectively without having to modify individual configurations.

A profile allows access point administration across large wireless network segments. However, an administrator cannot manage more than one model's profile and its set configuration policies at any one time. Therefore, an administrator should manage multiple access points directly from the Virtual Controller AP. As individual access point updates are made, the access point no longer shares the profile based configuration it previously deployed. Changes made to the profile are automatically inherited by all member access points, but not those who have had their configuration overridden from their previous profile designation. These devices require careful administration, as they no longer can be tracked and as profile members. Their customized configurations overwrite their profile assignments until the profile can be re-applied to the access point.

Each access point model is automatically assigned a default profile. The default profile is available within the access point's configuration file. Default profiles are ideal for single site deployments where several access points may need to share a common configuration.



**NOTE:** A central difference compared to the default-radio configurations in previous releases is default profiles are used as pointers for an access point's configuration, not just templates from which the configuration is copied. Therefore, if a change is made in one of the parameters in a profile, the change is reflected across all access points using that profile.

---

---

For more information, refer to the following:

- *General Profile Configuration*
  - *Profile Radio Power*
  - *Profile Adoption (Auto Provisioning) Configuration*
  - *Profile Wired 802.1X Configuration*
  - *Profile Interface Configuration*
  - *Profile Network Configuration*
  - *Profile Security Configuration*
  - *Virtual Router Redundancy Protocol (VRRP) Configuration*
  - *Profile Critical Resources*
  - *Profile Services Configuration*
  - *Profile Management Configuration*
  - *Mesh Point Configuration*
  - *Advanced Profile Configuration*
  - *Environmental Sensor Configuration*
-

## 5.2.1 General Profile Configuration

### ► System Profile Configuration

An access point profile requires unique clock synchronization settings as part of its general configuration.

*Network time protocol* (NTP) manages time and/or network clock synchronization within the access point managed network. NTP is a client/server implementation. The access point periodically synchronizes its clock with a master clock (an NTP server). For example, the access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Use the *General* screen of *System Profile* configuration screen to define whether the access point can act as a RF Domain manager for its RF Domain.

To define a profile's general configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.

*General* configuration options display by default, with the profile activated for use with this access point model.

**Network Time Protocol (NTP)**

Autokey	Key	Preferred	Server IP	Version	
<input checked="" type="checkbox"/>	secretgarden	<input checked="" type="checkbox"/>	172.16.10.10	1	

**RF Domain Manager**

Capable

Priority  1 (1 to 255)

**OK** **Reset**

**Figure 5-9** General Profile screen

4. Select **+ Add Row** below the *Network Time Protocol* (NTP) table to define the configurations of NTP server resources used to obtain system time. Up to 3 NTP servers can be configured. Set the following parameters to define the NTP configuration:

<b>AutoKey</b>	Select this option to enable an autokey configuration for the NTP resource. The default setting is disabled.
<b>Key</b>	If an autokey is not being used, manually enter a 64 character maximum key the access point and NTP resource share to securely interoperate.
<b>Preferred</b>	Select this option designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources are given first opportunity to connect and provide NTP calibration.
<b>Server IP</b>	Set the IP address of each server added as a potential NTP resource.

<b>Version</b>	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.
----------------	---

- Use the **RF Domain Manager** field to configure how this access point behaves in standalone mode. Set the following parameters:

<b>Capable</b>	Select to enable this access point to act as a RF Domain Manager in a particular RF Domain.
<b>Priority</b>	Select to prioritize this access point in becoming a RF Domain Manager in its; particular RF Domain. The higher the value, the more likely the device becomes the RF Domain Manager for the domain.

- Select **OK** to save the changes made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.2 Profile Radio Power

### ► System Profile Configuration

Use the *Power* screen to set one of two power modes (*3a* for *Auto*) for the access point profile. When *Automatic* is selected, the access point safely operates within available power. Once the power configuration is determined, the access point configures its operating power characteristics based on its model and power configuration.

An access point uses a *complex programmable logic device* (CPLD) to manage power. The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the maximum power budget. When an access point is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the access point. The CPLD also determines the access point hardware SKU (model) and the number of radios.

If the access point's POE resource cannot provide sufficient power to run the access point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- *The access point's transmit and receive algorithms could be negatively impacted*
- *The access point's transmit power could be reduced due to insufficient power*
- *The access point's WAN port configuration could be changed (either enabled or disabled)*

To define an access point's power configuration:

- Select the **Configuration** tab from the Web UI.
- Select **Devices**.
- Select **System Profile** from the options on left-hand side of the UI.
- Select **Power**.

A screen displays where the access point profile's power mode can be defined.

**Power Mode Configuration on this AP**

**Power Mode** ⓘ Automatic ▼

! AP must be restarted for power-management change to take effect.

**802.3af Power Mode**

**802.3af Mode** ⓘ Throughput ▼

**802.3at Power Mode**

**802.3at Mode** ⓘ Throughput ▼

OK Reset

**Figure 5-10** Profile - Power screen

- Use the **Power Mode** drop-down menu to set the **Power Mode Configuration on this AP**.



**NOTE:** Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio access point models.

When an access point is powered on for the first time, it determines the power budget available. Using the *Automatic* setting, the access point automatically determines the best power configuration based on the available power budget. *Automatic* is the default setting.

If 802.3af is selected, the access point assumes 12.95 watts are available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts are available.

- Set the access point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

Use the drop-down menu for each power mode to define a mode of either *Range* or *Throughput*.

Select *Throughput* to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance.

Select *Range* when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. Throughput is the default setting for both 802.3af and 802.3at.

- Select **OK** to save the changes made to the access point power configuration. Select **Reset** to revert to the last saved configuration

### 5.2.3 Profile Adoption (Auto Provisioning) Configuration

#### ▶ System Profile Configuration

Adoption is the process an access point uses to discover Virtual Controller APs available in the network, pick the most desirable Virtual Controller, establish an association with the Virtual Controller and optionally obtain an image upgrade, obtains its configuration and considers itself provisioned. This is a configurable activity that can be supported within an access point profile and applied to other access points (of the same model) supported by the profile.

At adoption, an access point solicits and receives multiple adoption responses from Virtual Controller APs available on the network. These adoption responses contain loading policy information the access point uses to select the optimum Virtual Controller AP for adoption.



**NOTE:** An access point configuration does not need to be present for an auto provisioning (adoption) policy to take effect. Once adopted, and the access point's configuration is defined and applied by the Virtual Controller. The auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

---

---

To define the access point profile's adoption configuration:

1. Select the **Configuration** tab from the Web UI.
  2. Select **Devices**.
  3. Select **System Profile** from the options on left-hand side of the UI.
  4. Select **Adoption**.
- 
-

**Controller Group**

Preferred Group

**Controller VLAN**

VLAN  (1 to 4,094)

**Auto-Provisioning Policy**

Auto-Provisioning Policy   

Learn and Save Network Configuration

**Controller Hello Interval**

Hello Interval  (1 to 120)

Adjacency Hold Time  (2 to 600)

**Controller Adoption Settings**

Offline Duration  (5 to 43,200)

**Controller Hostnames**

Host	Pool	Routing Level	IPsec Secure	IPsec GW	Force	Remote VPN Client	

**Figure 5-11** Profile Adoption screen

- Define the **Preferred Group** used as optimal group of Virtual Controller for adoption. The name of the preferred group cannot exceed 64 characters.
- Select the **VLAN** option to define a **VLAN** the access point's associating Virtual Controller AP is reachable on. VLANs 0 and 4,095 are reserved and cannot be used. This setting is disabled by default.
- Define the **Auto-Provisioning Policy** configuration. Set the following parameters:

<b>Auto-Provisioning Policy</b>	Use the drop-down menu to specify the Auto-Provisioning policy to use while adopting. If a suitable Auto-Provisioning policy does not exist, click the <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.
<b>Learn and Save Network Configuration</b>	Select this option to enable the access point to learn and save the configuration for any device it has adopted. Default is <i>Enabled</i> .
<b>Rerun Policy Rules Everytime AP Adopts</b>	Select this option to enable an Auto-Provisioning policy to run every time an access point adopts a client. Default is <i>Disabled</i> .

- Define the **Hello Interval** value in seconds.

The Hello interval is the interval between two consecutive hello keep alive messages exchanged between the access point and the adopting wireless controller. These messages serve as a connection validation mechanism to ensure the availability of the adopting wireless controller. Use the spinner to set a value from 1 - 120 seconds.

9. Define the **Adjacency Hold Time** value. This value sets the time after which the preferred controller group is considered down and unavailable to provide services. Use the spinner to set a value from 2 - 600 seconds.
10. Enter **Controller Hostnames** as needed to define resources for adoption. Click **+Add Row** to add controllers. Set the following parameters to define **Controller Hostnames**:

<b>Host</b>	Use the drop-down menu to specify whether the controller adoption resource is defined as a (non DNS) IP address or a hostname. Once defined, provide the numerical IP or hostname. A hostname cannot exceed 64 characters.
<b>Pool</b>	Use the spinner controller to set a pool of either 1 or 2. This is the pool the target Virtual Controller belongs to. The default setting is 1.
<b>Routing Level</b>	Use the spinner controller to set the routing level for the Virtual Controller link. The default setting is 1.
<b>IPSec Support</b>	Select to enable secure communication between the access point and wireless controllers.
<b>IPSec GW</b>	Use the drop-down menu to specify if the IPSec gateway resource is defined as a (non DNS) IP address or a hostname. Once defined, provide the numerical IP or hostname. A hostname cannot exceed 64 characters.
<b>Force</b>	Select to enable the link to the adopting controller or the controller group to be created even when not required.

11. Select **+ Add Row** as needed to populate the table with IP addresses or hostnames of adoption resources.
12. Select **OK** to save the changes made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

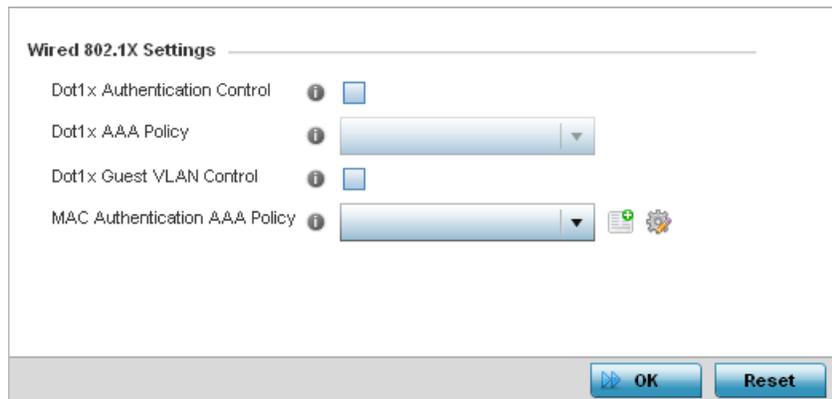
## 5.2.4 Profile Wired 802.1X Configuration

### ► System Profile Configuration

802.1X provides administrators secure, identity based access control as another data protection option to utilize with a device profile.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the user or device.

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Select **Wired 802.1x**.



**Figure 5-12** Profile Wired 802.1X screen

5. Set the following **Wired 802.1x Settings**:

<b>Dot1x Authentication Control</b>	Select this option to globally enable 802.1x authentication for the selected device. This setting is disabled by default.
<b>Dot1x AAA Policy</b>	Use the drop-down menu to select an AAA policy to associate with wired 802.1x traffic. If a suitable AAA policy does not exist, click the <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.
<b>Dot1x Guest VLAN Control</b>	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
<b>MAC Authentication AAA Policy</b>	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.

6. Select **OK** to save the changes to the 802.1x configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.5 Profile Interface Configuration

### ► System Profile Configuration

A access point profile can support customizable Ethernet port, virtual interface, port channel, radio and PPPoE configurations unique to each supported access point model.

A profile's interface configuration process consists of the following:

- [Ethernet Port Configuration](#)
- [Virtual Interface Configuration](#)
- [Port Channel Configuration](#)
- [Access Point Radio Configuration](#)
- [WAN Backhaul Configuration](#)
- [PPPoE Configuration](#)

Additionally, deployment considerations and guidelines for profile interface configurations are available for review prior to defining a configuration that could significantly impact the performance of the network. For more information, see [WAN Backhaul Deployment Considerations on page 5-55](#).



5. Refer to the following to assess port status, mode and VLAN configuration:

<b>Name</b>	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on model.
<b>Type</b>	Displays the physical port type.
<b>Description</b>	Displays an administrator defined description for each listed port.
<b>Admin Status</b>	A green check mark defines the port as active and currently enabled with the profile. A red "X" defines the port as currently disabled and not available for use. The interface status can be modified with the port configuration as required.
<b>Mode</b>	Displays the profile's current switching mode as either <i>Access</i> or <i>Trunk</i> . If <i>Access</i> is listed, the port accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to <i>Trunk</i> , the port allows packets from a list of VLANs added to the trunk. A port configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
<b>Native VLAN</b>	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
<b>Tag Native VLAN</b>	A green check mark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
<b>Allowed VLANs</b>	Displays the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to <i>Trunk</i> .

6. To edit an access point profile's port configuration, select it from amongst those displayed and then select the **Edit** button. The Ethernet port *Basic Configuration* screen displays by default.

The screenshot shows the 'Ethernet Ports' configuration window for port 'ge1'. The 'Basic Configuration' tab is active. The 'Properties' section includes fields for Description, Admin Status (radio buttons for Disabled and Enabled), Speed (dropdown menu set to Automatic), and Duplex (dropdown menu set to Automatic). The 'CDP/LLDP' section has four checkboxes, all of which are checked. The 'Captive Portal Enforcement' section has a checkbox for 'Enforce captive portal'. The 'Switching Mode' section has radio buttons for 'Access' and 'Trunk', with 'Access' selected. Below this, there are input fields for 'Native VLAN' (set to 1), 'Tag Native VLAN', and 'Allowed VLANs'. The 'Port Channel Membership' section has a dropdown menu set to 1.

**Figure 5-14** Ethernet Ports - Basic Configuration screen

7. Set the following Ethernet port **Properties**:

<b>Description</b>	Enter a brief description for the port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port as active to the profile it supports. Select the <i>Disabled</i> radio button to disable this physical port in the profile. It can be activated at any future time when needed.
<b>Speed</b>	Select the speed at which the port can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> , <i>1000 Mbps</i> . Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select <i>Automatic</i> to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.
<b>Duplex</b>	Select either <i>half</i> , <i>full</i> or <i>automatic</i> as the duplex option. Select Half duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port performance needs dictate. Automatic is the default setting.

8. Define the following *Cisco Discovery Protocol* (CDP) and LLDP parameters to apply to the Ethernet port configuration:

<b>Cisco Discover Protocol Receive</b>	Select this option to allow the Cisco discovery protocol for receiving data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
<b>Cisco Discover Protocol Transmit</b>	Select this option to allow the Cisco discovery protocol for transmitting data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
<b>Link Layer Discovery Protocol Receive</b>	Select this option to snoop LLDP on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
<b>Link Layer Discovery Protocol Transmit</b>	Select this option to transmit LLDP PDUs on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.

9. Select **Enforce Captive Portal** to automatically apply captive portal access permission rules to data transmitted over this specific Ethernet port. This setting is disabled by default.

A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance. For information on configuring a captive portal policy, see [Configuring Captive Portal Policies on page 9-2](#).

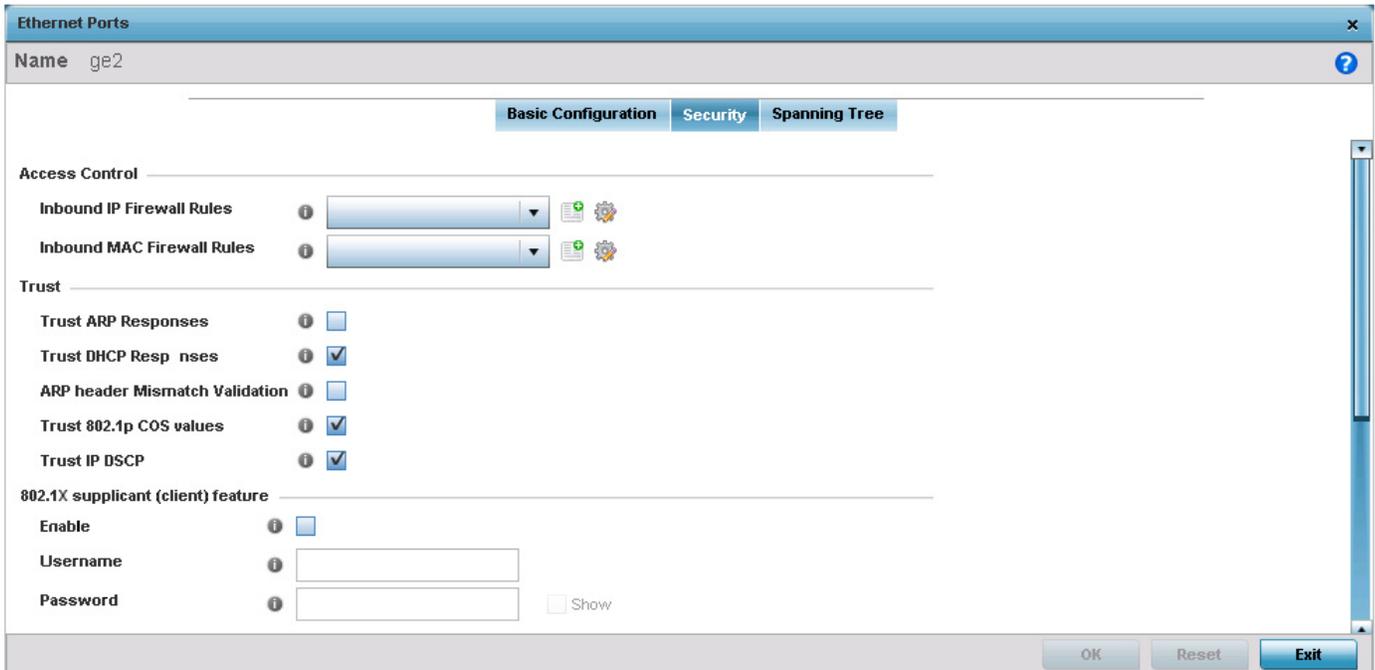
10. Define the following **Switching Mode** parameters to apply to the Ethernet port configuration:

<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port. If <i>Access</i> is selected, the port accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to <i>Trunk</i> , the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode.
<b>Native VLAN</b>	Use the spinner control to define a numerical Native VLAN ID from 1 - 4094. The native VLAN allows the access point to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.
<b>Tag Native VLAN</b>	Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.

**Allowed VLANs**

Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the listed port.

- Optionally select the **Port Channel** option and define a setting from 1 - 8 using the spinner control. This sets the channel group for the port.
- Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.
- Select the **Security** tab.



**Figure 5-15** Ethernet Ports - Security tab

- Refer to the **Access Control** field. As part of the port's security configuration, Inbound *IP* and *MAC* address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **Inbound MAC Firewall Rules** drop-down menus to select the firewall rules to apply to this profile's Ethernet port configuration.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

If a firewall rule does not exist suiting the data protection needs of the target port configuration, select the Create icon to define a new rule configuration.

- Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	Select this option to enable ARP trust on this access point port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled.
<b>Trust DHCP Responses</b>	Select this option to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.

<b>ARP header Mismatch Validation</b>	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is disabled.
<b>Trust 8021p COS values</b>	Select this option to enable 802.1p COS values on this port. The default value is enabled.
<b>Trust IP DSCP</b>	Select this option to enable IP DSCP values on this port. The default value is enabled.



**NOTE:** Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, despite a conflict existing.

16. Set the following **802.1X Settings**:

<b>Host Mode</b>	Use the drop-down menu to select the host mode configuration to apply to this port. Options include <i>single-host</i> or <i>multi-host</i> . The default setting is <i>single-host</i> .
<b>Guest VLAN</b>	Specify a guest VLAN for this port from 1 - 4094. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled.
<b>Port Control</b>	Use the drop-down menu to set the port control state to apply to this port. Options include <i>force-authorized</i> , <i>force-unauthorized</i> and <i>automatic</i> . The default setting is <i>port-authorized</i> .
<b>Re Authenticate</b>	Select this setting to force clients to reauthenticate on this port. The default setting is disabled, thus clients do not need to reauthenticate for connection over this port until this setting is enabled.
<b>Max Reauthenticate Count</b>	Set the maximum reauthentication attempts (1 - 10) before this port is moved to unauthorized. The default setting is 2.
<b>Maximum Request</b>	Set the maximum number of authentication requests (1 - 10) before returning a failed message to the requesting client. The default setting is 2.
<b>Quiet Period</b>	Set the quiet period for this port from 1 - 65,535 seconds. This is the maximum wait time 802.1x waits upon a failed authentication attempt. The default setting is 60 seconds.
<b>Reauthenticate Period</b>	Use the spinner control to set the reauthentication period for this port from 1 - 65,535 seconds. The default setting is 60 seconds.
<b>Port MAC Authentication</b>	When enabled, a port's MAC address is authenticated, as only one MAC address is supported per wired port. When successfully authenticated, packets from the source are processed. Packets from all other sources are dropped. Port MAC authentication is supported on RFS4000, RFS6000 model controllers and NX4500, NX6500, NX7500 and NX9000 series service platforms.  Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

17. Select the **Enable** option within the **802.1x supplicant (client) feature** to enable a username and password pair to be used when authenticating users on this port. Use the **Show** option to view the actual characters comprising the password entered in the **Password** field.
18. Select the **Spanning Tree** tab.

*Spanning Tree Protocol* (STP) (IEEE 802.1D standard) configures a meshed network for robustness by eliminating loops within the network and calculating and storing alternate paths to provide fault tolerance.

STP calculation happens when a port comes up. As the port comes up and STP calculation happens, the port is set to *Blocked* state. In this state, no traffic can pass through the port. Since STP calculations take up to a minute to complete, the port is not operational there by effecting the network behind the port. Once the STP calculation is complete, the port's state is changed to *Forwarding* and traffic is allowed.

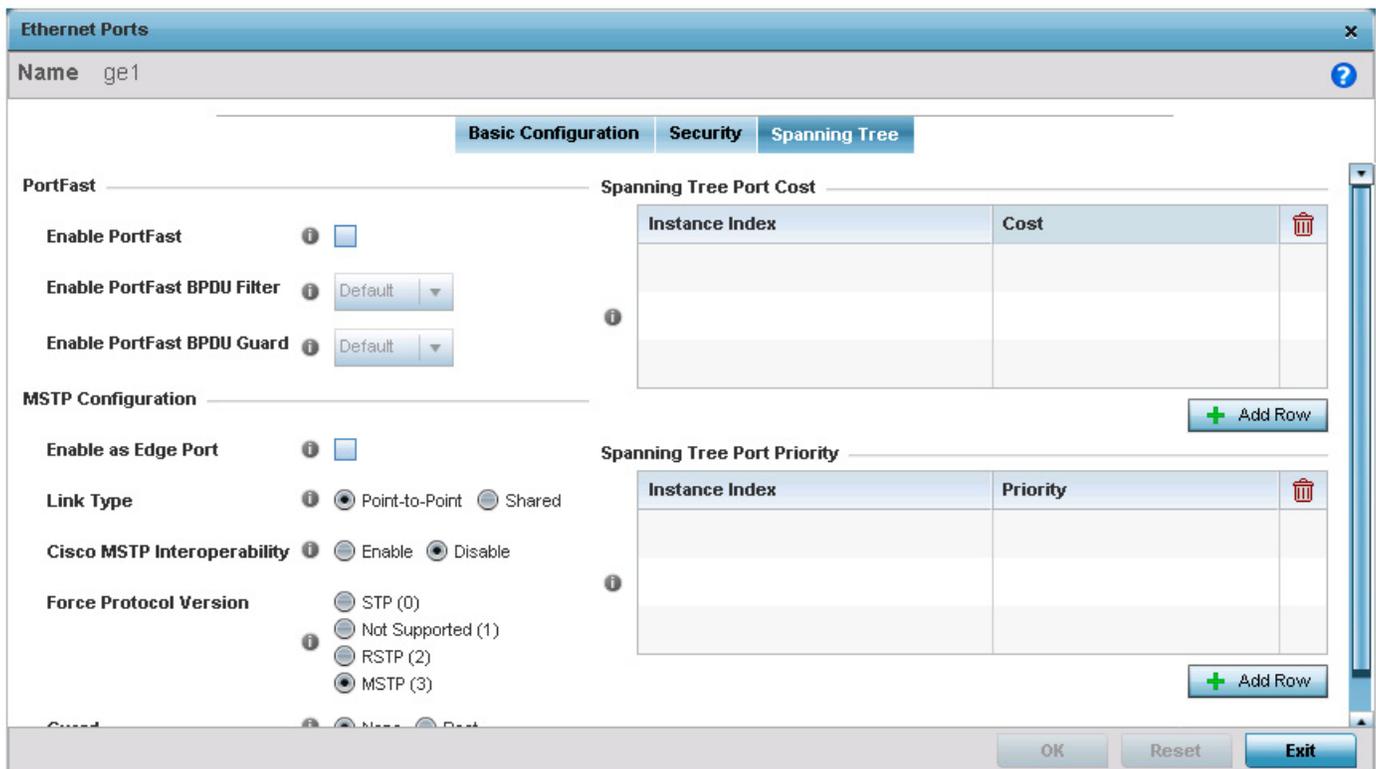
*Rapid Spanning Tree Protocol* (RSTP) (IEEE 802.1w standard) is an evolution over the standard STP where the primary aim was to reduce the time taken to respond to topology changes while being backward compatible with STP. *PortFast* quickly changes the port state from *Blocked* to *Forwarding* to allow traffic while the STP calculation occurs.

*Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there is just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with multiple *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST)

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI message conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.



**Figure 5-16** Ethernet Ports - Spanning Tree tab

19. Refer to the **PortFast** field to define the following:

<p><b>Enable PortFast</b></p>	<p>PortFast reduces the time taken for a port to complete STP. PortFast must only be enabled on ports on the wireless controller which are directly connected to a server/workstation and not to another hub or controller. PortFast can be left unconfigured on the access point.</p> <p>Select this option to enable drop-down menus for both the Enable PortFast BPDU Filter and Enable PortFast BPDU Guard options. This setting is disabled by default.</p>
<p><b>Enable PortFast BPDU Filter</b></p>	<p>MSTP BPDUs are messages exchanged when controllers gather information about the network topology during STP scan. When enabled, PortFast enabled ports do not transmit or receive BPDU messages. 'Default' sets the PortFast BPDU Filter value to the bridge's BPDU filter value.</p> <p>Select <i>Enable</i> to invoke a BPDU filter for this PortFast enabled port channel.</p>
<p><b>Enable PortFast BPDU Guard</b></p>	<p>When enabled, PortFast enabled ports are forced to shut down when they receive BPDU messages. When set to <i>Default</i> sets the PortFast BPDU Guard value to the bridge's BPDU guard value.</p>

20. Refer to the **MSTP Configuration** field to define the following:

<p><b>Enable as Edge Port</b></p>	<p>Select to enable the port as an Edge Port for MSTP. An Edge Port is a port known to connect to a LAN which has no other bridges attached to it or is directly connected to a user device.</p>
-----------------------------------	--

<b>Link Type</b>	Select either the <i>Point-to-Point</i> or <i>Shared</i> radio button. Selecting <i>Point-to-Point</i> indicates the port should be treated as connected to a point-to-point link. Selecting <i>Shared</i> means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point is a point-to-point link. Point-to-Point is the default setting.
<b>Cisco MSTP Interoperability</b>	Select to enable or disable interoperability with CISCO's implementation of MSTP which is incompatible with standard MSTP.
<b>Force Protocol Version</b>	Select the STP protocol to use with this port. Select <i>Not Supported</i> to disable STP on this port.
<b>Guard</b>	The Root Guard mechanism prevents election of roots other than those designated as roots in a network. When this port receives a better BPDU, port state becomes <i>Blocked</i> . It retains this state till the port no longer receives the better BPDUs and the state is changed to <i>Forwarding</i> . Select <i>Root</i> to enable this feature. Select <i>None</i> to disable this feature.

21. Refer to the **Spanning Tree Port Cost** table.

Define an *Instance Index* using the spinner control and then set the cost. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

<b>Speed</b>	<b>Default Path Cost</b>
<=100000 bits/sec	2000000000
<=1000000 bits/sec	200000000
<=10000000 bits/sec	20000000
<=100000000 bits/sec	2000000
<=1000000000 bits/sec	200000
<=10000000000 bits/sec	20000
<=100000000000 bits/sec	2000
<=1000000000000 bits/sec	200
<=10000000000000 bits/sec	20
>100000000000000 bits/sec	2

22. Select **+ Add Row** as needed to include additional indexes.

23. Refer to the **Spanning Tree Port Priority** table.

Define an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, the greater the likelihood of the port becoming a designated port.

24. Select **+ Add Row** needed to include additional indexes.

25. Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration.



<b>VLAN</b>	Displays the numerical VLAN ID associated with each listed interface.
<b>IP Address</b>	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.

Once the configurations of existing Virtual Interfaces have been reviewed, determine whether a new interface requires creation, or an existing Virtual Interface requires edit or deletion.

6. Select **Add** to define a new Virtual Interface configuration, **Edit** to modify the configuration of an existing Virtual Interface or **Delete** to permanently remove a selected Virtual Interface.

**Figure 5-18** Virtual Interfaces - Basic Configuration tab

The *Basic Configuration* screen displays by default regardless of whether a new Virtual Interface is being created or an existing one is being modified.

7. If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID from 1 - 4094.
8. Define the following parameters from within the **Properties** field:

<b>Description</b>	Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Either select the <i>Disabled</i> or <i>Enabled</i> radio button to define this interface's current status within the network. When set to <i>Enabled</i> , the Virtual Interface is operational and available. The default value is <i>Disabled</i> .

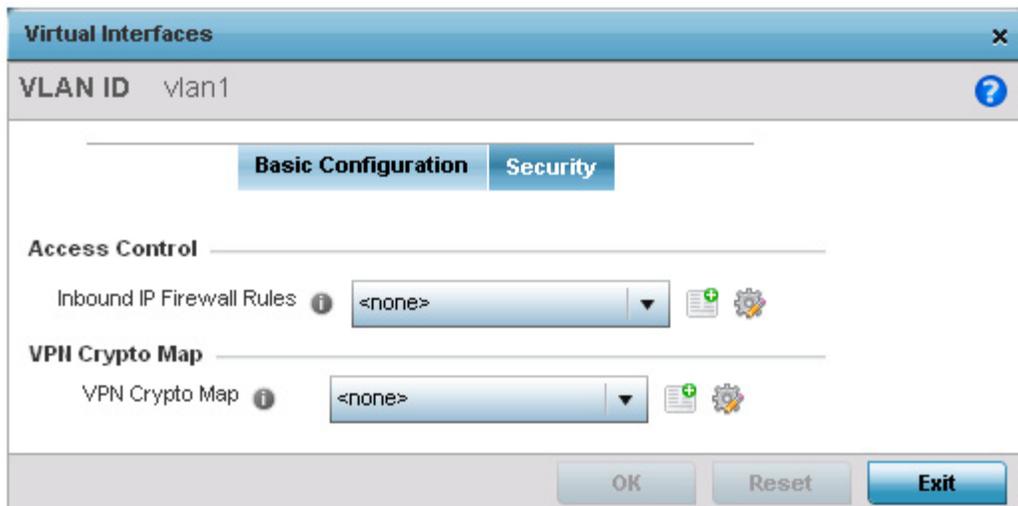
9. Set the following network information from within the **IP Addresses** field:

<b>Enable Zero Configuration</b>	The access point can use Zero Config for IP assignments on an individual virtual interface basis. Select <i>Primary</i> to use Zero Config as the designated means of providing an IP address, this eliminates the means to assign one manually. Selecting <i>Secondary</i> is preferred when wanting the option to either use Zero Config or manual assignments. Zero Configuration (or Zero Config) is a wireless connection utility included with Microsoft Windows XP and later as a service that dynamically selects a network to connect based on a user's preference and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device.
<b>Primary IP Address</b>	Define the IP address for the VLAN associated Virtual Interface.
<b>Use DHCP to Obtain IP</b>	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
<b>Use DHCP to obtain Gateway/DNS Servers</b>	Select this option to allow DHCP to obtain a default gateway address, and DNS resource for one virtual interface. This setting is disabled by default and only available when the <i>Use DHCP to Obtain IP</i> option is selected.
<b>Secondary Addresses</b>	Use the Secondary Addresses parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

10. Define the **Network Address Translation (NAT)** direction.

Select either the *Inside*, *Outside* or *None* radio buttons.

- *Inside* - The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
  - *Outside* - Packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.
  - *None* - No NAT activity takes place. This is the default setting.
11. Select **OK** button to save the changes to the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.
12. Select the **Security** tab.



**Figure 5-19** Virtual Interfaces - Security tab

- Use the **Inbound IP Firewall Rules** drop-down menu to select the firewall rule configuration to apply to this Virtual Interface.

The firewall inspects and packet traffic to and from connected clients.

If a firewall rule does not exist suiting the data protection needs of this Virtual Interface, select the Create icon to define a new firewall rule configuration or the Edit icon to modify an existing configuration. For more information, see [Wireless Firewall on page 8-2](#).

- Use the **VPN Crypto Map** drop-down menu to select and assign a VPN crypto map entry to this virtual interface. The VPN Crypto Map entry defines the type of VPN connection and its parameters. For more information, see [Defining Profile VPN Settings on page 5-104](#).
- Select the **OK** button located at the bottom right of the screen to save the changes to the *Security* screen. Select **Reset** to revert to the last saved configuration.

### 5.2.5.3 Port Channel Configuration

#### ▶ Profile Interface Configuration

The access point's profile can be applied to customize the port channel configurations as part of its interface configuration.

To define a port channel configuration for an access point profile:



The screenshot shows the 'Port Channels' configuration window with the 'Basic Configuration' tab selected. The 'Name' field is 'port-channel1'. Under 'Properties', 'Description' is 'Portchannel 1', 'Admin Status' is 'Enabled', 'Speed' is 'Automatic', and 'Duplex' is 'Automatic'. Under 'Client Load Balancing', 'Port Channel Load Balance' is 'Source/Destination IP'. Under 'Switching Mode', 'Mode' is 'Access', 'Native VLAN' is '1', 'Tag Native VLAN' is unchecked, and 'Allowed VLANs' is empty. The window has 'OK', 'Reset', and 'Exit' buttons at the bottom right.

**Figure 5-21** Port Channels - Basic Configuration tab

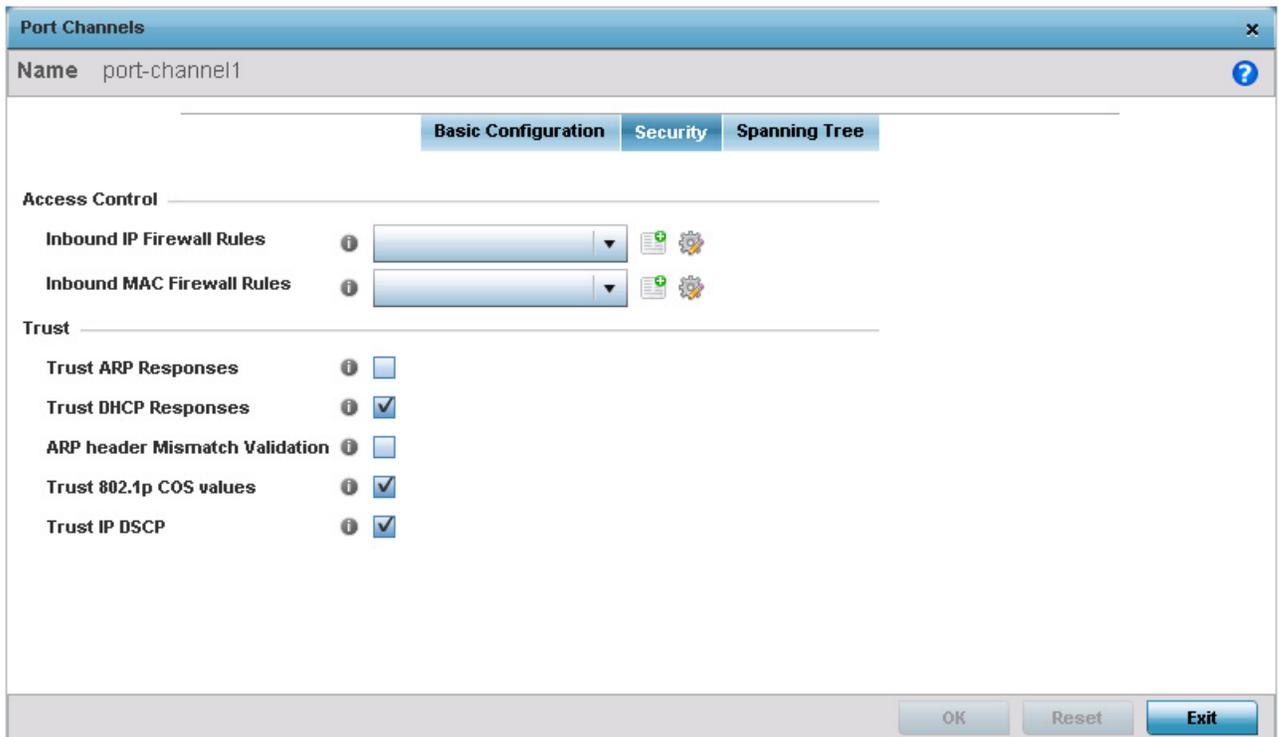
7. Set the following port channel **Properties**:

<b>Description</b>	Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port channel as active to the controller profile it supports. Select the <i>Disabled</i> radio button to disable this port channel configuration within the profile. It can be activated at any future time when needed. The default setting is disabled.
<b>Speed</b>	Select the speed at which the port channel can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> , <i>1000 Mbps</i> . Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select Automatic to enable the port channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.
<b>Duplex</b>	Select either <i>Half</i> , <i>Full</i> or <i>Automatic</i> as the duplex option. Select Half duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a Full duplex transmission, a Half duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port channel at the same time. Using Full duplex, the port channel can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.

8. Use the **Port Channel Load Balance** drop-down menu within the **Client Load Balancing** field to define whether port channel load balancing is conducted using a *Source/Destination IP* or a *Source/Destination MAC* as criteria. Source/Destination IP is the default setting.
9. Define the following **Switching Mode** parameters to apply to the port channel configuration:

<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port channel. If <i>Access</i> is selected, the port channel accepts packets only from the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to <i>Trunk</i> , the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. <i>Access</i> is the default setting.
<b>Native VLAN</b>	Use the spinner control to define a numerical ID from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using trunk mode. The default value is 1.
<b>Tag the Native VLAN</b>	Select this option to tag the native VLAN. Access points support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs to. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
<b>Allowed VLANs</b>	Selecting <i>Trunk</i> as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the port channel.

10. Select **OK** to save the changes made to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.
11. Select the **Security** tab.



**Figure 5-22** Port Channels - Security tab

12. Refer to the **Access Control** field. As part of the port channel's security configuration, Inbound IP and MAC address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **Inbound MAC Firewall Rules** drop-down menus to select firewall rules to apply to this profile's port channel configuration.

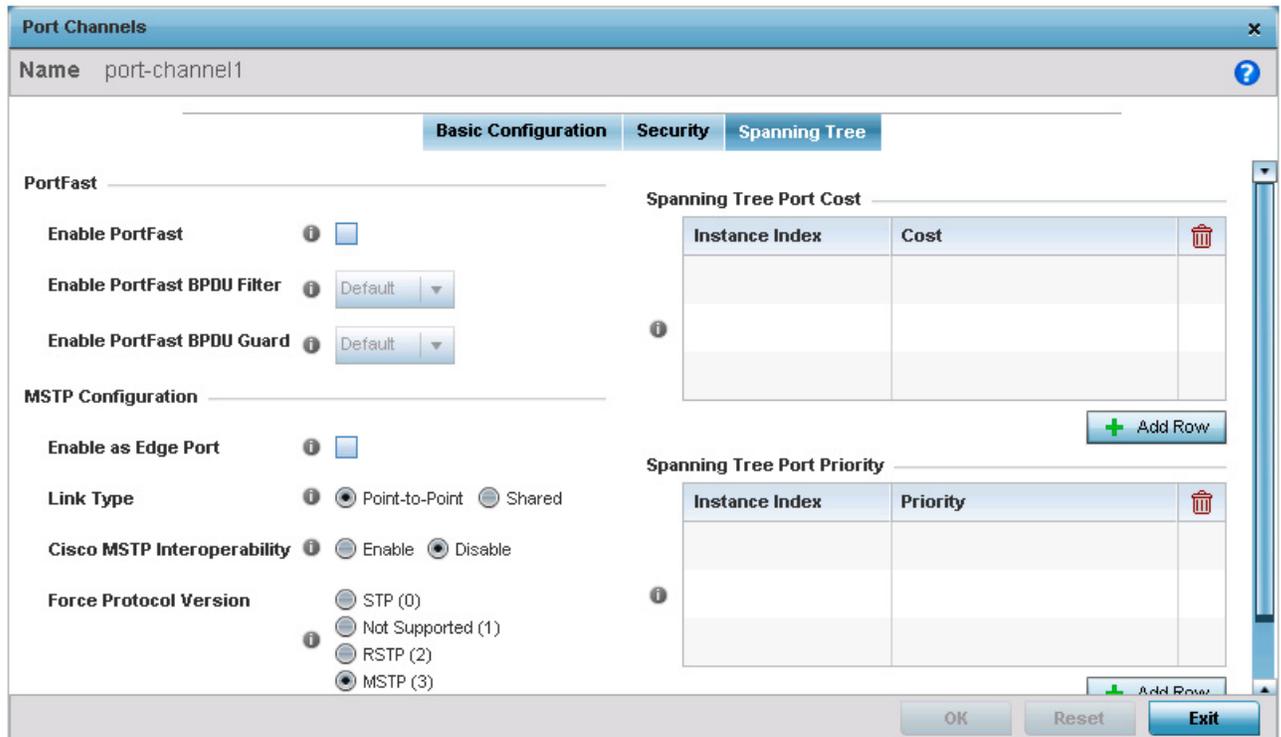
The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

If a firewall rule does not exist suiting the data protection needs of the target port channel configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing firewall rule configuration. For more information, see [Wireless Firewall on page 8-2](#).

13. Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	Select this option to enable ARP trust on this port channel. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the managed network. The default value is disabled.
<b>Trust DHCP Responses</b>	Select this option to enable DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
<b>ARP header Mismatch Validation</b>	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
<b>Trust 802.1p COS values</b>	Select this option to enable 802.1p COS values on this port channel. The default value is enabled.
<b>Trust IP DSCP</b>	Select this option to enable IP DSCP values on this port channel. The default value is enabled.

14. Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.
15. Select the **Spanning Tree** tab.



**Figure 5-23** Port Channels - Spanning Tree tab

16. Define the following **PortFast** parameters for the port channel's MSTP configuration:

<b>Enable PortFast</b>	PortFast reduces the time required for a port to complete a MSTP state change from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller directly connected to a server/workstation and not another hub or controller. PortFast can be left unconfigured on an access point. Select this option to enable drop-down menus for both the <i>Enable PortFast BPDU Filter</i> and <i>Enable PortFast BPDU Guard</i> options. This setting is disabled by default.
<b>PortFast BPDU Filter</b>	Select <i>Enable</i> to invoke a BPDU filter for this PortFast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. The default setting is None.
<b>PortFast BPDU Guard</b>	Select <i>Enable</i> to invoke a BPDU guard for this PortFast enabled port channel. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. The default setting is None.

17. Set the following **MSTP Configuration** parameters for the port channel:

<b>Enable as Edge Port</b>	Select this option to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port channel. This setting is disabled by default.
----------------------------	--

<b>Link Type</b>	Select either the <i>Point-to-Point</i> or <i>Shared</i> radio button. Selecting <i>Point-to-Point</i> indicates the port should be treated as connected to a point-to-point link. Selecting <i>Shared</i> means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point is a point-to-point link. <i>Point-to-Point</i> is the default setting.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
<b>Force Protocol Version</b>	Sets the protocol version to either <i>STP(0)</i> , <i>Not Supported(1)</i> , <i>RSTP(2)</i> or <i>MSTP(3)</i> . <i>MSTP</i> is the default setting.
<b>Guard</b>	Determines whether the port channel enforces root bridge placement. Setting the guard to <i>Root</i> ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior <i>Bridge Protocol Data Units</i> (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.

18. Refer to the **Spanning Tree Port Cost** table.

Define an Instance Index using the spinner control and then set the cost. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

<b>Speed</b>	<b>Default Path Cost</b>
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000
<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

19. Select **+ Add Row** as needed to include additional indexes.

20. Refer to the **Spanning Tree Port Priority** table.

Define an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, a greater likelihood of the port becoming a designated port.

21. Select **+ Add Row** needed to include additional indexes.

22. Select **OK** to save the changes made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.



<b>RF Mode</b>	Displays whether each listed radio is operating in the 802.11a/n or 802.11b/g/n radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client-bridge, it will be listed as a client bridge and does not provide typical WLAN support. The radio band is set from within the Radio Settings tab.
<b>Channel</b>	Lists the channel setting for the radio. <i>Smart</i> is the default setting. If set to Smart, the access point scans non-overlapping channels listening for beacons from other access points. After the channels are scanned, it selects the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level.
<b>Transmit Power</b>	Lists the transmit power for each radio. The column displays <i>smart</i> if set for dynamic Smart RF support.

6. If required, select a radio configuration and select the **Edit** button to modify the radio configuration.

The screenshot shows the 'Radios' configuration window with the 'Radio Settings' tab selected. The 'Properties' section includes fields for Description (radio1), Admin Status (Enabled), Radio QoS Policy (default), and Association ACL. The 'Radio Settings' section includes RF Mode (2.4GHz-wlan), DFS Revert Home (checked), Lock RF Mode (unchecked), and Channel (smart). The 'WLAN Properties' section includes Beacon Interval (100), DTIM Interval BSSID (2), RTS Threshold (2347), Short Preamble (unchecked), Guard Interval (Any), Probe Response Rate (follow-probe-request), and Probe Response Retry (checked). The 'Channel Scanning' section includes Enable Off Channel Scan (unchecked) and Off Channel Scan list for 5 GHz (34, 36, 36+).

**Figure 5-25** Access Point Radio - Radio Settings tab

The **Radio Settings** tab displays by default.

7. Define the following radio configuration parameters from within the **Properties** field:

<b>Description</b>	Provide or edit a description (1 - 64 characters) for the radio that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Either select the <i>Disabled</i> or <i>Enabled</i> radio button to define this radio's current status within the network. When defined as Enabled, the access point is operational and available for client support.

<b>Radio QoS Policy</b>	Use the drop-down menu to specify an existing QoS policy to apply to the access point radio in respect to its intended radio traffic. If there's no existing suiting the radio's intended operation, select the Create icon to define a new QoS policy that can be applied to this profile.
<b>Association ACL</b>	Use the drop-down menu to specify an existing Association ACL policy to apply to the access point radio. An Association ACL is a policy-based <i>Access Control List</i> (ACL) that either prevents or allows wireless clients from connecting to a access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the packet is compared against any applied ACLs to verify the packet has the required permissions to be forwarded based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped. Select the Create icon to define a new Association ACL that can be applied to this profile.

8. Set the following profile **Radio Settings** for the selected access point radio:

<b>RF Mode</b>	Set the mode to either <i>2.4 GHz WLAN</i> or <i>5.0 GHz WLAN</i> support depending on the radio's intended client support. Set the mode to <i>sensor</i> if using the radio for rogue device detection. The radio cannot support rogue detection when one of the radios is functioning as a WIPS sensor. To set a radio as a detector, disable Sensor support on the other access point radio. Set the mode to <i>client-bridge</i> to configure the radio as a client bridge. A client bridge enables the access point to connect to a 3rd party access point and bridge frames to it.
<b>Lock RF Mode</b>	Select this option to lock Smart RF operation for this radio. The default setting is disabled, as Smart RF utilization will impact throughput.
<b>Channel</b>	Use the drop-down menu to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select <i>Smart</i> for the radio to scan non-overlapping channels listening for beacons from other access points. After the channels are scanned, the radio selects the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level. The default value is Smart.  Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, only appear when using an AP8232 or AP7522 or AP7532, and are unique to the 80 MHz band.
<b>DFS Revert Home</b>	Select this option to enable a radio to return back to its original channel. <i>Dynamic Frequency Selection</i> (DFS) prevents a radio from operating in a channel where radar signals are present. When radar signals are detected in a channel, the radio changes its channel of operation to another channel. The radio cannot use the channel it has moved from for the next thirty (30) minutes. When selected, the radio can return back to its original channel of operation once the thirty minute period is over. When not selected, the radio cannot return back to its original channel of operation even after the mandatory thirty minute evacuation period is over.
<b>Transmit Power</b>	Set the transmit power of the selected radio. If using a dual or three radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value.

<b>Antenna Gain</b>	Set the antenna from 0.00 - 30.00 dBm. The access point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Motorola Solutions recommends that only a professional installer set the antenna gain. The default value is 0.00.
<b>Antenna Mode</b>	Set the number of transmit and receive antennas on the access point. 1x1 is used for transmissions over just the single "A" antenna. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. 1xAll is used when transmission occurs on one antenna and is received on all receiving antennas. The default setting is dynamic based on the access point model deployed and its transmit power settings.
<b>Enable Antenna Diversity</b>	Select this option to enable the radio to have antenna diversity for transmit frames at non 802.11n data rates. This setting is disabled by default.
<b>Wireless Client Power</b>	Select this option to manually set the radio's transmission power (in dBm) to connected clients. The setting is disabled by default.
<b>Dynamic Chain Selection</b>	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.
<b>Data Rates</b>	<p>Once the radio band is provided, the drop-down menu populates with rate options depending on the 2.4 or 5.0 GHz band selected. If the radio band is set to <i>Sensor</i> or <i>Detector</i>, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5.0 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).</p> <p>If dedicating an AP81XX model radio to either 2.4 or 5 GHz support, a <i>Custom Rates</i> option is available to set a <i>modulation and coding scheme</i> (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If <i>Basic</i> is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a Supported rate and that option is greyed out. If <i>Basic</i> is not selected, any combination of MCS0-7, MCS8-15 and MCS16-23 can be supported, including a case where MCS0-7 and MCS16-23 are selected and not MCS8-15. The MCS0-7 and MCS8-15 options are available to each support access point. However, the MCS16-23 option is only available to AP81XX model access points and its ability to provide 3x3x3 MIMO support.</p> <p>For more information on the 802.11n rates, see section <a href="#">MCS Data Rates on page 5-51</a>.</p>

<b>Radio Placement</b>	Use the drop-down menu to specify whether the radio is located <i>Indoors</i> or <i>Outdoors</i> . The placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions. The default setting is <i>Indoors</i> .
<b>Max Clients</b>	Use the spinner control to set a maximum permissible number of clients to connect with this access point radio. The available range is from 1- 256 for AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models and from 1-128 for AP6511 and AP6521 models.
<b>Rate Selection Methods</b>	Use the drop-down menu to specify the algorithm to use for rate selection. Select <i>Standard</i> to use the standard rate selection algorithm. Select <i>Opportunistic</i> to use the Opportunistic rate selection algorithm.



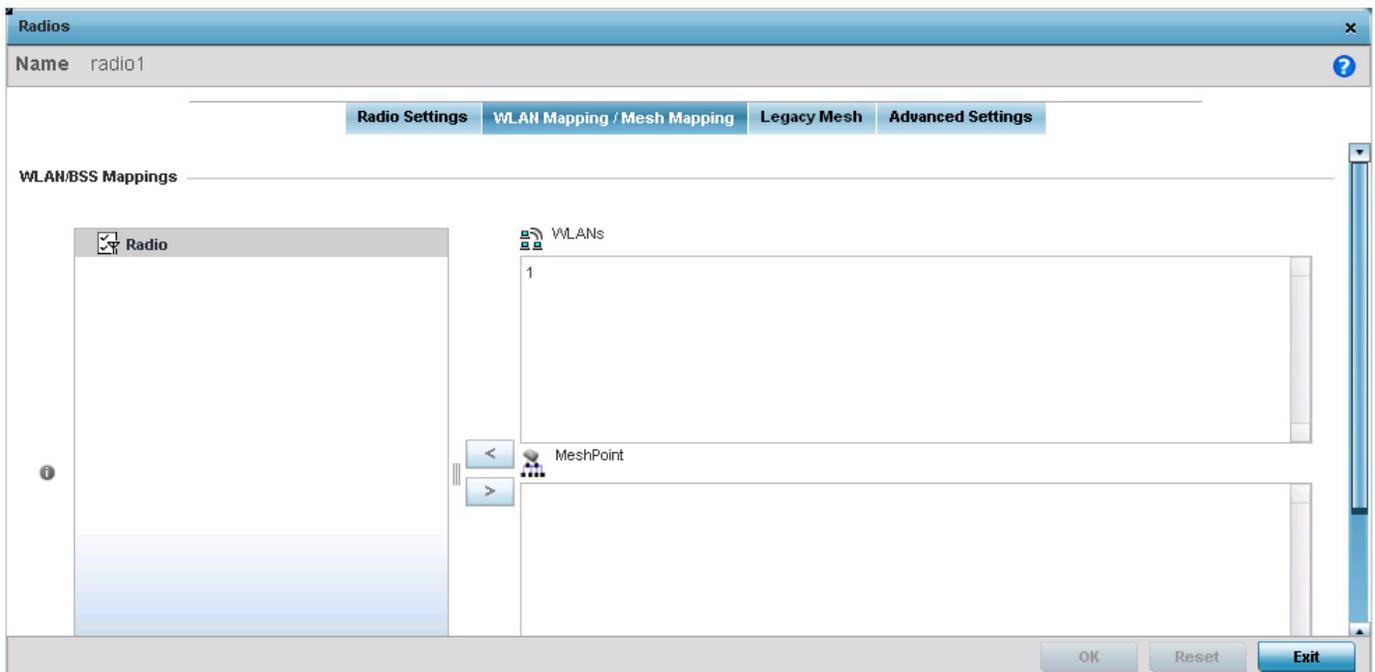
**NOTE:** AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 client connections to a single access point radio. AP6511 and AP6521 model access points (both single radio models) can support up to 128 client connections to a single radio.

9. Set the following profile **WLAN Properties** for the selected access point radio:

<b>Beacon Interval</b>	Set the interval between radio beacons in milliseconds (either 50, 100 or 200). A beacon is a packet broadcast by adopted radios to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds.
<b>DTIM Interval BSSID</b>	Set a DTIM Interval to specify a period for <i>Delivery Traffic Indication Messages</i> (DTIM). A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates broadcast and multicast frames (buffered at the access point) are soon to arrive. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.

<b>RTS Threshold</b>	<p>Specify a <i>Request To Send</i> (RTS) threshold (from 1 - 2,347 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a <i>Clear To Send</i> (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.</p> <p>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.</p> <p>Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.</p>
<b>Short Preamble</b>	<p>If using an 802.11bg radio, select this option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. The default value is disabled.</p>
<b>Guard Interval</b>	<p>Use the drop-down menu to specify a <i>Long</i> or <i>Any</i> guard interval. The guard interval is the space between symbols (characters) being transmitted. The guard interval is there to eliminate <i>inter-symbol interference</i> (ISI). ISI occurs when echoes or reflections from one symbol interfere with another symbol. Adding time between transmissions allows echo's and reflections to settle before the next symbol is transmitted. A shorter guard interval reduces overhead and increases data rates by up to 10%. The default value is Long.</p>
<b>Probe Response Rate</b>	<p>Use the drop-down menu to specify the data transmission rate used for the transmission of probe responses. Options include, <i>highest-basic</i>, <i>lowest-basic</i> and <i>follow-probe-request</i> (default setting).</p>
<b>Probe Response Retry</b>	<p>Select this option to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.</p>

10. Use the **Feed WLAN Packets to Sensor** drop-down menu to radio's tap mode of operation. Options include, *Off*, *Inline* and *Promiscuous*. The default setting is Off.
11. Select the **WLAN Mapping/Mesh Mapping** tab.



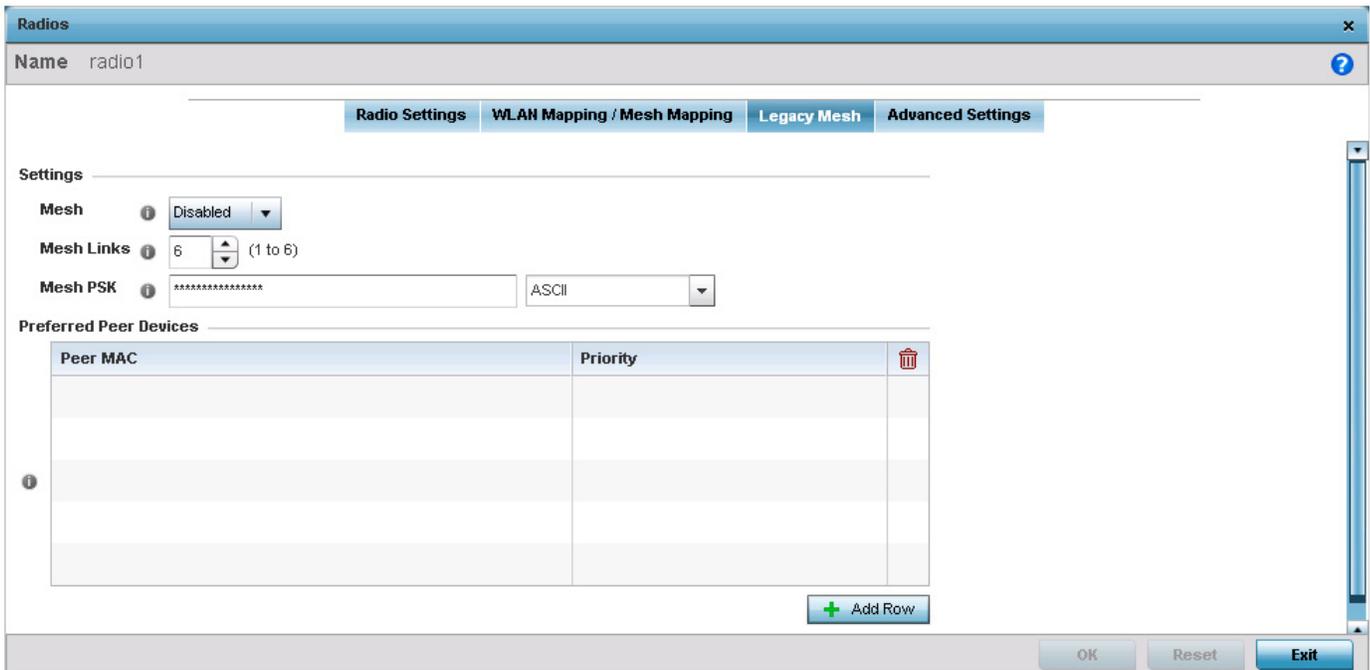
**Figure 5-26** Access Point Radio - WLAN Mapping tab

12. Refer to the **WLAN Mapping/Mesh Mapping** field to set WLAN BSSID assignments for an existing access point deployment.

Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n/c radio.

Each supported access point model can support up to 8 BSS IDs.

13. Select **Advanced Mapping** to list all the available BSSIDs for the radio.
14. Select **Create New WLAN** to open a dialog where new WLANs are created.
15. Select **Create New MeshPoint** to open a dialog where new Mesh Points are created.
16. Select the **OK** button located at the bottom right of the screen to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.
17. Select the **Legacy Mesh** tab.



**Figure 5-27** Access Point Radio - Mesh Legacy tab

Use the *Legacy Mesh* screen to define how mesh connections are established and the number of links available amongst access points within the mesh network.

18. Define the following **Mesh Settings**:

<b>Mesh</b>	Options include <i>Client</i> , <i>Portal</i> and <i>Disabled</i> . Select <i>Client</i> to scan for mesh portals, or nodes that have connection to portals, and then connect through them. <i>Portal</i> operation begins beaconing immediately and accepts connections from other mesh supported nodes. Select <i>Portal</i> when setting a mesh connection between two Standalone APs. The default value is <i>Disabled</i> .
<b>Mesh Links</b>	Use the spinner control to define the number of mesh links (1 -6) an access point radio will attempt to create. The default settings is 3 links.
<b>Mesh PSK</b>	Use the text box to enter the mesh's secret key. Select either <i>ASCII</i> or <i>HEX</i> from the drop-down menu. Click the <i>Show</i> option to display the secret key entered in the <i>Mesh PSK</i> field.

19. Refer to the **Preferred Peer Devices** table and select **+ Add Row** to define MAC addresses representing peer devices for preferred mesh connection. Use the Priority spinner control to set a priority (1 -6) for connection preference.
20. Select the **OK** button located at the bottom right of the screen to save the changes to the Mesh configuration. Select **Reset** to revert to the last saved configuration.
21. Select the **Advanced Settings** tab.

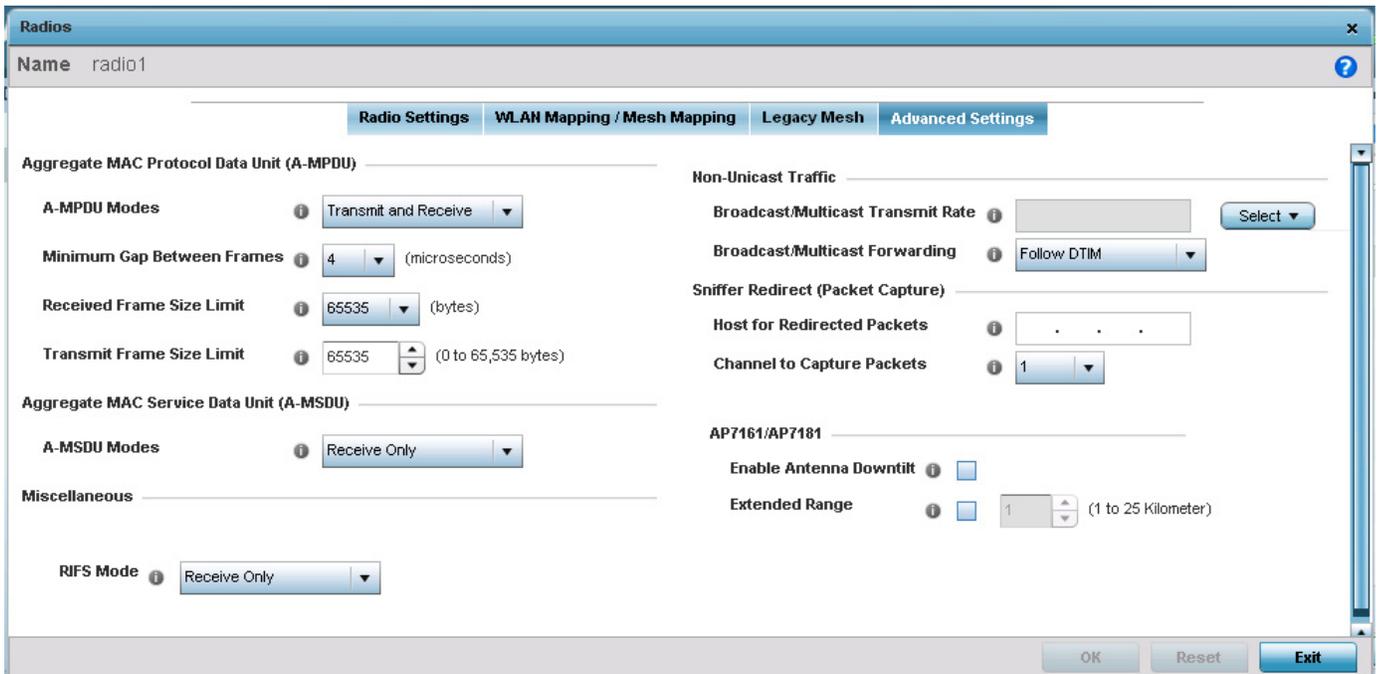


Figure 5-28 Access Point Radio - Advanced Settings tab

22. Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** field to define how MAC service frames are aggregated by the access point radio.

<b>A-MPDU Modes</b>	Use the drop-down menu to define the A-MPDU mode supported. Options include <i>Transmit Only</i> , <i>Receive Only</i> , <i>Transmit and Receive</i> and <i>None</i> . The default value is <i>Transmit and Receive</i> . Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit (or both).
<b>Minimum Gap Between Frames</b>	Use the drop-down menu to define the minimum gap between A-MPDU frames (in microseconds). The default value is 4 microseconds.
<b>Received Frame Size Limit</b>	If a support mode is enable allowing A-MPDU frames to be received, define an advertised maximum limit for received A-MPDU aggregated frames. Options include 8191, 16383, 32767 or 65535 bytes. The default value is 65535 bytes.
<b>Transmit Frame Size Limit</b>	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is from 2000 - 65,535 bytes). The default value is 65535 bytes.

23. Use the **Aggregate MAC Service Data Unit (A-MSDU)** drop-down menu to set the supported A-MSDU mode. Available modes include *Receive Only* and *Transmit and Receive*. *Transmit and Receive* is the default value. Using *Transmit and Receive*, frames up to 4 KB can be sent and received. The buffer limit is not configurable.

24. Set the following **Aeroscout Properties** for the selected access point radio:

<b>Forward</b>	Use the Forward option to forward Aeroscout packets to the server.
<b>MAC to be forwarded</b>	Use the text area to provide a MAC address that identifies that the packet is received from Aeroscout tags.

25. Set the following **Ekahau Properties** for the selected access point radio:

<b>Forwarding Host</b>	Use the Forward Host text area to provide the IP address of the Ekahau Engine.
------------------------	--

<b>Forwarding Port</b>	Use the Forward Port spinner to configure the port on which to forward captured packets to the Ekahau Engine.
<b>MAC to be forwarded</b>	Use the text area to provide a MAC address that identifies that the packet is received from Ekahau tags.

26. Set the following **Non-Unicast Traffic** values for the profile's supported access point radio and its connected wireless clients:

<b>Broadcast/Multicast Transmit Rate</b>	Use the <i>Select</i> drop-down menu to launch a sub screen to define the data rate broadcast and multicast frames are transmitted. Seven different rates are available if the not using the same rate for each BSSID, each with a separate menu.
<b>Broadcast/Multicast Forwarding</b>	Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is Follow DTIM.

27. Refer to the **Sniffer Redirect (Packet Capture)** field to define the radio's captured packet configuration.

<b>Host for Redirected Packets</b>	If packets are re-directed from an access point radio, define an IP address of a resource (additional host system) used to capture the re-directed packets. This address is the numerical (non DNS) address of the host used to capture the re-directed packets.
<b>Channel to Capture Packets</b>	Use the drop-down menu to specify the channel used to capture re-directed packets. The default value is channel 1.

28. Select the **Enable Off Channel Scan** radio button to permit scans on non designated channels for this radio. While this affords the access point a greater likelihood of catching an unauthorized device, it does consume more bandwidth. The default setting is disabled. Set the following **Channel Scanning** properties for the selected access point radio:

<b>Off Channel Scan list for 5 GHz</b>	Use the drop-down menu to select the channels to scan in the 5 GHz band when performing off channel scans.
<b>Off Channel Scan list for 2.4 GHz</b>	Use the drop-down menu to select the channels to scan in the 2.4 GHz band when performing off channel scans.
<b>Max Multicast</b>	Use the spinner to set the number of multicast and broadcast packets queued in the radio's queue, when exceeded, off channel scan is skipped during the current scanning interval.
<b>Scan Interval</b>	Use the spinner to set the off channel scan interval in number of dtim periods.
<b>Sniffer Redirect</b>	Use <i>Sniffer Redirect</i> text area to provide the IP address of a remote host where the captured off channel scan packets are re-directed.

29. Set the following **AP7161/AP7181** specific values:

<b>Enable Antenna Downtilt</b>	Antenna Downtilt is used where there is a need for a separation between the 2.4 GHz and 5.0 GHz bands. The 2.4 GHz band is tilted by 15 degrees (up/down tilt) using software. Select to enable downtilt.
<b>Extend Range</b>	Select to enable extending the range of the access points. The access point uses various technologies to extend their service range. Use the spinner to set the range of service. Range can be 1 - 25 Kilometers.

30. Select the **OK** button located at the bottom right of the screen to save the changes to the **Advanced Settings** screen.  
Select **Reset** to revert to the last saved configuration.

#### 5.2.5.4.1 MCS Data Rates

► *Access Point Radio Configuration*

802.11n MCS rates are defined as follows both with and without *short guard intervals* (SGI):

**Table 5.1** MCS-1Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30
2	1	19.5	21.7	40.5	45
3	1	26	28.9	54	60
4	1	39	43.4	81	90
5	1	52	57.8	108	120
6	1	58.5	65	121.5	135
7	1	65	72.2	135	150

**Table 5.2** MCS-2Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240
6	2	117	130	243	270
7	2	130	144.4	270	300

**Table 5.3** MCS-3Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	3	19.5	21.7	40.5	45
1	3	39	43.3	81	90
2	3	58.5	65	121.5	135

**Table 5.3** MCS-3Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
3	3	78	86.7	162	180
4	3	117	130.7	243	270
5	3	156	173.3	324	360
6	3	175.5	195	364.5	405
7	3	195	216.7	405	450

802.11ac MCS rates are defined as follows both with and without *short guard intervals* (SGI):

**Table 5.4** MCS-802.11ac (theoretical throughput for single spatial streams)

<b>MCS Index</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>	<b>80 MHz No SGI</b>	<b>80MHz With SGI</b>
0	6.5	7.2	13.5	15	29.3	32.5
1	13	14.4	27	30	58.5	65
2	19.5	21.7	40.5	45	87.8	97.5
3	26	28.9	54	60	117	130
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260
6	58.5	65	121.5	135	263.3	292.5
7	65	72.2	135	150	292.5	325
8	78	86.7	162	180	351	390
9	n/a	n/a	180	200	390	433.3

### 5.2.5.5 WAN Backhaul Configuration

#### ▶ Profile Interface Configuration

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a Cellular Wide Area Network. The AP7131N model access point has a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses *point to point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

The following 3G cards are supported:

- Verizon V740
- Verizon PC770
- Sprint C777
- Novatel Merlin XU870
- Sierra Aircard 880E
- Telstra Elite Mobile Broadband
- Option GT Ultra Express
- Vodaphone Mobile Connect E3730
- Aircard 503
- Aircard 504 / AT & T 890

To define a WAN Backhaul configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Interface** menu and select **WAN Backhaul**.

**WAN (3G) Backhaul**

**WAN Interface Name** \* wwan1

**Enable WAN (3G)**  Disabled  Enabled

**Basic Settings**

**Username**

**Password**   Show

**Access Point Name (APN)**

**Authentication Type** CHAP

**Network Address Translation (NAT)**

**NAT Direction**  Inside  Outside  None

**Security Settings**

**Inbound IP Firewall Rules**

**VPN Crypto Map**

**Default Route Priority**

**WWAN Default Route Priority**  (1 to 8,000)

**Figure 5-29** Profile Interface - WAN Backhaul screen

5. Refer to the **WAN (3G) Backhaul** configuration to specify the access point's WAN card interface settings:

<b>WAN Interface Name</b>	Displays the WAN Interface name for the WAN 3G Backhaul card.
<b>Enable WAN (3G)</b>	Select this option to enable 3G WAN card support on the access point. A supported 3G card must be connected for this feature to work.

6. Define the following authentication parameters from within the **Basic Settings** field:

<b>Username</b>	Provide username for authentication support by the cellular data carrier.
<b>Password</b>	Provide password for authentication support by the cellular data carrier.
<b>Access Point Name (APN)</b>	Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols such as Europe, the Middle East and Asia.
<b>Authentication Type</b>	Use the drop-down menu to specify the authentication type used by the cellular data provider. Supported authentication options include <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

7. Use the **NAT Direction** field to specify the NAT direction used with the access point's WAN card. Options include *Inside*, *Outside* or *None*. The default is *None*.

8. Configure the **Inbound IP Firewall Rules**. Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the Create icon to define a new rule configuration or the Edit icon to modify an existing rule.
9. Select the **VPN Crypto Map** to use with this WWAN configuration. Use the drop-down menu to apply an existing crypto map configuration to this WWAN interface.
10. Use the **WWW Default Route Priority** spinner to set a default route priority for this interface. The default value is 3000.
11. Select **OK** to save the changes to the *Advanced Settings* screen. Select **Reset** to revert to the last saved configuration.

### 5.2.5.5.1 WAN Backhaul Deployment Considerations

#### ▶ *WAN Backhaul Configuration*

Before defining a profile's WAN Backhaul configuration refer to the following deployment guidelines to ensure these configuration are optimally effective:

- If the WAN card does not connect after a few minutes after a *no shutdown*, check the access point's syslog for a *detected ttyUSB0 No such file* event. If this event has occurred, linux didn't detect the card. Re-seat the card.
- If the WAN card has difficulty connecting to an ISP (syslog shows that it retries LCP ConfReq for a long time), ensure the SIM card is still valid and is plugged in correctly.
- If a modem doesn't responding with an OK during the dialing sequence, the WAN card is in an unknown state and will not accept a command. Re-seat the card and begin the dialup sequence again until the card is recognized.
- If encountering a *panic* when conducting a hotplug, power off the access point for one minute. The access point could continue to panic or detect the descriptor of the last utilized WAN card. Thus, it's a good idea to clear the panic state by temporarily disconnecting then re-applying access point power.
- If wanting to unplug the WAN card, ensure sure you shutdown first, as the probability of getting a panic is reduced. With the new high-speed WAN cards currently being utilized, the chances of getting a panic significantly increase.

## 5.2.5.6 PPPoE Configuration

### ▶ Profile Interface Configuration

*PPP over Ethernet* (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG supported controllers and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN were to fail.



**NOTE:** Access points with PPPoE enabled continue to support VPN, NAT, PBR and 3G failover over the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.



**NOTE:** PPPoE is supported on AP6522, AP6522M, AP6532, AP6562, AP71XX, AP7522, AP7532, AP81XX and AP82XX models and is not available on AP6511 and AP6521 model access points.

---

---

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic flow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

To create a PPPoE point-to-point configuration:

1. Select the **Configuration** tab from the Web UI.
  2. Select **Devices**.
  3. Select **System Profile** from the options on left-hand side of the UI.
  4. Expand the **Interface** menu and select **PPPoE**.
-

**Basic Settings**

Enable PPPoE  Disabled  Enabled

Service

DSL Modem Network (VLAN)  (1 to 4,094)

Client IP Address

**Authentication**

Username

Password   Show

Authentication Type

**Connection**

Maximum Transmission Unit (MTU)  (500 to 1,492)

Client Idle Timeout   (1 to 1,093)

Keep Alive

**Network Address Translation (NAT)**

NAT Direction  Inside  Outside  None

**Security Settings**

Inbound IP Firewall Rules

VPN Crypto Map

**Default Route Priority**

PPPoE Default Route Priority  (1 to 8,000)

**Figure 5-30** Profile Interface - PPPoE screen

5. Use the **Basic Settings** field to enable PPPoE and define a PPPoE client.

<b>Enable PPPoE</b>	Select <i>Enable</i> to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled.
<b>Service</b>	Enter the 128 character maximum PPPoE client service name issued by the service provider.
<b>DSL Modem Network (VLAN)</b>	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 - 4,094. The default VLAN is VLAN1.
<b>Client IP Address</b>	Provide the numerical (non hostname) IP address of the PPPoE client.

6. Define the following **Authentication** parameters for PPPoE client interoperation:

<b>Username</b>	Provide the 64 character maximum username used for authentication support by the PPPoE client.
<b>Password</b>	Provide the 64 character maximum password used for authentication by the PPPoE client. Use the <i>Show</i> option to view the actual characters comprising the password.
<b>Authentication Type</b>	Use the drop-down menu to specify authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

7. Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

<b>Maximum Transmission Unit (MTU)</b>	Set the PPPoE client <i>Maximum Transmission Unit</i> (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
<b>Client Idle Timeout</b>	Set a timeout in either <i>Seconds</i> (1 - 65,535), <i>Minutes</i> (1 - 1,093) or <i>Hours</i> . The access point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes.
<b>Keep Alive</b>	Select this option to ensure the point-to-point connection to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

8. Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

*Network Address Translation* (NAT) converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point router maps its local (*Inside*) network addresses to WAN (*Outside*) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is None (neither inside or outside).

9. Define the following **Security Settings** for the PPPoE configuration:

<b>Inbound IP Firewall Rules</b>	Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the <i>Create</i> icon to define a new rule configuration or the <i>Edit</i> icon to modify an existing rule. For more information, see <a href="#">Wireless Firewall on page 8-2</a> .
<b>VPN Crypto Map</b>	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

10. Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

11. Select **OK** to save the changes to the PPPoE screen. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

## 5.2.6 Profile Network Configuration

### ▶ *System Profile Configuration*

Setting an access point profile's network configuration is a large task comprised of numerous administration activities.

An access point profile network configuration process consists of the following:

- *DNS Configuration*
- *ARP*
- *L2TPv3 Profile Configuration*
- *IGMP Snooping*
- *Quality of Service (QoS)*
- *Spanning Tree Configuration*
- *Routing*
- *Dynamic Routing (OSPF)*
- *Forwarding Database*
- *Bridge VLAN*
- *Cisco Discovery Protocol Configuration*
- *Link Layer Discovery Protocol Configuration*
- *Miscellaneous Network Configuration*
- *Alias*

Before beginning any of the profile network configuration activities described in the sections above, review the configuration and deployment considerations available in *Profile Network Configuration and Deployment Considerations on page 5-103*.

---

### 5.2.6.1 DNS Configuration

#### ► Profile Network Configuration

*Domain Naming System (DNS)* is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server does not know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (www.domainname.com).

To define the DNS configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **DNS**.

**Domain Name System (DNS)**

**Domain Name**

**Enable Domain Lookup**

**DNS Server Forwarding**

**DNS Servers**

Name Servers	IP
<input type="text" value="0 . 0 . 0 . 0"/>	<a href="#">Clear</a>
<input type="text" value="0 . 0 . 0 . 0"/>	<a href="#">Clear</a>
<input type="text" value="0 . 0 . 0 . 0"/>	<a href="#">Clear</a>

**OK** **Reset**

**Figure 5-31** Network - DNS screen

5. Provide a default **Domain Name** used when resolving DNS names. The name cannot exceed 64 characters.
6. Set the following DNS configuration data:

<b>Enable Domain Lookup</b>	Select this option to enable DNS. When enabled, human friendly domain names can be converted into numerical IP destination addresses. This feature is enabled by default.
<b>DNS Server Forwarding</b>	Select to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by the access point's own DNS resources. This feature is disabled by default.

7. In the **Name Servers** field, provide the IP addresses of up to three DNS server resources available to the access point.

- Select **OK** to save the changes made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.6.2 ARP

#### ► Profile Network Configuration

*Address Resolution Protocol (ARP)* is a protocol for mapping an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, the gateway uses ARP to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to the destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply. ARP updates the ARP cache for future reference, and then sends the packet to the MAC address that replied.

To define an ARP supported configuration:

- Select the **Configuration** tab from the Web UI.
- Select **Devices**.
- Select **System Profile** from the options on left-hand side of the UI.
- Expand the **Network** menu and select **ARP**.
- Select **+ Add Row** from the lower right-hand side of the screen to populate the ARP table with rows used to define ARP network address information.

**Address Resolution Protocol (ARP)**

Switch VLAN Interface	IP Address	MAC Address	Device Type	
1	192.168.13.2	00-43-8D-62-71-AB	DHCP Server	

**+ Add Row**

**OK** **Reset**

**Figure 5-32** Network - ARP screen

- Set the following parameters to define the ARP configuration:

<b>Switch VLAN Interface</b>	Use the spinner control to select a VLAN for an address requiring resolution.
<b>IP Address</b>	Define the IP address used to fetch a MAC Address.
<b>MAC Address</b>	Displays the target MAC address that's subject to resolution. This is the MAC used for mapping an IP address to a MAC address that's recognized on the network.

<b>Device Type</b>	Specify the device type the ARP entry supports ( <i>Host, Router or DHCP Server</i> ). Host is the default setting.
--------------------	---

7. Select the **OK** button located at the bottom right of the screen to save the changes to the ARP configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.6.3 L2TPv3 Profile Configuration

#### ► Profile Network Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables WING supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WING devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. Access points support an Ethernet VLAN pseudowire type exclusively.



**NOTE:** A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.



**NOTE:** If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

To define an L2TPV3 configuration for an access point profile:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **L2TPv3**.

The screenshot shows the 'General Settings' section of the L2TPv3 configuration interface. It includes the following fields:

- Host Name:** A text input field with a pencil icon for editing.
- Router ID:** A dropdown menu labeled 'IP Address' showing the value '0 . 0 . 0 . 0'.
- UDP Listen Port:** A spin box showing the value '1024' with a range of '(1,024 to 65,535)'. It includes information and help icons.
- Tunnel Bridging:** A checkbox with an information icon.

At the bottom right of the window, there are 'OK' and 'Reset' buttons.

**Figure 5-33** Network - L2TPv3 screen - General tab

5. Set the following **General Settings** for an L2TPv3 profile configuration:

<b>Host Name</b>	Define a 64 character maximum hostname to specify the name of the host that's sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
<b>Router ID</b>	Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunnelled peer.
<b>UDP Listen Port</b>	Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,353.
<b>Tunnel Bridging</b>	Select this option to enable or disable bridge packets between two tunnel end points. This setting is disabled by default.

6. Select the **L2TPv3 Tunnel** tab.



8. Either select **Add** to create a new L2TPv3 tunnel configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

**L2TPv3 Tunnel**

Name \*

**Settings**

Local IP Address

MTU  (128 to 1,460)

Use Tunnel Policy

Local HostName

Local Router ID

Establishment Criteria

VRRP Group  (1 to 255)

Critical Resource 

--

**Peer**

Peer ID	Router ID	Host Name	Encapsulation	Peer IP Address	UDP Port	

**Session**

Name	Pseudowire ID	Traffic Source Type	Traffic Source Value	Native VLAN	

**Figure 5-35** Network - L2TPv3 screen - Add T2TP Tunnel Configuration

9. If creating a new tunnel configuration, assign it a 31 character maximum **Name**.
10. Define the following **Settings** required for the L2TP tunnel configuration:

<b>Local IP Address</b>	Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests.
-------------------------	---

<b>MTU</b>	Set the <i>maximum transmission unit</i> (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU between 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data.
<b>Use Tunnel Policy</b>	Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available a new policy can be created or an existing one can be modified. For more information, refer to <a href="#">L2TP V3 Configuration on page 7-8</a> .
<b>Local Hostname</b>	Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages.
<b>Local Router ID</b>	Specify the router ID sent in tunnel establishment messages with a potential peer device.
<b>Establishment Criteria</b>	<p>Configure establishment criteria for creating a tunnel between the device and the NOC. This criteria ensures only one tunnel is created between two sites where the tunnel is established between the vrrp-master/cluster master/rf-domain manager at the remote site and the controller at the NOC. The tunnel is created based on the role of the remote peer.</p> <ul style="list-style-type: none"> <li>• <i>always</i> – The tunnel is always created irrespective of the role of the local device.</li> <li>• <i>vrrp-master</i> – The tunnel is only created when the local device is a VRRP master.</li> <li>• <i>cluster-master</i> – The tunnel is only created when the local device is a cluster master.</li> <li>• <i>rf-domain-manager</i> – The tunnel is only created when the local device is a RF-Domain manager.</li> </ul> <p>In all the above cases, if the local device goes offline for any reason, the tunnel is brought down.</p>
<b>VRRP Group</b>	This field is enabled only when the <i>Establishment Criteria</i> is set to <i>vrrp-master</i> . Use the spinner to select the VRRP group.
<b>Critical Resource</b>	<p>Enter the critical resources required for creating and maintaining a L2TPv3 tunnel. A tunnel is only established when all critical resources for the tunnel to be operational are available at the time when the tunnel is created. If any one of the listed critical resources goes down, the tunnel is disabled.</p> <p>When a tunnel is established, the listed critical resources are checked for availability. Tunnel establishment is started if the critical resources are available. Similarly, for incoming tunnel termination requests, listed critical resources are checked and tunnel terminations are only allowed when the critical resources are available.</p> <p>For more information on managing critical resources, see <a href="#">Profile Critical Resources on page 5-139</a>.</p>

11. Refer to the **Peer** table to review the configurations of the peers available for tunnel connection.

Select **+ Add Row** to populate the table with a maximum of two peer configurations.

The screenshot shows a dialog box titled "Add Row" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Peer ID:** A spinner control set to "1" with a range indicator "(1 to 2)".
- Peer IP Address:** A text input field with a blue information icon (i) to its left.
- Host Name:** A text input field with a blue information icon (i) to its left.
- Router ID:** A text input field with a blue pencil icon to its left and a dropdown menu set to "Integer/Range".
- Encapsulation:** A dropdown menu set to "IP" with a blue information icon (i) to its left.
- UDP Port:** A spinner control set to "1701" with a blue information icon (i) to its left.
- Isec Secure:** A checkbox that is currently unchecked, with a blue information icon (i) to its left.
- Isec Gateway:** A text input field with a blue information icon (i) to its left.

At the bottom of the dialog, there are two buttons: "OK" and "Exit".

**Figure 5-36** Network - L2TPv3 screen - Add T2TP Peer Configuration

12. Define the following **Peer** parameters:

<b>Peer ID</b>	Define the primary peer ID used to set the primary and secondary peer for tunnel failover. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or Router ID matches.
<b>Peer IP Address</b>	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment.
<b>Host Name</b>	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process.
<b>Router ID</b>	Specify the router ID sent in tunnel establishment messages with this specific peer.
<b>Encapsulation</b>	Select either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port.
<b>IPSEC Secure</b>	Select this option to provide IPSEC security for the tunnel.
<b>IPSEC Gateway</b>	Enter the IP address/Hostname for the IPSEC gateway.

13. Select **OK** to save the peer configuration.

14. Refer to the **Session** table to review the configurations of the peers available for tunnel connection.

Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

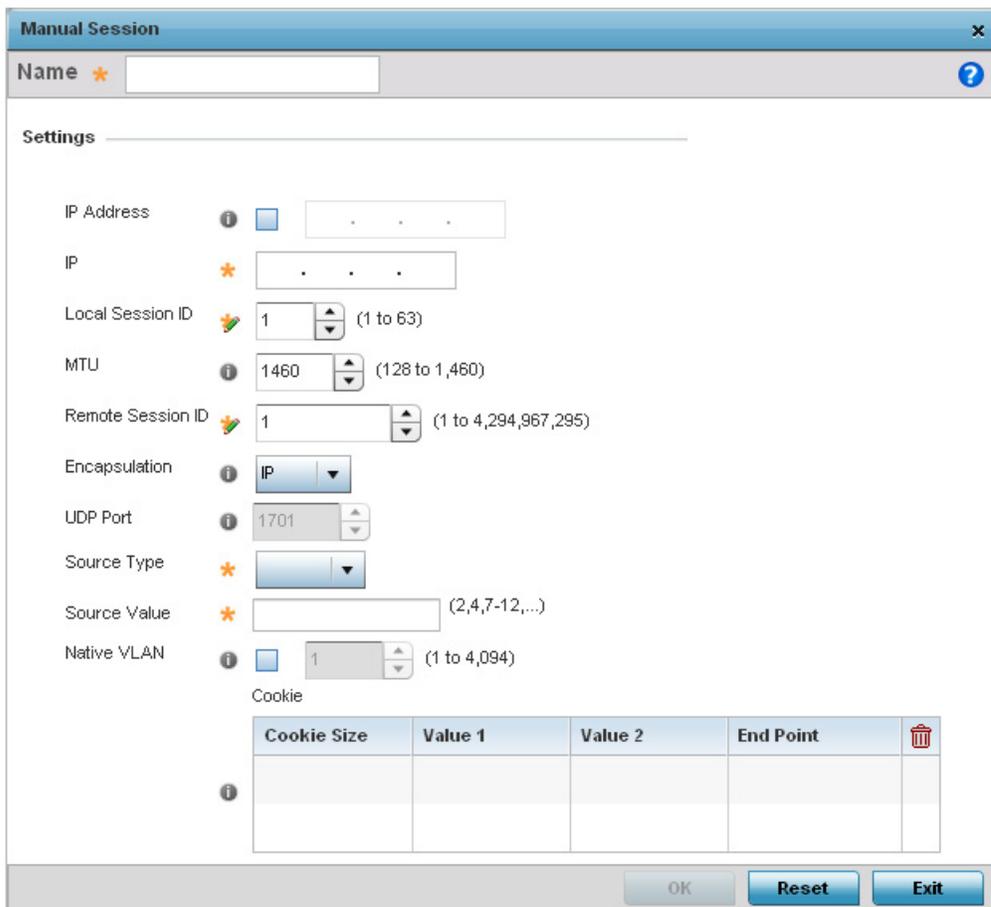
15. Define the following **Session** parameters:

<b>Name</b>	Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed.
-------------	--



<b>Local Session ID</b>	Displays the numeric identifier assigned to each listed tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.
<b>MTU</b>	Displays each sessions's <i>maximum transmission unit</i> (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
<b>Name</b>	Lists the name assigned to each listed manual session.
<b>Remote Session ID</b>	Lists the remote session ID passed in the establishment of the tunnel session.

19. Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.



**Figure 5-38** Network - L2TPv3 screen, Add T2TP Peer Configuration

20. Set the following session parameters:

<b>Name</b>	Define a 31 character maximum name for this tunnel session. Each session name represents a single data stream.
-------------	--

<b>IP Address</b>	Specify the IP address used as a tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, the tunnel would use the IP address received in the tunnel create request.
<b>IP</b>	Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel.
<b>Local Session ID</b>	Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in session establishment message to the L2TP peer.
<b>MTU</b>	Define the session maximum transmission unit (MTU) as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
<b>Remote Session ID</b>	Use the spinner control to set the remote session ID passed in the establishment of the tunnel session. Assign an ID from 1 - 4,294,967,295.
<b>Encapsulation</b>	Select either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running.
<b>Source VLAN</b>	Define the VLAN range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames.
<b>Native VLAN</b>	Select this option to define the native VLAN that will not be tagged.

21. Select the **+ Add Row** button to set the following:

<b>Cookie Size</b>	Set the size of the cookie field within each L2TP data packet. Options include 0, 4 and 8. The default setting is 0.
<b>Value 1</b>	Set the cookie value first word.
<b>Value 2</b>	Set the cookie value second word.
<b>End Point</b>	Define whether the tunnel end point is local or remote.

22. Select **OK** to save the changes to the session configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.6.4 IGMP Snooping

### ► Profile Network Configuration

*Internet Group Management Protocol* (IGMP) is a protocol to establish and maintain multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP Snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.

To configure IGMP Snooping:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **IGMP Snooping**.

The screenshot shows the IGMP Snooping configuration interface. It is divided into two main sections: 'General' and 'IGMP Querier'. In the 'General' section, 'Enable IGMP Snooping' and 'Forward Unknown Multicast Packets' are both checked. The 'IGMP Querier' section has 'Enable IGMP Querier' unchecked. The 'IGMP Version' is set to 3. The 'IGMP Query Interval' is set to 1 minute. The 'IGMP Robustness Variable' is set to 2. The 'Maximum Response Time' is set to 10 seconds. The 'Other Querier Time Expiry' is set to 1 minute. At the bottom right, there are 'OK' and 'Reset' buttons.

**Figure 5-39** IGMP Snooping screen

5. Set the following parameters to configure general IGMP Snooping values:

<b>Enable IGMP Snooping</b>	Select this option to enable IGMP Snooping on the access point. This feature is enabled by default.
<b>Forward Unknown Multicast Packets</b>	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the <i>Unknown Multicast Forward</i> feature is also disabled for the selected VLANs. This is enabled by default.

6. Set the following for **IGMP Querier** configuration:

<b>Enable IGMP Querier</b>	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then forwarded on that port. An AP71XX model access point can also be an IGMP querier.
<b>IGMP Version</b>	Use the spinner control to set the IGMP version compatibility to IGMP version 1, 2 or 3. The default IGMP version is 3.
<b>IGMP Query Interval</b>	Sets the IGMP query interval. This parameter is used only when the querier functionality is enabled. Define an interval value in <i>Seconds</i> (1 - 18000 seconds), <i>Minutes</i> (1 - 300 minutes) or <i>Hours</i> (1 - 5 hours) up to maximum of 5 hours. The default value is 60 seconds.
<b>IGMP Robustness Variable</b>	Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value is 2.
<b>Maximum Response Time</b>	Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
<b>Other Querier Time Expiry</b>	Specify an interval in either <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

7. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

### 5.2.6.5 Quality of Service (QoS)

#### ► Profile Network Configuration

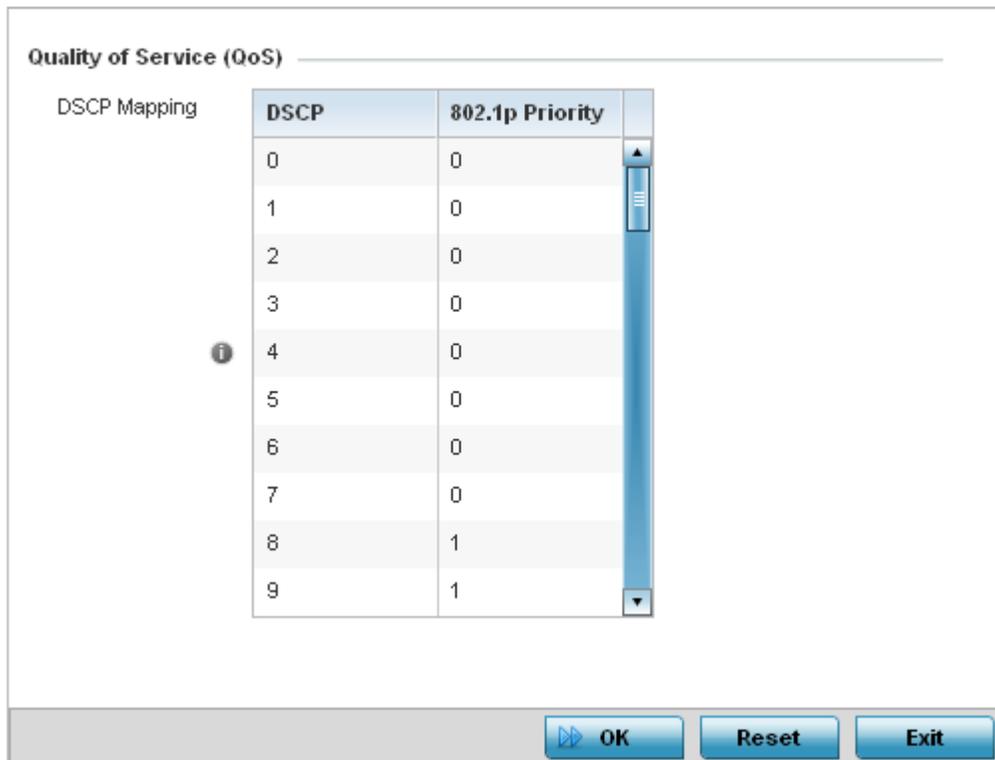
The uses different *Quality of Service (QoS)* screens to define WLAN and device radio QoS configurations. The *System Profiles > Network > QoS* facility is separate from WLAN and radio QoS configurations, and is used to configure the priority of different DSCP packet types.

QoS values are required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit *Differentiated Service Code Point (DSCP)* code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior applied to a packet.

To define an QoS configuration for DSCP mappings:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Quality of Service (QoS)**.



**Figure 5-40** Network - Quality of Service (QoS) screen

5. Set the following parameters for IP DSCP mappings for untagged frames:

<b>DSCP</b>	Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification.
-------------	--

<b>802.1p Priority</b>	<p>Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are:</p> <ul style="list-style-type: none"> <li>• 0 – Best Effort</li> <li>• 1 – Background</li> <li>• 2 – Spare</li> <li>• 3 – Excellent Effort</li> <li>• 4 – Controlled Load</li> <li>• 5 – Video</li> <li>• 6 – Voice</li> <li>• 7 – Network Control</li> </ul>
------------------------	---

6. Use the spinner controls within the **802.1p Priority** field for each DSCP row to change its priority value.
7. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

### 5.2.6.6 Spanning Tree Configuration

#### ▶ Profile Network Configuration

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with multiple *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To define the spanning tree configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Spanning Tree**.

**MSTP Configuration**

MSTP Enable

Max Hop Count  (7 to 127)

MST Config Name

MST Revision Level  (0 to 255)

Cisco MSTP Interoperability

Hello Time  (1 to 10)

Forward Delay  (4 to 30)

Maximum Age  (6 to 40)

**PortFast**

PortFast BPDUs Filter

PortFast BPDUs Guard

**Error Disable**

Enable Recovery

Recovery Interval  (10 to 1,000,000)

**Spanning Tree Instance**

Instance	Priority	

**Spanning Tree Instance VLANs**

Instance	VLANs	

OK Reset Exit

**Figure 5-41** Network - Spanning Tree screen

5. Set the following **MSTP Configuration** parameters:

<b>MSTP Enable</b>	Select this option to enable MSTP for this profile. MSTP is disabled by default. Enable this setting if requiring different (groups) of VLANs with the profile supported network segment.
<b>Max Hop Count</b>	Define the maximum number of hops the BPDU considers valid in the spanning tree topology. The available range is from 7 -127. The default setting is 20.
<b>MST Config Name</b>	Define a 64 character maximum name for the MST region as an identifier for the configuration.
<b>MST Revision Level</b>	Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.

<b>Hello Time</b>	Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and start/stop port forwarding as required.
<b>Forward Delay</b>	Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately start to forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay it goes through the listening and learning states. The time spent in the listening and learning states is defined by the forward delay (15 seconds by default).
<b>Maximum Age</b>	Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40. The default setting is 20.

6. Define the following **PortFast** parameters for the profile configuration:

<b>PortFast BPDU Filter</b>	Select <i>Enable</i> to invoke a BPDU filter for this PortFast enabled port. Enabling the BPDU filter ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly, and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is <i>Disabled</i> .
<b>PortFast BPDU Guard</b>	Select <i>Enable</i> to invoke a BPDU guard for the PortFast enabled port. Enabling the BPDU Guard means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly, and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is <i>Disabled</i> .

7. Define the following **Error Disable** settings:

<b>Enable Recovery</b>	Select this option to enable an error disable timeout resulting from a BPDU guard. This setting is disabled by default.
<b>Recovery Interval</b>	Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds, with a default setting of 300.

8. Use the **Spanning Tree Instance** table to add indexes to the spanning tree topology.

Add up to 16 indexes and use the **Priority** setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.

9. Use the **Spanning Tree Instance VLANs** table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.
10. Select the **OK** button located at the bottom right of the screen to save the changes. Select Reset to revert to the last saved configuration.

## 5.2.6.7 Routing

### ► Profile Network Configuration

Routing is the process of selecting IP paths to send access point managed network traffic. Use the *Routing* screen to set destination IP and gateway addresses enabling assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the resource space required to maintain address pools.

To create static routes:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Routing**.

**IP Routing**

IP Routing

**Policy Based Routing**

Policy Based Routing   

**Static Routes**

Network Address	Gateway	Default Gateway	



**Default Route Priority**

Static Default Route Priority  (1 to 8,000)

DHCP Client Default Route Priority  (1 to 8,000)

Enable Routing Failure

Use Network Address of 0.0.0.0/0 to Set Default Gateway

**Figure 5-42** Network - Routing screen

5. Select **IP Routing** to enable static routes using IP addresses. This option is enabled by default.

6. Select the **Policy Based Routing** policy to apply to this profile. Select the **Create** icon to create a policy based route or select the **Edit** icon to edit an existing policy after selecting it in the drop-down list.
7. Select **Add Row +** as needed to include single rows with in the static IPv4 route table.
8. Add IP addresses and network masks in the **Network Address** column of the **Static Routes** table.
9. Provide the **Gateway** used to route traffic.
10. Refer to the **Default Route Priority** field and set the following parameters:

<b>Static Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is weight assigned to this route versus others that have been defined. The default setting is 100.
<b>DHCP Client Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000.
<b>Enable Routing Failure</b>	When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default.

11. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

### 5.2.6.8 Dynamic Routing (OSPF)

#### ► Profile Network Configuration

*Open Shortest Path First* (OSPF) is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers.

OSPF uses a route table managed by the link *cost* (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability. Setting a cost value provides a dynamic way to load balancing traffic between routes of equal cost.

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can be defined as:

- *stub area* - A stub area is an area which does not receive route advertisements external to the *autonomous system* (AS), and routing from within the area is based entirely on a default route.
- *totally-stub* - A totally stubby area does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there's only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- *non-stub* - A non-stub area imports autonomous system external routes and sends them to other areas. However, it still cannot receive external routes from other areas.
- *nssa* - NSSA is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- *totally nssa* - Totally nssa is an NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an *autonomous system boundary router* (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a *point-to-point* link, OSPF knows it is sufficient, and the link stays *up*. If on a *broadcast* link, the router waits for election before determining if the link is functional.

To define a dynamic routing configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Dynamic Routing**.

The screenshot shows the OSPF Settings tab with the following configuration:

- Enable OSPF:
- Router ID: [ . . . ]
- Auto-Cost: 1 (1 to 4,294,967)
- Passive Mode on All Interfaces:
- Passive Removed: VLAN ID 1, [ ]
- Passive Mode: VLAN ID 1, [ ]
- VRRP State Check:

**OSPF Overload Protection**

- Number of Routes: 2048 (1 to 4,294,967,295)
- Retry Count: 5 (1 to 32)
- Retry Time Out: 60 (1 to 3,600)
- Reset Time: 360 (1 to 86,400)

Buttons: OK, Reset

**Figure 5-43** Network - OSPF Settings tab

5. Enable/disable OSPF and provide the following dynamic routing settings:

<b>Enable OSPF</b>	Select this option to enable OSPF for this access point. OSPF is disabled by default.
<b>Router ID</b>	Select this option to define a router ID (numeric IP address) for this access point. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
<b>Auto-Cost</b>	Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1.
<b>Passive Mode on All Interfaces</b>	When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default.
<b>Passive Removed</b>	If <i>enabling</i> Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF non passive interfaces. Multiple VLANs can be added to the list.
<b>Passive Mode</b>	If <i>disabling</i> Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list.

<b>VRRP State Check</b>	Select this option to enable checking VRRP state. If the interface's VRRP state is not <i>Backup</i> , then the interface is published via OSPF.
-------------------------	--

6. Set the following **OSPF Overload Protection** settings:

<b>Number of Routes</b>	Use the spinner controller to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295.
<b>Retry Count</b>	Set the maximum number of retries (OSPF resets) permitted before the OSPF process is shut down. The available range is from 1 - 32. The default setting is 5.
<b>Retry Time Out</b>	Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds.
<b>Reset Time</b>	Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds.

7. Set the following **Default Information**:

<b>Originate</b>	Select this option to make the default route a distributed route. This setting is disabled by default.
<b>Always</b>	Enabling this settings continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default.
<b>Metric Type</b>	Select this option to define the exterior metric type (1 or 2) used with the default route.
<b>Route Metric</b>	Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting a given route.

8. Refer to the **Route Redistribution** table to set the types of routes used by OSPF.

Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include *connected*, *kernel* and *static*.

Select the **Metric Type** option to define the exterior metric type (1 or 2) used with the route redistribution. Select the **Metric** option to define route metric used with the redistributed route.

9. Use the **OSPF Network** table to define networks (IP addresses) to connect using dynamic routes.

Select the **+ Add Row** button to populate the table. Add the IP address and mask of the **Network(s)** participating in OSPF. Additionally, define the OSPF area (IP address) to which the network belongs.

10. Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route learnt from OSPF.

11. Select the **Area Settings** tab.

An OSPF *Area* contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.

OSPF Settings			Area Settings	Interface Settings
Area ID	Authentication Type	Type		
0.0.0.12	None	nssa		
Type to search in tables			Row Count: 0	
			Add	Edit
			Delete	

Figure 5-44 Network - Area Settings tab

12. Review existing **Area Settings** configurations using:

<b>Area ID</b>	Displays either the IP address or integer representing the OSPF area.
<b>Authentication Type</b>	Lists the authentication schemes used to validate the credentials of dynamic route connections.
<b>Type</b>	Lists the OSPF area type in each listed configuration.

13. Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

OSPF Area
✕

Area ID ★

Integer
?

Authentication Type i None

Type i non-stub

Default Cost i  1 (1 to 16,777,215)

Translate Type i translate-candidate

Range i . . . / ↓

OK
Reset
Exit

Figure 5-45 Network - OSPF Area Configuration screen

14. Set the **OSPF Area** configuration.

<b>Area ID</b>	Use the drop-down menu and specify either an IP address or Integer for the OSPF area.
<b>Authentication Type</b>	Select either <i>None</i> , <i>simple-password</i> or <i>message-digest</i> as credential validation scheme used with the OSPF dynamic route. The default setting is <i>None</i> .
<b>Type</b>	Set the OSPF area type as either <i>stub</i> , <i>totally-stub</i> , <i>nssa</i> , <i>totally-nssa</i> or <i>non-stub</i> .
<b>Default Cost</b>	Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215.
<b>Translate Type</b>	Define how messages are translated. Options include <i>translate-candidate</i> , <i>translate-always</i> and <i>translate-never</i> . The default setting is <i>translate-candidate</i> .
<b>Range</b>	Specify a range of addresses for routes matching address/mask for OSPF summarization.

15. Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

16. Select the **Interface Settings** tab.

OSPF Settings   Area Settings   <b>Interface Settings</b>						
Name	Type	Description	Admin Status	VLAN	IP Address	
vlan1	VLAN		✓ Enabled	1	dhcp	
Type to search in tables					Row Count: 0	
			Add		Edit	
			Delete			

**Figure 5-46** Network - Interface Settings tab

17. Review existing **Interface Settings**.

<b>Name</b>	Displays the name defined for the interface configuration.
<b>Type</b>	Displays the type of interface.
<b>Description</b>	Lists each interface's 32 character maximum description.
<b>Admin Status</b>	A green check mark defines the interface as active and currently enabled with the profile. A red "X" defines the interface as currently disabled and not available for use.
<b>VLAN</b>	Lists the VLAN IDs set for each listed OSPF route virtual interface.
<b>IP Address</b>	Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.

18. Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.

The screenshot shows the 'Virtual Interfaces' configuration window for 'vlan1'. It has two tabs: 'Basic Configuration' (selected) and 'Security'. Under 'Properties', there is a 'Description' text box, 'Admin Status' with radio buttons for 'Disabled' and 'Enabled', and 'Network Address Translation (NAT)' with 'NAT Direction' radio buttons for 'Inside', 'Outside', and 'None'. Under 'IP Addresses', there is an 'Enable Zero Configuration' section with radio buttons for 'None', 'Primary', and 'Secondary'. Below that is the 'Primary IP Address' field, a checked 'Use DHCP to Obtain IP' checkbox, and a checked 'Use DHCP to obtain Gateway/DNS Servers' checkbox with the note '(Allowed on 1 virtual interface)'. At the bottom, there is a 'Secondary Addresses' field with a dropdown arrow and a plus icon. The window has 'OK', 'Reset', and 'Exit' buttons at the bottom right.

**Figure 5-47** Network - OSPF Virtual Interfaces - Basic Configuration tab

19. Within the **Properties** field, enter a 32 character maximum **Description** to help differentiate the virtual interface configuration used with this OSPF route. Enable/disable admin privileges as need. They're disabled by default.
20. Use the **IP Addresses** Area to set how route addresses are created for the virtual configuration.
- Zero Configuration can be enabled and set as the *Primary* or *Secondary* means of providing IP addresses for the OSPF virtual route. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. The drivers for the wireless adapter query the NDIS Object IDs and pass the available network names (SSIDs) to the service. The service then lists them in the user interface on the **Wireless Networks** tab in the connection's Properties or in the *Wireless Network Connection* dialog box accessible from the notification area. A checked build version of the WZC service can be used by developers to obtain additional diagnostic and tracing information logged by the service.
21. Select **Use DHCP to Obtain IP** to use the access point's DHCP server resource as the means of providing requested IP addresses to the OSPF route's virtual interface.
22. Select **Use DHCP to Obtain Gateway/DNS Servers** to learn the default gateway, name servers, and domain name on just this interface. Once selected, specify an IP address and mask in dot-decimal format.
23. Define the **NAT Direction** as either *Inside*, *Outside* or *None*. *Network Address Translation (NAT)*, is an Internet standard that enables a *Local Area Network (LAN)* to use IP addresses for internal traffic (inside) and a second set of addresses for external (outside) traffic.
24. Select **OK** to save the changes to the basic configuration. Select **Reset** to revert to the last saved configuration.
25. Select the **Security** tab.



**Figure 5-48** Network - OSPF Virtual Interface - Security tab

26. Use the **Inbound IP Firewall Rules** drop-down menu to select the IP access and deny rules to apply to the OSPF dynamic route.

Either select an existing IP firewall policy or use the default set of IP firewall rules. The firewall inspects OSPF route traffic flows and detects potential attacks on the dynamic route not visible to traditional wired firewall appliances. Select the **Create** icon to define a new set of IP firewall rules that can be applied to the OSPF route configuration. Selecting **Edit** allows for the modification of an existing IP firewall rules configuration. For more information, see [Wireless Firewall on page 8-2](#).

27. Use the **VPN Crypto Map** drop-down menu to select and apply a VPN crypto map entry to apply to the OSPF dynamic route. Crypto Map entries are sets of configuration parameters for encrypting packets passing through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration.
28. Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.6.9 Forwarding Database

#### ► Profile Network Configuration

A *Forwarding Database* is used by a bridge to forward or filter packets. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop (filter) it. If it is determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

To define a forwarding database configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Forwarding Database**.

**Aging Time**

Bridge Aging Time  (0,10-1000000 seconds)

**Static Forwarding Table**

MAC Address	VLAN Id	Interface Name	
02-03-04-05-06-07	1	FI123	
0A-0B-0C-0D-0E-0F	4	FI345	

**Figure 5-49** Network - Forwarding Database screen

5. Define a **Bridge Aging Time** from 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry will remain in the bridge's forwarding table before it is deleted due to lack of activity. If an entry replenishes a destination, generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

6. Use the **+ Add Row** button to create a new row within the MAC address table.
7. Set a destination **MAC Address** address. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).



<b>Description</b>	Lists a description of the VLAN assigned when it was created or modified. The description should be unique to the VLAN's specific configuration and help differentiate it from other VLANs with similar configurations.
<b>Edge VLAN Mode</b>	Defines whether the VLAN is currently in edge VLAN mode. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is defined with wireless clients and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't be marked as an edge VLAN. When defining a VLAN as edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active.
<b>Trust ARP Response</b>	When ARP trust is enabled, a green check mark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks.
<b>Trust DHCP Responses</b>	When DHCP trust is enabled, a green check mark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.

- Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify the configuration of an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

**Figure 5-51** Network - Bridge VLAN Configuration screen

- If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN ID** from 1 - 4095. This value must be defined and saved before the **General** tab can become enabled and the remainder of the settings defined.

7. If creating a new Bridge VLAN, provide a **Description** (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
8. Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate flow tables that store information on the traffic allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory that could be used for other critical purposes. With the per VLAN firewall feature enabled on an interface, flow tables are only generated for that interface. Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory which can be used for other purposes.

Firewalls can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network. Select the **Per VLAN Firewall** option to enable firewall on this interface.

9. Select the **L2 Tunnel Broadcast Optimization** option to prevent flooding of ARP packets on this bridge interface.

Broadcast Optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered at the wireless controller level.

10. Define the following **Extended VLAN Tunnel** parameters:

<b>Bridging Mode</b>	Specify one of the following bridging mode for use on the VLAN: <ul style="list-style-type: none"> <li>• <i>Automatic</i>: Select Automatic mode to let the access point determine the best bridging mode for the VLAN.</li> <li>• <i>Local</i>: Select Local to use local bridging mode for bridging traffic on the VLAN.</li> <li>• <i>Tunnel</i>: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. Tunnel must be selected to successfully create a mesh connection between two Standalone APs.</li> <li>• <i>isolated-tunnel</i>: Select isolated-tunnel to use a dedicated tunnel for bridging traffic on the VLAN.</li> </ul>
<b>IP Outbound Tunnel ACL</b>	Select an <i>IP Outbound Tunnel ACL</i> for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available select the create icon to make a new one.
<b>MAC Outbound Tunnel ACL</b>	Select a <i>MAC Outbound Tunnel ACL</i> for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available select the create icon to make a new one.



**NOTE:** If creating a mesh connection between two access points in Standalone AP mode, *Tunnel* must be selected as the Bridging Mode to successfully create the mesh link between the two access points.

11. Select **Tunnel Over Level 2** to tunnel extended VLAN traffic over level 2 links.
12. Define the following **Layer 2 Firewall** parameters:

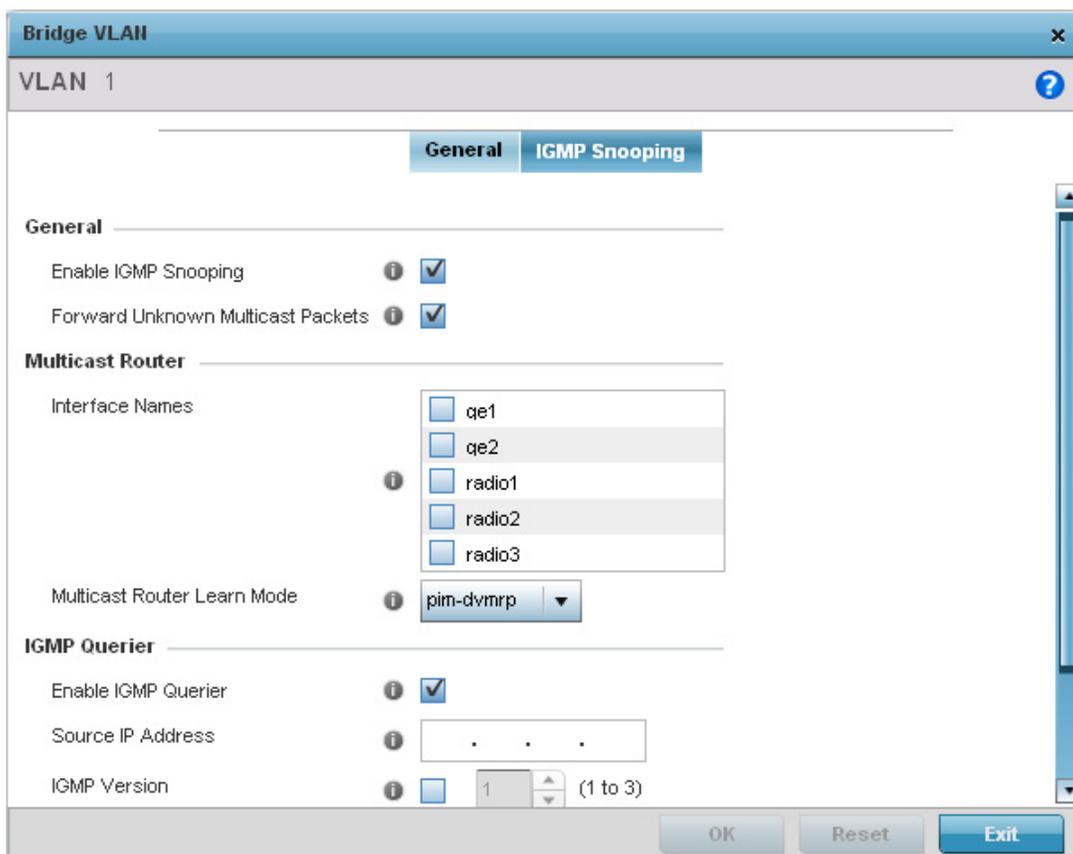
<b>Trust ARP Response</b>	Select this option to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default.
<b>Trust DHCP Responses</b>	Select this option to use DHCP packets from a DHCP server as trusted and permissible within the network. DHCP packets update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default.
<b>Enable Edge VLAN Mode</b>	Select this option to enable edge VLAN mode. When selected, the IP address in the VLAN is not used for normal operations, as its now designated to isolate devices and prevent connectivity. This feature is enabled by default.

13. Refer to the **Captive Portal** field to select an existing captive portal configuration to apply access restrictions to the bridge VLAN configuration.

A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance.

If an existing captive portal does not suite the bridge VLAN configuration, either select the **Edit** icon to modify an existing configuration or select the **Create** icon to define a new configuration that can be applied to the bridge VLAN. For information on configuring a captive portal policy, see [Configuring Captive Portal Policies on page 9-2](#).

14. Select the **IGMP Snooping** tab.



**Figure 5-52** Network - Bridge VLAN - IGMP Snooping screen

15. Define the following IGMP **General** parameters:

<b>Enable IGMP Snooping</b>	Select this option to enable IGMP snooping. If disabled, snooping on this bridge VLAN is disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden.
<b>Forward Unknown Multicast Packets</b>	Select this option to enable forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for this bridge VLAN. This settings is enabled by default.

16. Define the following **Multicast Router** settings:

<b>Interface Names</b>	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
<b>Multicast Router Learn Mode</b>	Select <i>static</i> or <i>pim-dvmrp</i> as the mode used to determine client multicast traffic levels on specific routes.

17. Set the following **IGMP Querier** parameters for the bridge VLAN configuration:

<b>Enable IGMP Querier</b>	IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server, hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
<b>Source IP Address</b>	Define an IP address applied as the source address in the IGMP query packet. This address is used as the default VLAN querier IP address.
<b>IGMP Version</b>	Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. The default setting is 3.
<b>Maximum Response Time</b>	Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. For IGMP reports from wired ports, reports are only forwarded to the multicast router ports. The default setting is 10 seconds.
<b>Other Querier Timer Expiry</b>	Specify an interval in either <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

18. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

### 5.2.6.11 Cisco Discovery Protocol Configuration

#### ▶ Profile Network Configuration

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To define the profile's CDP configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Cisco Discovery Protocol**.

**Cisco Discovery Protocol (CDP)**

Enable CDP

Hold Time  (10 to 1,800)

Timer  (5 to 900)

**OK** **Reset**

**Figure 5-53** Network - Cisco Discovery Protocol (CDP) screen

5. Enable/disable CDP and set the following settings:

<b>Enable CDP</b>	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default.
<b>Hold Time</b>	Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 1,800 seconds.
<b>Timer</b>	Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds.

6. Select the **OK** button located at the bottom right of the screen to save the changes to the CDP configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.6.12 Link Layer Discovery Protocol Configuration

### ► Profile Network Configuration

The *Link Layer Discovery Protocol* (LLDP) provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one *Link Layer Discovery Protocol Data Unit* (LLDP PDU). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To set the LLDP configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Link Layer Discovery Protocol**.

**Link Layer Discovery Protocol (LLDP)**

Enable LLDP

Hold Time  (10 to 1,800)

Timer  (5 to 900)

Inventory Management Discovery

Extended Power via MDI Discovery

OK Reset

**Figure 5-54** Network - Link Layer Discovery Protocol (LLDP) screen

5. Set the following LLDP parameters for the profile configuration:

<b>Enable LLDP</b>	Select this option to enable LLDP on the access point. LLDP is enabled by default. When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them.
<b>Hold Time</b>	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds.
<b>Timer</b>	Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds.
<b>Inventory Management Discovery</b>	Select this option to include LLDP-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.

**Extended Power via MDI Discovery**

Select this option to include LLPD-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default.

6. Select the **OK** button to save the changes to the LLDP configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.6.13 Miscellaneous Network Configuration

#### ► *Profile Network Configuration*

A profile can be configured to include a hostname in a DHCP lease for a requesting device and its profile. This helps an administrator track the leased DHCP IP address by hostname for the supported device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include hostnames in DHCP requests:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Network** menu and select **Miscellaneous**.

The screenshot shows the 'DHCP Settings' configuration page. It features two settings: 'Include Hostname in DHCP Request' with an information icon and a checked checkbox, and 'DHCP Persistent Lease' with an information icon and an unchecked checkbox. At the bottom right, there are two buttons: 'OK' and 'Reset'.

**Figure 5-55** Network - Miscellaneous screen

5. Select the **Include Hostname in DHCP Request** option to include a hostname in a DHCP lease for a requesting device. This feature is enabled by default.
6. Select the **DHCP Persistent Lease** option to retain the lease that was last used by the access point if the access point's DHCP server resource were to become unavailable. This feature is enabled by default.
7. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

## 5.2.6.14 Alias

### ► Profile Network Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An *alias* enables an administrator to define a configuration item, such as a hostname, as an *alias* once and use the defined *alias* across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the *alias* used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration > Network > Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from **Configuration > Devices > System Profile > Network > Alias** screen. These aliases are available for use to a specific group of wireless controllers or access points. *Alias* values defined in this profile override alias values defined within global aliases.
- *RF Domain aliases* are defined from **Configuration > Devices > RF Domain > Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an *Network Alias* defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the *Network Alias* can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the *Network Alias* works with the 172.16.10.0/24 network. Existing ACLs using this *Network Alias* need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias are classified as:

- *Network Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

### 5.2.6.14.1 Network Basic Alias

#### ► Alias

A *basic alias* is a set of configurations that consist of VLAN, host, network and address range alias configurations. VLAN configuration is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

A basic alias configuration can contain multiple instances for each of the five (5) alias types.

To edit or delete a basic alias configuration:

1. Select **Configuration** tab from the web user interface.

2. Select **System Profiles**.
3. Select **Network** to expand it and display its sub menus.
4. Select the **Alias** item.

The screenshot shows the 'Alias' configuration interface. It features four tables for defining aliases:

- Vlan Alias:** A table with columns 'Name' and 'Vlan'. One row is visible with 'Name' as '\$TPLL' and 'Vlan' as '1'.
- Host Alias:** A table with columns 'Name' and 'Host'. One row is visible with 'Name' as '\$DNS\_Main' and 'Host' as '192.168.13.2'.
- Address Range Alias:** A table with columns 'Name', 'Start IP', and 'End IP'. One row is visible with 'Name' as '\$IPRange\_S', 'Start IP' as '172.16.10.11', and 'End IP' as '172.16.10.100'.
- Network Alias:** A table with columns 'Name' and 'Network'. One row is visible with 'Name' as '\$NW\_01' and 'Network' as '192.168.13.0/24'.

Each table includes an 'Add Row' button at the bottom. The interface also has 'OK' and 'Reset' buttons at the bottom right.

**Figure 5-56** Network - Basic Alias Screen

5. Select **+ Add Row** to define **VLAN Alias** settings:

Use the **VLAN Alias** field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

<b>Name</b>	If adding a new <i>VLAN Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>VLAN</b>	Use the spinner control to set a numeric VLAN from 1 - 4094.

A *VLAN alias* is used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3
- Switchport

- Wireless LANs

6. Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

<b>Name</b>	If adding a new <i>Address Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Start IP</b>	Set a starting IP address used with a range of addresses utilized with the address range alias.
<b>End IP</b>	Set a ending IP address used with a range of addresses utilized with the address range alias.

An *address range alias* can be used to replace an IP address range in IP firewall rules.

7. Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	Set the IP address of the host machine.

A *host alias* can be used to replace hostnames in the following locations:

- IP Firewall Rules
- DHCP

8. Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	Provide a network address in the form of <i>host/mask</i> .

A *network alias* can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

9. Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.

<b>Name</b>	If adding a new <i>String Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	Provide a string value to use in the alias.

A *string alias* can be used to replace domain name strings in DHCP.

10. Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.2.6.14.2 Network Group Alias

#### ► *Alias*

A *network group alias* is a set of configurations that consist of host and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20. Host configuration is in the form of single IP address, 192.168.10.23.

A *network group alias* can contain multiple definitions for Host, Network, and IP address range. A maximum of eight (8) Host entries, eight (8) Network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 Network Group Alias entries can be created.

A *network group alias* can be used in IP firewall rules to substitute hosts, subnets and IP address ranges:

To edit or delete a network alias configuration:

1. Select **Configuration** tab from the web user interface.
2. Select **System Profiles**.
3. Select **Network** to expand it and display its sub menus.
4. Select the **Alias** item, the **Basic Alias** screen displays.
5. Select the **Network Group Alias** tab.



**Figure 5-58** Network - Alias - Network Group Alias Add screen

7. If adding a new **Network Group Alias**, provide it a name of up to 32 characters.



**NOTE:** The **Network Group Alias Name** always starts with a dollar sign (\$).

8. Define the following network group alias parameters:

<b>Host</b>	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
<b>Network</b>	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

9. Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.
10. Select **OK** when completed to update the network group alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.2.6.14.3 Network Service Alias

#### ► Alias

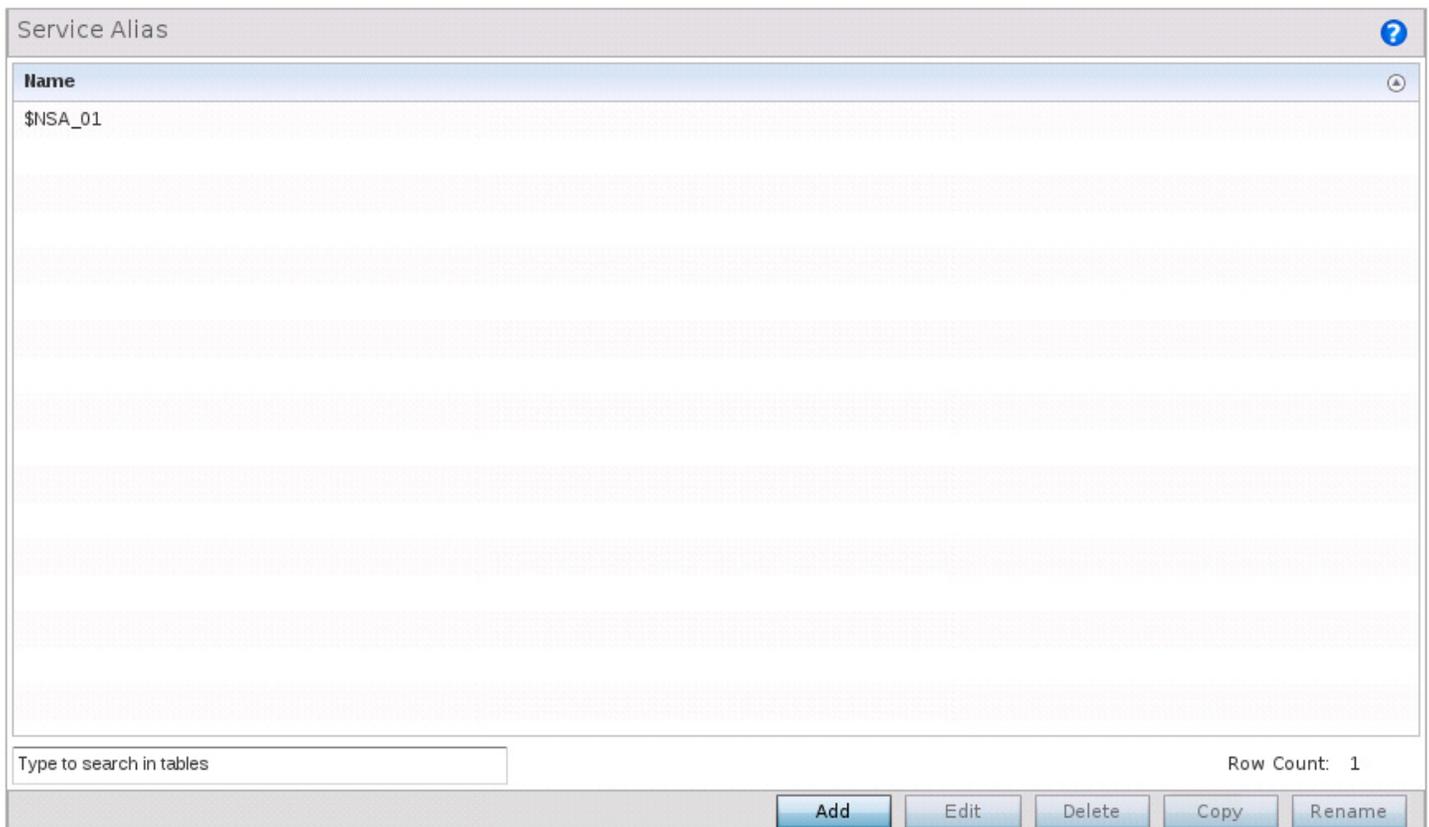
*Network Service Alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per *Network Service Alias*.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

A *network service alias* can be used to substitute protocols and ports in IP firewall rules:

To edit or delete a network service alias configuration:

1. Select **Configuration** tab from the web user interface.
2. Select **System Profiles**.
3. Select **Network** to expand it and display its sub menus.
4. Select the **Alias** item, the **Basic Alias** screen displays.
5. Select the **Network Service Alias** tab.



**Figure 5-59** Network - Alias - Network Service Alias screen

6. Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Service Alias**.

**Figure 5-60** Network - Alias - Network Service Alias Add screen

7. If adding a new **Network Service Alias**, provide it a name up to 32 characters.



**NOTE:** The **Network Service Alias Name** always starts with a dollar sign (\$).

8. Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

<b>Protocol</b>	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from <i>eigrp</i> , <i>gre</i> , <i>icmp</i> , <i>igmp</i> , <i>ip</i> , <i>rrp</i> , <i>igp</i> , <i>ospf</i> , <i>tcp</i> and <i>udp</i> . Select <i>other</i> if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
<b>Source Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
<b>Destination Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

9. Select **OK** when completed to update the network service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.2.6.15 Profile Network Configuration and Deployment Considerations

#### ▶ *Profile Network Configuration*

Before defining a profile's network configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception.
  - Static routes, while easy, can be overwhelming within a large or complicated network. Each time there is a change, someone must manually make changes to reflect the new route. If a link goes down, even if there is a second path, the router would ignore it and consider the link down.
  - Static routes require extensive planning and have a high management overhead. The more routers that exist in a network, the more routes need to be configured. If you have N number of routers and a route between each router is needed, then you must configure  $N \times N$  routes. Thus, for a network with nine routers, you will need a minimum of 81 routes ( $9 \times 9 = 81$ ).
-

## 5.2.7 Profile Security Configuration

### ▶ System Profile Configuration

An access point profile can have its own firewall policy, wireless client role policy, WEP shared key authentication and NAT policy applied.

For more information, refer to the following:

- [Defining Profile VPN Settings](#)
- [Defining Profile Security Settings](#)
- [Setting the Certificate Revocation List \(CRL\) Configuration](#)
- [Setting the Profile's NAT Configuration](#)
- [Setting the Profile's Bridge NAT Configuration](#)

### 5.2.7.1 Defining Profile VPN Settings

#### ▶ Profile Security Configuration

IPSec VPN provides a secure tunnel between two networked peer access points or controllers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPSec peer, however for remote VPN deployments one crypto map is used for all the remote IPSec peers.

*Internet Key Exchange* (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

To define a profile's VPN settings:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **VPN**.

Name	DPD Keep ALive	IKE LifeTime	DPD Retries
ikev1-default	30s	1d 0h 0m 0s	5

**Figure 5-61** Profile Security - VPN IKE Policy screen

- Select either the **IKEv1** or **IKEv2** radio button to enforce VPN peer key exchanges using either IKEv1 or IKEv2. IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the IKE Policy screens differ depending on the selected IKEv1 or IKEv2 mode.
- Refer to the following to determine whether an **IKE Policy** requires creation, modification or removal:

<b>Name</b>	Displays the 32 character maximum name assigned to the IKE policy.
<b>DPD Keep Alive</b>	Lists each policy's IKE keep alive message interval defined for IKE VPN tunnel dead peer detection.
<b>IKE LifeTime</b>	Displays each policy's lifetime for an IKE SA. The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.
<b>DPD Retries</b>	Lists each policy's maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead by the peer. This screen only appears when IKEv1 is selected.

- Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

**ikev1 policy**

Name \*

**Settings**

DPD Keep Alive   ( 10 to 3,600 )

Mode

DPD Retries  ( 1 to 100 )

IKE LifeTime   ( 1 to 1 )

IKE Proposal

Name	DH Group	Encryption	Authentication	
default	2	AES-256	SHA	

**Figure 5-62** Profile Security - VPN IKE Policy create/modify screen (IKEv1 example)

<b>Name</b>	If creating a new IKE policy, assign it a name (32 character maximum) to help differentiate this IKE configuration from others with similar parameters.
<b>DPD Keep Alive</b>	Configure the IKE keep alive message interval used for dead peer detection on the remote end of the IPsec VPN tunnel. Set this value in either <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) or <i>Hours</i> (1). The default setting is 30 seconds. This setting is required for both IKEv1 and IKEv2.
<b>Mode</b>	If using IKEv1, use the drop-down menu to define the IKE mode as either <i>Main</i> or <i>Aggressive</i> . IPSEC has two modes in IKEv1 for key exchanges. <i>Aggressive</i> mode requires 3 messages be exchanged between the IPSEC peers to setup the SA, <i>Main</i> requires 6 messages. The default setting is <i>Main</i> .
<b>DPD Retries</b>	Use the spinner control to set the maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead. The available range is from 1 - 100. The default setting is 5.
<b>IKE LifeTime</b>	Set the lifetime defining how long a connection (encryption/authentication keys) should last from successful key negotiation to expiration. Set this value in either <i>Seconds</i> (600 - 86,400), <i>Minutes</i> (10 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). This setting is required for both IKEv1 and IKEv2.

8. Select **+ Add Row** to define the network address of a target peer and its security settings.

<b>Name</b>	If creating a new IKE policy, assign the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration.
<b>DH Group</b>	Use the drop-down menu to define a <i>Diffie-Hellman</i> (DH) identifier used by the VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include <i>2</i> , <i>5</i> and <i>14</i> . The default setting is <i>5</i> .
<b>Encryption</b>	Select an encryption method used by the tunnelled peers to securely interoperate. Options include <i>3DES</i> , <i>AES</i> , <i>AES-192</i> and <i>AES-256</i> . The default setting is <i>AES-256</i> .
<b>Authentication</b>	Select an authentication hash algorithm used by the peers to exchange credential information. Options include <i>SHA</i> and <i>MD5</i> . The default setting is <i>SHA</i> .

9. Select **OK** to save the changes made within the IKE Policy screen. Select **Reset** to revert to the last saved configuration. Select the Delete Row icon to remove a peer configuration.
10. Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.

Name	IP/HostName	Authentication Type	LocalID	RemoteID	IKE Policy Name
Peer_01	192.168.13.10	PSK	local	remote	ikev1-default

Type to search in tables Row Count: 1

Add Edit Delete

**Figure 5-63** Profile Security - VPN Peer Destination screen (IKEv1 example)

11. Select either the **IKEv1** or **IKEv2** radio button to enforce VPN key exchanges using either IKEv1 or IKEv2.
12. Refer to the following to determine whether a VPN **Peer Configuration** requires creation, modification or removal:

<b>Name</b>	Lists the 32 character maximum name assigned to each listed peer configuration.
<b>IP/Hostname</b>	Displays the IP address (or host address FQDN) of the IPSec VPN peer targeted for secure tunnel connection and data transfer.
<b>Authentication Type</b>	Lists whether the peer configuration has been defined to use <i>pre-shared key</i> (PSK) or RSA. <i>Rivest, Shamir, and Adleman</i> (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption. If using <i>IKEv2</i> , this screen displays both local and remote authentication, as both ends of the VPN connection require authentication.

<b>LocalID</b>	Lists the access point's local identifier used within this peer configuration for an IKE exchange with the target VPN IPsec peer.
<b>RemoteID</b>	Displays the means the target remote peer is to be identified (string, FQDN etc.) within the VPN tunnel.
<b>IKE Policy Name</b>	Lists the IKEv1 or IKE v2 policy used with each listed peer configuration. If a policy requires creation, select the <i>Create</i> button.

13. Select **Add** to define a new peer configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing peer configuration. The parameters vary depending on whether IKEv1 or IKEv2 is selected.

**Figure 5-64** Profile Security - VPN Peer Configuration create/modify screen (IKEv2 example)

<b>Name</b>	If creating a new peer configuration (remote gateway) for VPN tunnel connection, assign it a name (32 character maximum) to distinguish it from others with similar attributes.
<b>IP Type</b>	Enter either the IP address or FQDN hostname of the IPsec VPN peer used in the tunnel setup. If <i>IKEv1</i> is used, this value is titled <i>IP Type</i> , if <i>IKEv2</i> is used, this parameter is titled <i>Select IP/Hostname</i> .
<b>Authentication Type or Local Authentication Type</b>	Select either <i>pre-shared key</i> (PSK) or RSA. <i>Rivest, Shamir, and Adleman</i> (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption. If using <i>IKEv2</i> , this screen displays both <i>local</i> and <i>remote authentication</i> options, as both ends of the VPN connection require authentication. <i>RSA</i> is the default value for both local and remote authentication (regardless of IKEv1 or IKEv2).



<b>Encryption Algorithm</b>	Displays each transform set's encryption method for protecting transmitted traffic.
<b>Mode</b>	Displays either <i>Tunnel</i> or <i>Transport</i> as the IPSec tunnel type used with the transform set. Tunnel is used for site-to-site VPN and Transport should be used for remote VPN deployments.

17. Select **Add** to define a new transform set configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing transform set.

**Figure 5-66** Profile Security - VPN Transform Set create/modify screen

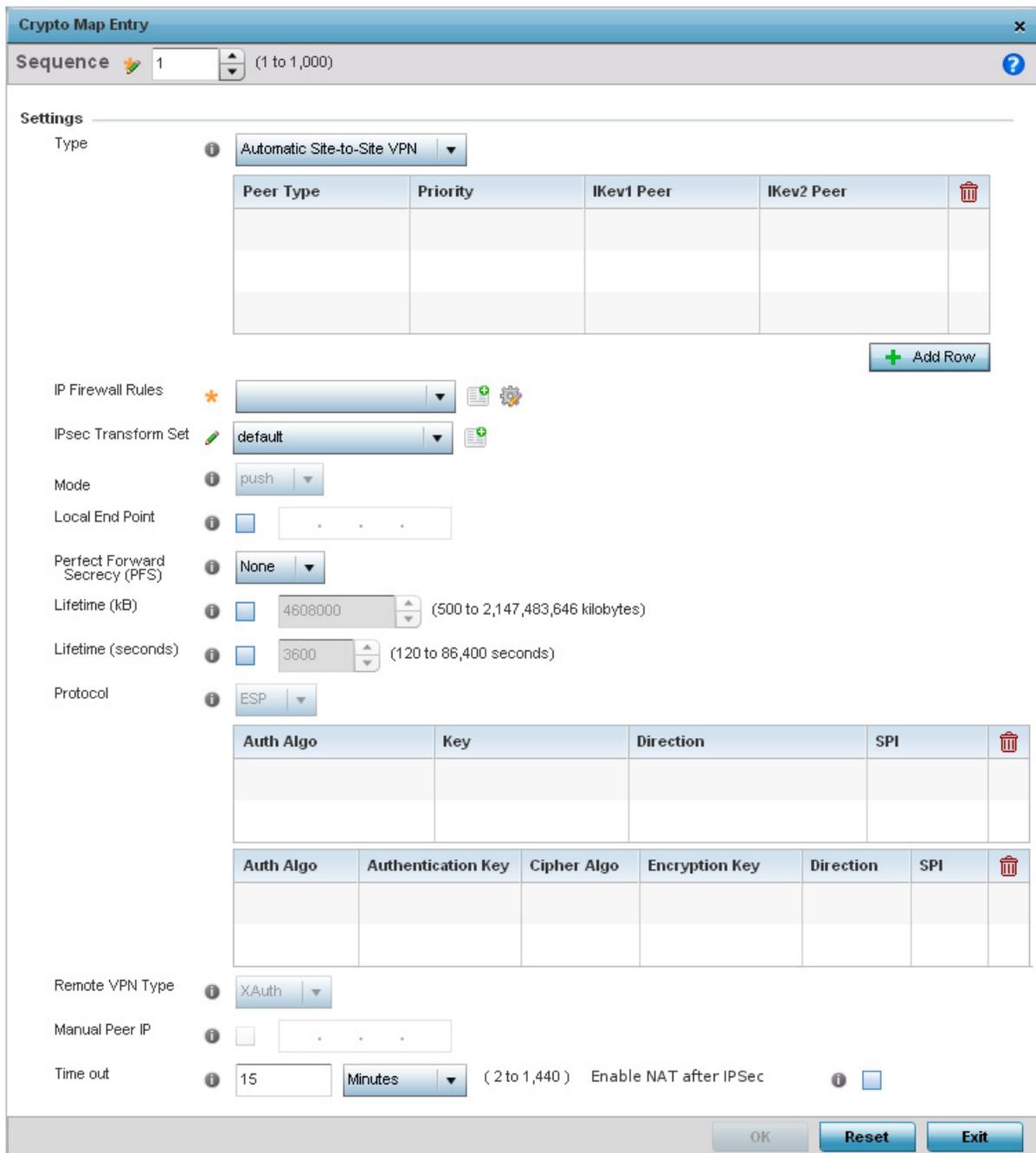
18. Define the following settings for the new or modified **Transform Set** configuration:

<b>Transform Set</b>	If creating a new transform set, define a 32 character maximum name to differentiate this configuration from others with similar attributes.
<b>Authentication Algorithm</b>	Set the transform sets's authentication scheme used to validate identity credentials. Use the drop-down menu to select either <i>HMAC-SHA</i> or <i>HMAC-MD5</i> . The default setting is HMAC-SHA.
<b>Encryption Algorithm</b>	Set the transform set encryption method for protecting transmitted traffic. Options include <i>DES</i> , <i>3DES</i> , <i>AES</i> , <i>AES-192</i> and <i>AES-256</i> . The default setting is AES-256.
<b>Mode</b>	Use the drop-down menu to select either <i>Tunnel</i> or <i>Transport</i> as the IPSec tunnel type used with the transform set. Tunnel is used for site-to-site VPN and Transport should be used for remote VPN deployments.

19. Select **OK** to save the changes made within the **Transform Set** screen. Select **Reset** to revert to the last saved configuration.
20. Select the **Crypto Map** tab.
- Use crypto maps (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).







**Figure 5-69** Profile Security - VPN Crypto Map Entry screen

26. Define the following parameters to set the crypto map configuration:

<p><b>Sequence</b></p>	<p>Each crypto map configuration uses a list of entries based on a sequence number. Specifying multiple sequence numbers within the same crypto map extends connection flexibility to multiple peers on the same interface, based on this selected sequence number (from 1 - 1,000).</p>
<p><b>Type</b></p>	<p>Define the site-to-site-manual, site-to-site-auto or remote VPN configuration defined for each listed crypto map configuration.</p>

<b>IP Firewall Rules</b>	Use the drop-down menu to select the <i>access list</i> (ACL) used to protect IPSec VPN traffic. New access/deny rules can be defined for the crypto map by selecting the <i>Create</i> icon, or an existing set of firewall rules can be modified by selecting the <i>Edit</i> icon.
<b>IPSec Transform Set</b>	Select the transform set (encryption and hash algorithms) to apply to this crypto map configuration.
<b>Mode</b>	Use the drop-down menu to define which mode (pull or push) is used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push.
<b>Local End Point</b>	Select this option to define an IP address as a local tunnel end-point address. This setting represents an alternative to an interface IP address.
<b>Perfect Forward Secrecy (PFS)</b>	PFS is key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include <i>None</i> , <i>2</i> , <i>5</i> and <i>14</i> . The default setting is <i>None</i> .
<b>Lifetime (kB)</b>	Select this option to define a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes.
<b>Lifetime (seconds)</b>	Select this option to define a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. The available range is from 120 - 86,400 seconds. The default setting is 120 seconds.
<b>Protocol</b>	Select the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include <i>ESP</i> and <i>AH</i> . The default setting is <i>ESP</i> .
<b>Remote VPN Type</b>	Define the remote VPN type as either <i>None</i> or <i>XAuth</i> . XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message. The default setting is XAuth.
<b>Manual Peer IP</b>	Select this option to define the IP address of an additional encryption/decryption peer.
<b>Time Out</b>	Select this option to set the IPSec SA time out value. Use the textbox and the drop-down list to configure the time out duration.
<b>Enable NAT after IPSec</b>	Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels.

27. Select **OK** to save the updates made to the **Crypto Map Entry** screen. Selecting **Reset** reverts the screen to its last saved setting.

28. Select **Remote VPN Server**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

The screenshot shows the configuration page for a Remote VPN Server. The 'Remote VPN Server' tab is active. At the top, there are radio buttons for 'IKEv1' (selected) and 'IKEv2'. Below this, the 'IKEv1 Settings' section includes a dropdown for 'Authentication Method' set to 'Local' and another dropdown for 'AAA Policy'. A table with columns 'User Name' and 'Password' is present, with an 'Add Row' button below it. The 'Wins Server Settings' section has a table with columns 'Wins Server Type' and 'Wins Server IP', also with an 'Add Row' button. The 'Name Server Settings' section has a table with columns 'NameServer Type' and 'NameServer IP', with an 'Add Row' button. At the bottom, there is an 'IP Local Pool' field with a dropdown arrow. 'OK' and 'Reset' buttons are at the bottom right.

**Figure 5-70** Profile Security - Remote VPN Server tab (IKEv2 example)

29. Select either the **IKEv1** or **IKEv2** radio button to enforce peer key exchanges over the remote VPN server using either IKEv1 or IKEv2.

IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the screen differs depending on the selected IKE mode.

30. Set the following **IKEv1** or **IKe v2 Settings**:

<p><b>Authentication Method</b></p>	<p>Use the drop-down menu to specify the authentication method used to validate the credentials of the remote VPN client. Options include <i>Local</i> (on board RADIUS resource if supported) and <i>RADIUS</i> (designated external RADIUS resource). If selecting <i>Local</i>, select the <i>+ Add Row</i> button and specify a <i>User Name</i> and <i>Password</i> for authenticating remote VPN client connections with the local RADIUS resource. The default setting is <i>Local</i>. AP6511 and AP6521 model access points do not have a local RADIUS resource and must use an external RADIUS server resource.</p>
-------------------------------------	---

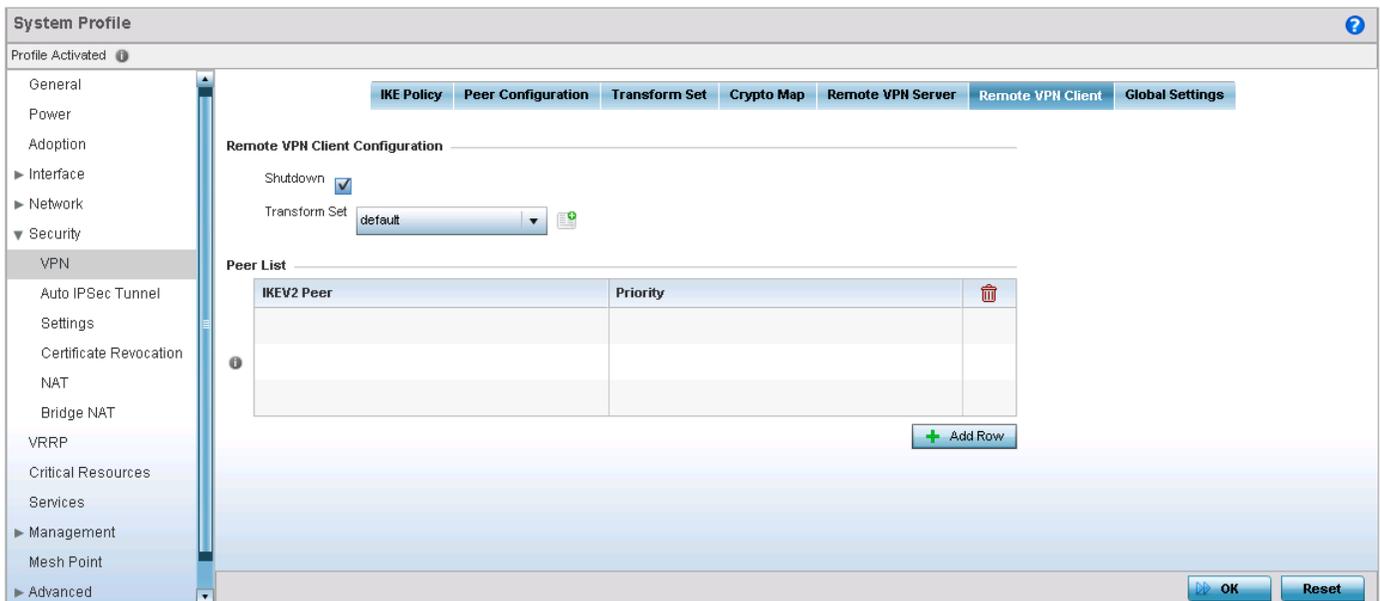
<b>AAA Policy</b>	Select the AAA policy used with the remote VPN client. AAA policies define RADIUS authentication and accounting parameters. The access point can optionally use AAA server resources (when using RADIUS as the authentication method) to provide user database information and user authentication data.
-------------------	--

31. Refer to the **Wins Server Settings** field and specify primary and secondary server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external WINS server resources are available to validate RADIUS resource requests.
32. Refer to the **Name Server Settings** field and specify primary and secondary server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external name server resources are available to validate RADIUS resource requests.
33. Select the **IP Local Pool** option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients.
34. If using IKEv2 specify following additional settings (required for IKEv2 only):

<b>DHCP Server Type</b>	Specify whether the <i>Dynamic Host Configuration Protocol</i> (DHCP) server is specified as an <i>IP address</i> , <i>Hostname (FQDN)</i> or <i>None</i> (a different classification will be defined). DHCP allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside.
<b>DHCP Server</b>	Depending on the DHCP server type selected, enter either the numerical IP address, hostname or other (if None is selected as the server type).
<b>IP Local Pool</b>	Select this option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients.
<b>Relay Agent IP Address</b>	Select this option to define DHCP relay agent IP address.

35. Select **OK** to save the updates made to the **Remote VPN Server** screen. Selecting **Reset** reverts the screen to its last saved configuration.
36. Select the **Remote VPN Client** tab.

The **Remote VPN Client** screen provides options for configuring the remote VPN client.



**Figure 5-71** Profile Security - Remote VPN Client tab

37. Refer to the following fields to define **Remote VPN Client Configuration** settings:

<b>Shutdown</b>	Select this option to disable the remote VPN client. The default is <i>disabled</i> .
<b>Transform Set</b>	Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down menu or click the icon next to the drop-down menu to create a new transform set.

38. Refer to the following fields to define the Remote VPN Client **Peer List**:

<b>IKEV2 Peer</b>	Use the drop-down menu to select the remote IKE v2 peer. Use the icon next to the drop-down to create a new peer.
<b>Priority</b>	Use the spinner to set the priority in which a remote peer is connected. The lower the number the higher the priority.

39. Select **OK** to save the updates made to the **Remote VPN Client** screen. Selecting **Reset** reverts the screen to its last saved configuration.

40. Select the **Global Settings** tab.

The **Global Settings** screen provides options for *Dead Peer Detection* (DPD). DPD represents the actions taken upon the detection of a dead peer within the IPsec VPN tunnel connection.

IKE Policy	Peer Configuration	Transform Set	Crypto Map	Remote VPN Server	Global Settings
df bit	<input type="text" value="copy"/>				
IPsec Lifetime (kB)	<input type="text" value="4608000"/> (500 to 2,147,483,646 kilobytes)				
IPsec Lifetime (seconds)	<input type="text" value="1"/> Hours (1 to 24)				
Plain Text Deny	<input type="text" value="global"/>				
<b>IKEV1 Settings</b>					
DPD KeepAlive	<input type="text" value="30"/> Seconds (10 to 3,600)				
DPD Retries	<input type="text" value="5"/> (1 to 100)				
NAT KeepAlive	<input type="text" value="20"/> Seconds (10 to 3,600)				
<b>IKEV2 Settings</b>					
DPD KeepAlive	<input type="text" value="30"/> Seconds (10 to 3,600)				
DPD Retries	<input type="text" value="5"/> (1 to 100)				
NAT KeepAlive	<input type="text" value="20"/> Seconds (10 to 3,600)				
Cookie challenge threshold	<input type="text" value="5"/> (1 to 100)				
				<input type="button" value="OK"/>	<input type="button" value="Reset"/>

Figure 5-72 Profile Security - Global VPN Settings tab

41. Refer to the following fields to define IPsec security, lifetime and authentication settings:

<b>df bit</b>	Select the DF bit handling technique used for the ESP encapsulating header. Options include <i>clear</i> , <i>set</i> and <i>copy</i> . The default setting is <i>copy</i> .
<b>IPsec Lifetime (kb)</b>	Set a connection volume lifetime (in kilobytes) for the duration of an IPsec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes. The default settings is 4,608,000 kilobytes.
<b>IPsec Lifetime (seconds)</b>	Set a lifetime (in seconds) for the duration of an IPsec VPN security association. Once the set value is exceeded, the association is timed out. Options include <i>Seconds</i> (120 - 86,400), <i>Minutes</i> (2 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). The default setting is 3,600 seconds.
<b>Plain Text Deny</b>	Select <i>global</i> or <i>interface</i> to set the scope of the ACL. The default setting is <i>global</i> , expanding the rules of the ACL beyond just the interface.

42. Define the following IKE Dead Peer Detection settings:

<b>DPD Keep Alive</b>	Define the interval (or frequency) of IKE keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 30 seconds.
-----------------------	--

<b>DPD Retries</b>	Use the spinner control to define the number of keep alive messages sent to an IPSec VPN client before the tunnel connection is defined as dead. The available range is from 1 - 100. The default number of messages is 5.
<b>NAT Keep Alive</b>	Define the interval (or frequency) of NAT keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 20 seconds.
<b>Cookie Challenge Threshold</b>	Use the spinner control to define the threshold (1 - 100) that, when exceeded, enables the cookie challenge mechanism.
<b>Crypto NAT Pool</b>	Use the drop-down menu to select the NAT pool for internal source NAT for IPSec tunnels.

43. Select **OK** to save the updates made to the **Global Settings** screen. Selecting **Reset** reverts the screen to its last saved configuration.

### 5.2.7.2 Auto IPSec Tunnel

#### ► Profile Security Configuration

IPSec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **Auto IPSec Tunnel**.

The screenshot shows the 'Settings' window for the Auto IPSec Tunnel configuration. It contains the following fields and controls:

- Group ID:** A text input field.
- Authentication Type:** A dropdown menu.
- Authentication Key:** A text input field.
- IKE Version:** A dropdown menu with 'ikev2' selected.
- Enable NAT after IPSec:** A checkbox that is currently unchecked.
- Use Unique ID:** A checkbox that is currently unchecked.

At the bottom right of the settings window, there are two buttons: 'OK' and 'Reset'.

**Figure 5-73** Profile Security – Auto IPSec Tunnel screen

5. Refer to the following table to configure the Auto IPSec Tunnel settings:

<b>Group ID</b>	Configure the ID string used for IKE authentication. String length can be between 1 - 64 characters.
<b>Authentication Type</b>	Set the IPSec Authentication Type. Options include <i>PSK</i> (Pre Shared Key) or <i>rsa</i> .
<b>Authentication Key</b>	Set the common key for authentication between the remote tunnel peer. Key length is between 8 - 21 characters.
<b>IKE Version</b>	Configure the IKE version to use. The available options are <i>ikev1-main</i> , <i>ikev1-aggr</i> and <i>ikev2</i> .
<b>Enable NAT after IPSec</b>	Select this option to enable NAT after IPSec. Enable this option if there are NATted networks behind VPN tunnels.
<b>Use Unique ID</b>	In scenarios where different access points behind different NAT boxes/routers have the same IP address, it is not possible to create a tunnel between the wireless controller and access point, as the wireless controller fails to identify the access point uniquely. When selected, each access point behind the same NAT box/router will have a unique ID. This unique ID is used to create the VPN tunnel.

6. Select **OK** to save the updates made to the **Auto IPSec Tunnel** screen. Selecting **Reset** reverts the screen to its last saved configuration.

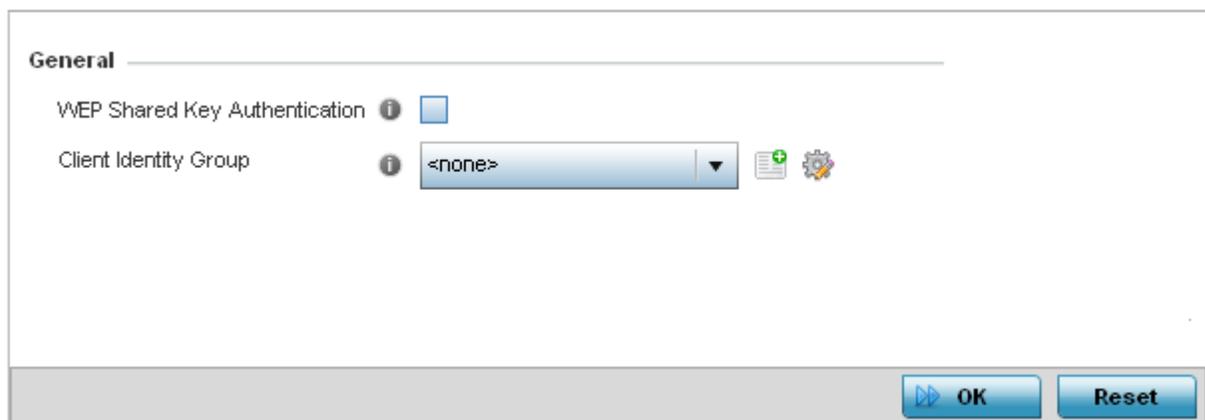
### 5.2.7.3 Defining Profile Security Settings

#### ▶ Profile Security Configuration

A profile can leverage existing firewall, wireless client role and WIPS policies and configurations and apply them to the profile's configuration. This affords each profile a truly unique combination of data protection policies best meeting the data protection requirements of the access point's numerous deployment scenarios.

To define a profile's security settings:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **Settings**.



**Figure 5-74** Profile Security - Settings screen

5. Select the **WEP Shared Key Authentication** radio button to require profile supported devices to use a WEP key to access the network using this profile. The access point, other proprietary routers, and Motorola Solutions clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola Solutions adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.
6. Client Identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for devices classes in the network. **Client Identity Group** is a collection of client identities that identify devices and applies specific permissions and restrictions on these devices. From the drop-down menu select the client identity group to use with this device profile. For more information, see [Device Fingerprinting on page 8-18](#).
7. Select **OK** to save the changes made within the **Settings** screen. Select **Reset** to revert to the last saved configuration.

### 5.2.7.4 Setting the Certificate Revocation List (CRL) Configuration

#### ► Profile Security Configuration

A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the *certificate authority* (CA) had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

To define a CRL configuration that can be applied to a profile:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **Certificate Revocation**.

The screenshot displays the 'Certificate Revocation List (CRL) Update Interval' configuration screen. It features a table with the following structure:

Trustpoint Name	URL	Hours	

Below the table is a '+ Add Row' button. At the bottom of the screen are 'OK' and 'Reset' buttons.

**Figure 5-75** Profile Security - Certificate Revocation List (CRL) Update Interval screen

5. Select the **+ Add Row** button to add a column within the **Certificate Revocation List (CRL) Update Interval** table to quarantine certificates from use in the network.
 

Additionally, a certificate can be placed on hold for a user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.
6. Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.
7. Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.
8. Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.
9. Select **OK** to save the changes made within the **Certificate Revocation List (CRL) Update Interval** screen. Select **Reset** to revert to the last saved configuration.

### 5.2.7.5 Setting the Profile's NAT Configuration

#### ▶ Profile Security Configuration

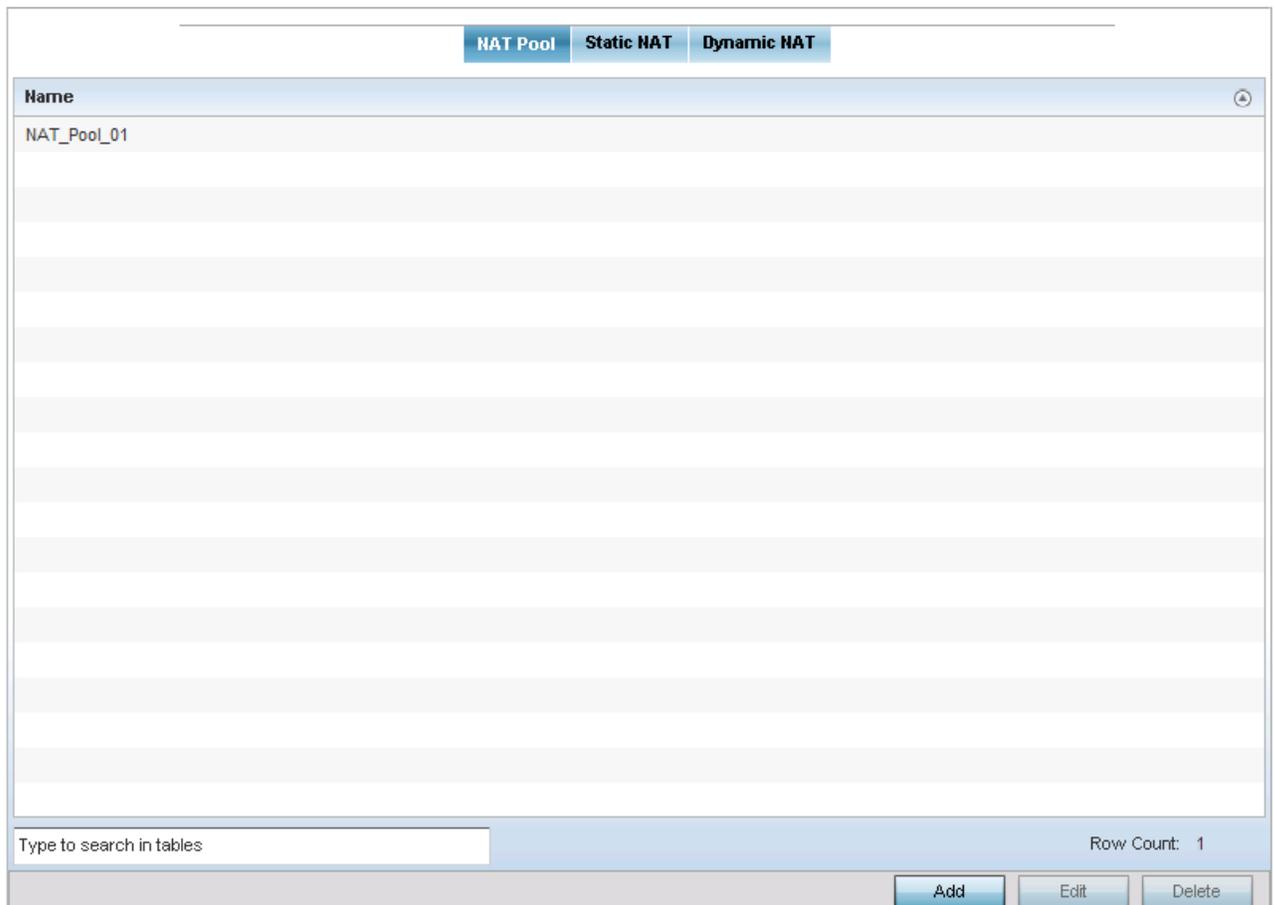
*Network Address Translation* (NAT) is a technique to modify network address information within IP packet headers in transit across a traffic routing device. This enables mapping one IP address to another to protect network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments, NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide a profile outbound Internet access to wired and wireless hosts connected to an access point. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an access point to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To define a NAT configuration that can be applied to a profile:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **NAT**.



**Figure 5-76** Profile Security - NAT Pool tab

The **NAT Pool** tab displays by default. The NAT Pool tab lists those NAT policies created thus far. Any of these policies can be selected and applied to the access point profile.

5. Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify the attributes of an existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.

**Figure 5-77** Profile Security - NAT Pool tab - NAT Pool field

6. If adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

<b>Name</b>	If adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
<b>IP Address Range</b>	Define a range of IP addresses that are hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

7. Select the **+ Add Row** button to append additional rows to the **IP Address Range** table.
8. Select **OK** to save the changes made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.
9. Select the **Static NAT** tab. The **Source** tab displays by default.

The **Source** tab displays by default and lists existing static NAT configurations. Existing static NAT configurations are not editable, but new configurations can be added or existing ones deleted as they become obsolete.

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.



11. Define the following Source NAT parameters:

<b>Protocol</b>	Select the protocol for use with static translation. <i>TCP</i> , <i>UDP</i> and <i>Any</i> are the available options. <i>Transmission Control Protocol</i> (TCP) is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The <i>User Datagram Protocol</i> (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is <i>Any</i> .
<b>Source IP</b>	Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Source Port</b>	Use the spinner control to set the local port number used at the (internal) end of the static NAT configuration. The default value is port 1.
<b>NAT IP</b>	Enter the IP address of the matching packet to the specified value. The IP address modified can be either <i>source</i> or <i>destination</i> based on the direction specified.
<b>NAT Port</b>	Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is <i>destination</i> .
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction. The default setting is <i>Inside</i> . Select <i>Inside</i> to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. <i>Inside</i> NAT is the default setting.

12. Select the **Destination** tab to view destination NAT configurations and define packets passing through the NAT on the way back to the LAN are searched against to the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.



14. Set the following **Destination** configuration parameters:

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

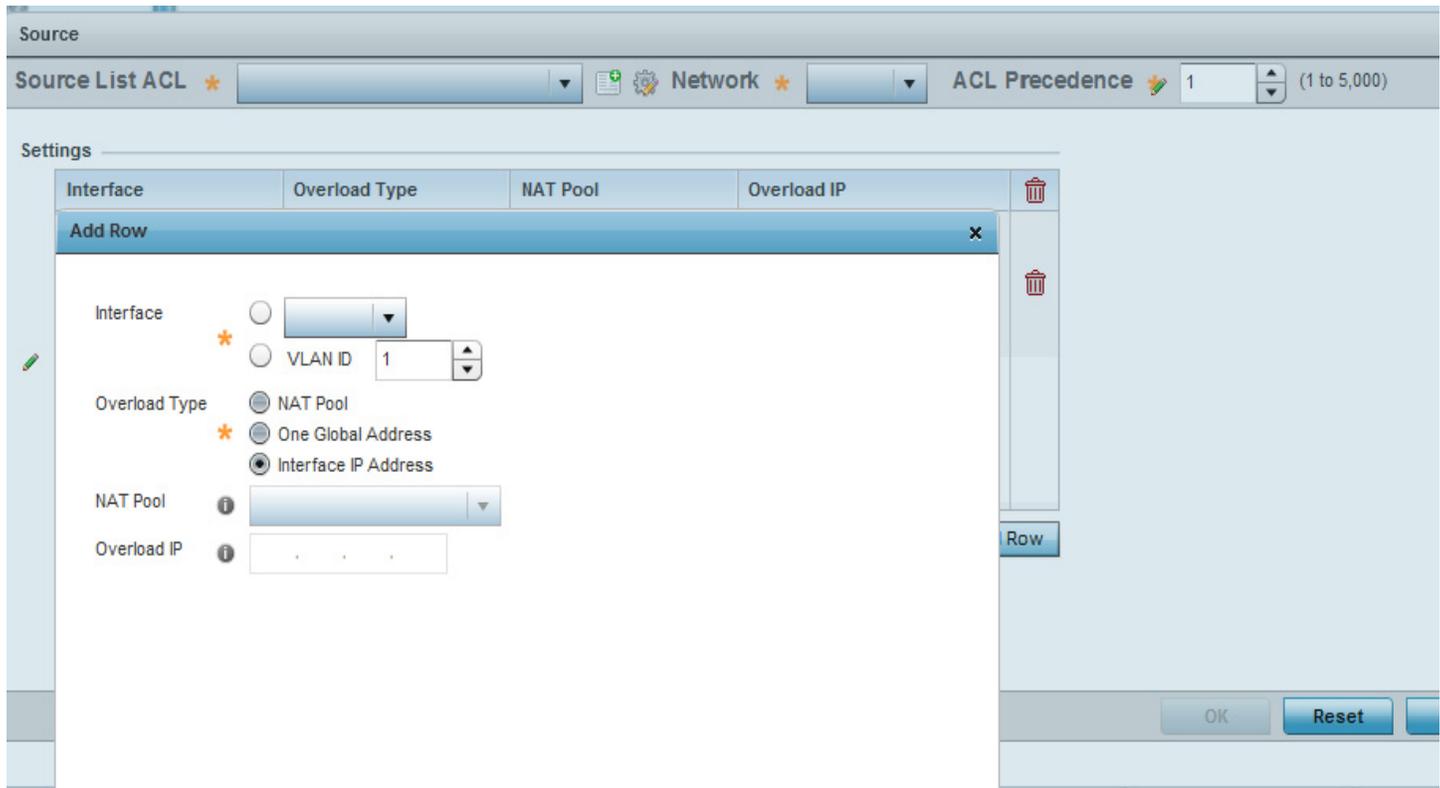
<b>Protocol</b>	Select the protocol for use with static translation. <i>TCP</i> , <i>UDP</i> and <i>Any</i> are the available options. <i>Transmission Control Protocol</i> (TCP) is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The <i>User Datagram Protocol</i> (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is <i>Any</i> .
<b>Destination IP</b>	Enter the address used at the (source) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Destination Port</b>	Use the spinner control to set the local port number used at the (source) end of the static NAT configuration. The default value is port 1.
<b>NAT IP</b>	Enter the IP address of the matching packet to the specified value. The IP address modified can be either <i>source</i> or <i>destination</i> based on the direction specified.
<b>NAT Port</b>	Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is <i>destination</i> .
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction. The default setting is <i>Inside</i> . Select <i>Inside</i> to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. <i>Inside</i> NAT is the default setting.

15. Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

16. Select the **Dynamic NAT** tab.

Dynamic NAT configurations translate the IP address of packets going out from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.





**Figure 5-83** Profile Security - Source ACL List screen

19. Set the following to define the Dynamic NAT configuration:

<b>Source List ACL</b>	Use the drop-down menu to select an ACL name to define the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access list. These addresses (once translated) <i>are not</i> exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.

20. Select **+ Add Row** to launch a pop up screen used to define the **Interface**, **Overload Type**, **Nat Pool** and **Overload IP** used with the dynamic NAT configuration.

<b>Interface</b>	Use the drop-down menu to select the VLAN ID (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default. Optionally, select the wwan1 radio button if the access point model supports a wwan interface as the outgoing layer 3 interface for NAT.
<b>Overload Type</b>	Select this option of Overload Type used with the listed IP ACL rule. Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . Interface IP Address is the default setting. If NAT Pool is selected, provide the Overload IP address.
<b>NAT Pool</b>	Provide the name of an existing NAT pool for use with the NAT configuration. Optionally select the <i>Create</i> icon to define a new NAT Pool configuration.
<b>Overload IP</b>	Enables the use of one global address for numerous local addresses.

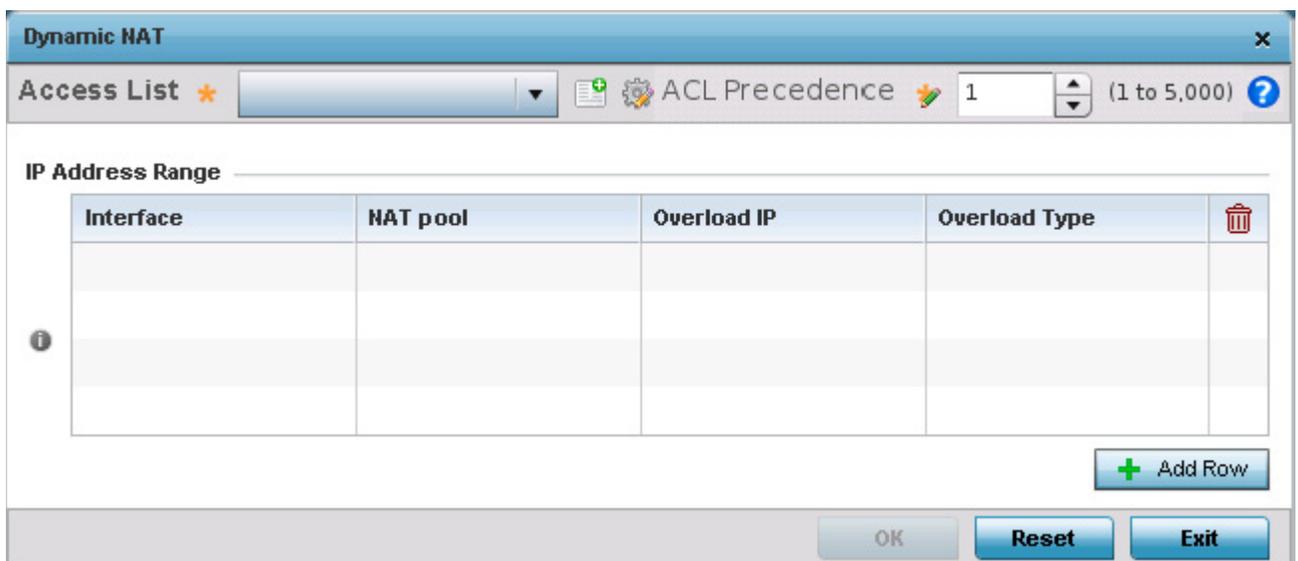
21. Select **OK** to save the changes made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.



- Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration modified or removed:

<b>ACL</b>	Lists the ACL applying IP address access/deny permission rules to the Bridge NAT configuration.
<b>Interface</b>	Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the access point's pppoe1 or wwan1 interface or the VLAN used as the redirection interface between the source and destination.
<b>NAT Pool</b>	Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when Overload Type is NAT Pool.
<b>Overload IP</b>	Lists the address used globally and collectively for numerous local addresses.
<b>Overload Type</b>	Lists the overload type used with the listed IP ACL rule. Set as either <i>NAT Pool</i> , <i>One Global Address</i> or <i>Interface IP Address</i> .

- Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.



**Figure 5-85** Profile Security - Dynamic NAT screen

- Select the **ACL** whose IP rules are to be applied to this policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.
- Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the Internet.

<b>Interface</b>	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN.
<b>NAT Pool</b>	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool.
<b>Overload IP</b>	Lists whether a single global address collectively supports numerous local addresses.
<b>Overload Type</b>	Displays the override type for this policy based forwarding rule.

- Select **+ Add Row** to set the IP address range settings for the Bridge NAT configuration.

**Figure 5-86** Profile Security - Source Dynamic NAT screen - Add Row field

10. Select **OK** to save the changes made within the **Add Row** and **Dynamic NAT** screens. Select **Reset** to revert to the last saved configuration.

### 5.2.7.7 Profile Security Configuration and Deployment Considerations

#### ► Profile Security Configuration

Before defining a profile's security configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Ensure the contents of the certificate revocation list are periodically audited to ensure revoked certificates remained quarantined or validated certificates are reinstated.
- NAT alone does not provide a firewall. If deploying NAT on a profile, add a firewall on the profile to block undesirable traffic from being routed. For outbound Internet access, a stateful firewall can be configured to deny all traffic. If port address translation is required, a stateful firewall should be configured to only permit the TCP or UDP ports being translated.

## 5.2.8 Virtual Router Redundancy Protocol (VRRP) Configuration

### ► System Profile Configuration

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available on an AP7131, and a router failure occurs, then the access point should act as a router and forward traffic on to its WAN link.

Define an external *Virtual Router Redundancy Protocol* (VRRP) configuration when router redundancy is required in a wireless network requiring high availability.

Central to the configuration of VRRP is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router MAC address
- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true

Those nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.



**NOTE:** VRRP support is available only on AP7131 model access point, and is not available in other models.

To define the configuration of a VRRP group:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Select **VRRP**.

VRRP		Version		
Virtual Router ID	Description	Virtual IP Addresses	Interface	Priority
1	VRRP_Group_01	192.168.13.9,192.168.13.10	Not Set	100

Type to search in tables Row Count: 1

**Figure 5-87** Profiles - VRRP screen - VRRP tab

5. Review the following VRRP configuration data to assess if a new VRRP configuration is required or if an existing VRRP configuration requires modification or removal:

<b>Virtual Router ID</b>	Lists a numerical index (from 1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
<b>Description</b>	Displays a description assigned to the VRRP configuration when it was either created or modified. The description is implemented to provide additional differentiation beyond the numerical virtual router ID.
<b>Virtual IP Addresses</b>	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
<b>Interface</b>	Displays the interfaces selected on the access point to supply VRRP redundancy failover support.
<b>Priority</b>	Lists a numerical value (from 1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process.

6. Select the **Version** tab to define the VRRP version scheme used with the configuration.

The screenshot shows the 'Version' tab of the VRRP configuration screen. The 'Version' dropdown menu is set to '2'. Below the dropdown, there is a warning icon (exclamation mark in a yellow triangle) followed by two lines of text: 'Advertisement interval for VRRP groups should be in centiseconds when updating to version 3.' and 'Advertisement interval for VRRP groups should be in seconds/milliseconds when updating to version 2.' At the bottom of the screen, there are three buttons: 'Add', 'Edit', and 'Delete'.

**Figure 5-88** Profiles - VRRP screen - Version tab

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are selectable to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications

(available publicly) refer to <http://www.ietf.org/rfc/rfc3768.txt> (version 2) and <http://www.ietf.org/rfc/rfc5798.txt> (version 3).

- From within the **VRRP** tab, select **Add** to create a new VRRP configuration or **Edit** to modify the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by selecting **Delete**.

If adding or editing a VRRP configuration, the following screen displays:

The screenshot shows the VRRP configuration window with the following fields and options:

- Virtual Router ID:** 1 (range 1 to 255)
- General Section:**
  - Description:  [Empty text box]
  - Priority: 100 (range 1 to 254)
  - Virtual IP Addresses: A table with 4 rows, each containing '0 . 0 . 0 . 0' and a 'Clear' button.
  - Advertisement Interval Unit: seconds
  - Advertisement Interval: 1 (range 1 to 255) [Seconds dropdown] and 250 (range 250 to 999)
  - Preempt:
  - Preempt Delay: 1 (range 1 to 65,535 seconds)
  - Interface:  VLAN ID: 1 (range 1 to 4,094)
- Protocol Extension Section:**
  - Sync Group:
  - Network Monitoring:
    - Local Interface:  wwan1,  pppoe1,  VLAN ID: 1 (range 1 to 4094)
    - Critical Resources: None
    - Delta Priority:  1 (range 1 to 253)

Buttons at the bottom: OK, Reset, Exit.

**Figure 5-89** Profiles - VRRP screen

- If creating a new VRRP configuration, assign a **Virtual Router ID** from 1 - 255. In addition to functioning as numerical identifier, the ID identifies the access point's virtual router a packet is reporting status for.

9. Define the following VRRP **General** parameters:

<b>Description</b>	In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration.
<b>Priority</b>	Use the spinner control to set a VRRP priority setting from 1 - 254. The access point uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master.
<b>Virtual IP Addresses</b>	Provide up to 8 IP addresses representing the Ethernet switches, routers or security appliances defined as virtual router resources to the AP7131 access point.
<b>Advertisement Interval Unit</b>	Select either <i>seconds</i> , <i>milliseconds</i> or <i>centiseconds</i> as the unit used to define VRRP advertisements. Once an option is selected, the spinner control becomes enabled for that <i>Advertisement Interval</i> option. The default interval unit is seconds. If changing the VRRP group version from 2 to 3, ensure the advertisement interval is in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.
<b>Advertisement Interval</b>	Once the <i>Advertisement Interval Unit</i> has been selected, use the spinner control to set the interval at which the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second.
<b>Preempt</b>	Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the <i>Preempt Delay</i> option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can takeover all the Virtual IPs from the nodes with a lower priority.
<b>Preempt Delay</b>	If the <i>Preempt</i> option is selected, use the spinner control to set the delay interval (in seconds) for preemption.
<b>Interface</b>	Select this value to enable/disable VRRP operation and define the AP7131 VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure.

10. Refer to the **Protocol Extension** field to define the following:

<b>Sync Group</b>	Select this option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled by default.
<b>Network Monitoring: Local Interface</b>	Select <i>wwan1</i> , <i>pppoe1</i> and <i>VLAN ID(s)</i> as needed to extend VRRP monitoring to these local access point interfaces. Once selected, these interfaces can be assigned an increasing or decreasing level or priority for virtual routing within the VRRP group.
<b>Network Monitoring: Critical Resources</b>	Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include <i>None</i> , <i>increment-priority</i> , and <i>decrement priority</i> .

**Network Monitoring:  
Delta Priority**

Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.

11. Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.9 Profile Critical Resources

### ► System Profile Configuration

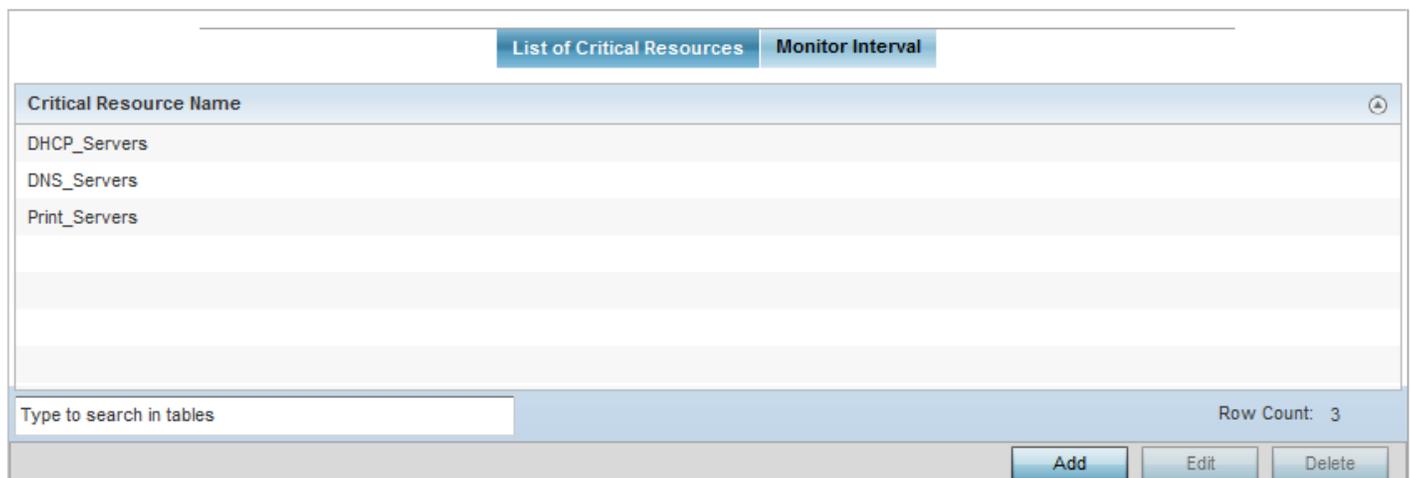
Critical resources are device IP addresses or interface destinations on the network interoperated as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, a AAA server, a WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they're discovered. For example, a critical resource on the same subnet as the access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resources can be configured for access points and wireless controllers using their respective profiles.

To define critical resources:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Select **Critical Resources**.



**Figure 5-90** Critical Resources screen - List of Critical Resources tab

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the access point or controller, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5. Select the **Add** button at the bottom of the screen to add a new critical resource and connection method, or select an existing resource and select **Edit** to update the resource's configuration.

**Figure 5-91** Critical Resources screen - Adding a Critical Resource

6. Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated. Options include *Any* and *All*. If selecting *Any*, an event is generated when the state of any single critical resource changes. If selecting *All*, an event is generated when the state of all monitored critical resources change.
7. Select the **IP** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided critical resource IP address as a network identifier.
8. Select the **Interface** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource using either the critical resource's VLAN, WWAN1 or PPPoE1 interface. If VLAN is selected, a spinner control is enabled to define the destination VLAN ID used as the interface for the critical resource.
9. Select **+ Add Row** to define the following for critical resource configurations:

<b>IP Address</b>	Provide the IP address of the critical resource. This is the address used by the access point to ensure the critical resource is available. Up to four addresses can be defined.
<b>Mode</b>	Set the ping mode used when the availability of a critical resource is validated. Select from: <ul style="list-style-type: none"> <li>• <i>arp-only</i> – Use the <i>Address Resolution Protocol</i> (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.</li> <li>• <i>arp-and-ping</i> – Use both ARP and <i>Internet Control Message Protocol</i> (ICMP) for pinging the critical resource and sending control messages (device not reachable, requested service not available, etc.).</li> </ul>
<b>Port</b>	Provide the port on which the critical resource is available. Use the spinner control to set the port number.
<b>VLAN</b>	Define the VLAN on which the critical resource is available using the spinner control.

10. Select the **Monitor Interval** tab.

The screenshot shows a configuration window titled "List of Critical Resources" with a sub-tab "Monitor Interval". Under the "General" section, there are two configuration fields:

- Monitor Interval:** A numeric input field containing "30" with a range "(5 to 86,400 seconds)" to its right.
- Source IP For Port-Limited Monitoring:** An IP address input field containing "0 . 0 . 0 . 0".

At the bottom right of the window, there are two buttons: "OK" and "Reset".

**Figure 5-92** Critical Resources screen - Monitor Interval tab

11. Set the duration between two successive pings from the access point to the critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.
12. Configure the IP address for Port-Limited Monitoring in the **Source IP for Port-Limited Monitoring** field. Sets the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. Generally, the source address 0.0.0.0 is used in the APR packets used to detect critical resources. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.
13. Select **OK** to save the changes to the critical resource configuration and monitor interval. Select **Reset** to revert to the last saved configuration.

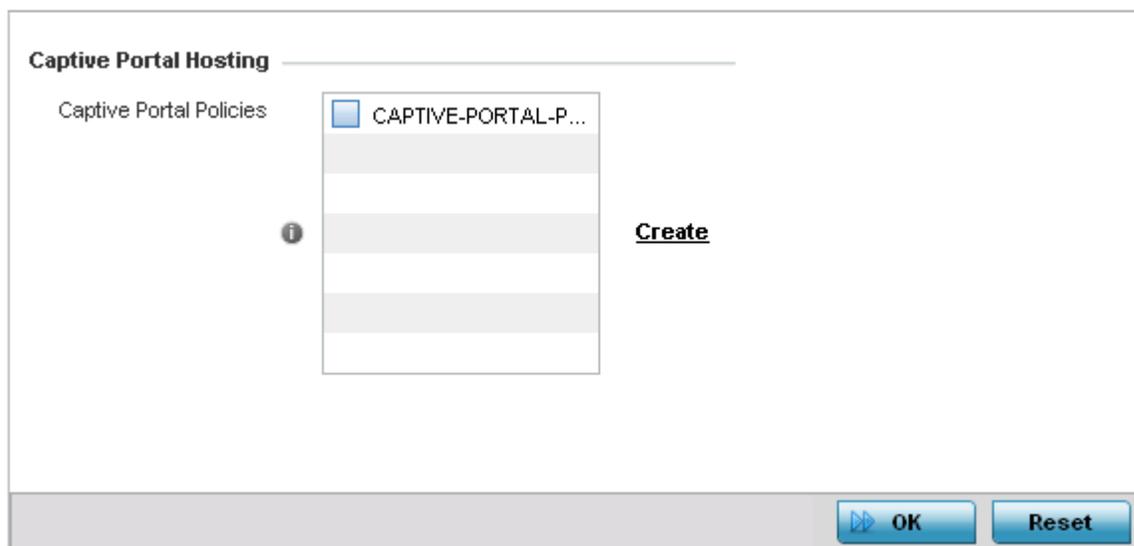
## 5.2.10 Profile Services Configuration

### ► System Profile Configuration

A profile can contain specific guest access (captive portal) server configurations. These guest network access permissions can be defined uniquely as profile requirements dictate.

To define a profile's services configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Select **Services**.



**Figure 5-93** Profile Services - Services screen

5. Refer to the **Captive Portal Hosting** field to select or set a guest access configuration (captive portal) for use with this profile.

A captive portal is guest access policy for providing guests temporary and restrictive access to the access point managed network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal configuration that can be applied to this profile. For more information, see [Configuring Captive Portal Policies on page 9-2](#).

6. Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.10.1 Profile Services Configuration and Deployment Considerations

#### ▶ *Profile Services Configuration*

Before defining a profile's captive portal and DHCP configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- A profile plan should consider the number of wireless clients allowed on the profile's guest (captive portal) network and the services provided, or if the profile should support guest access at all.
  - Profile configurations supporting a captive portal should include firewall policies to ensure logical separation is provided between guest and internal networks so internal networks and hosts are not reachable from guest devices.
  - DHCP's lack of an authentication mechanism means a DHCP server supported profile cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. Ensure a profile using DHCP resources is also provisioned with a strong user authorization and validation configuration.
-

## 5.2.11 Profile Management Configuration

### ▶ System Profile Configuration

The access point has mechanisms to allow/deny management access to the network for separate interfaces and protocols (*HTTP, HTTPS, Telnet, SSH* or *SNMP*). These management access configurations can be applied strategically to profiles as resource permissions dictate.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support.

To define a profile's management configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Management** menu item and select **Settings**.

### Message Logging

Enable Message Logging

Remote Logging Host

IP Address	
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>

Facility to Send Log Messages  local7

Syslog Logging Level  Warning

Console Logging Level  Warning

Buffered Logging Level  Warning

Time to Aggregate Repeated Messages  Seconds (0 to 60)

Forward Logs to Controller  Error

### System Event Messages

Enable System Events

Enable System Event Forwarding

### Events E-mail Notification

SMTP Server  Hostname

Port of SMTP  1 (1 to 65,535)

Sender Email Address

Recipient's Email Address

Username for SMTP Server

Password for SMTP Server

### Persist Configuration Across Reloads

Persist Configuration Across Reloads  Enabled

**Figure 5-94** Profile Management - Settings screen

- Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to discern an overall pattern that may be negatively impacting performance using the configuration defined for the access point's profile.

#### Enable Message Logging

Select this option to enable the profile to log system events to a user defined log file or a syslog server. Selecting this radio button enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.

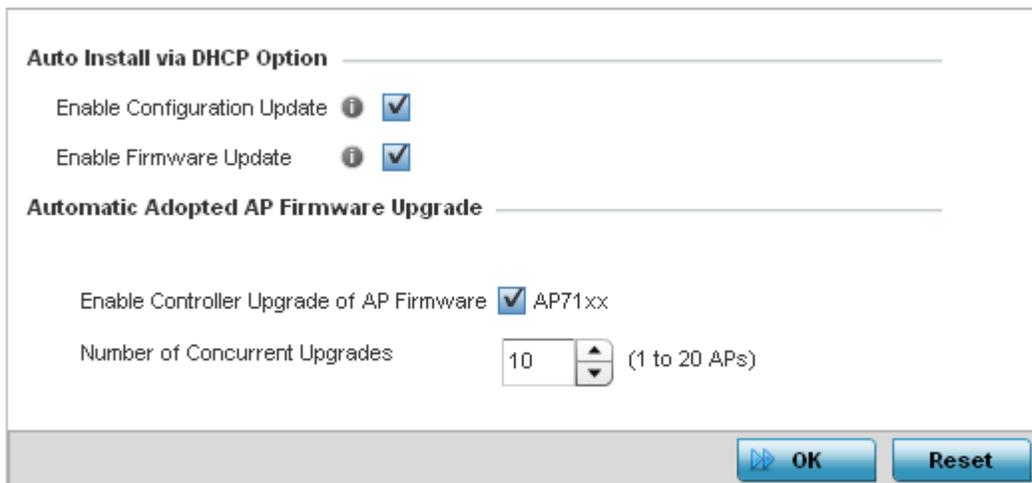
<b>Remote Logging Host</b>	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select <i>Clear</i> to remove an IP address.
<b>Facility to Send Log Messages</b>	Use the drop-down menu to specify the server facility (if used) for the profile event log transfer.
<b>Syslog Logging Level</b>	Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Console Logging Level</b>	Event severity coincides with the console logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Buffered Logging Level</b>	Event severity coincides with the buffered logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Time to Aggregate Repeated Messages</b>	Define the interval (duration) system events are logged on behalf of the access point profile. The shorter the interval, the sooner the event is logged. Either define an interval in <i>Seconds</i> (0 - 60) or <i>Minutes</i> (0 -1). The default value is 0 seconds.
<b>Forward Logs to Controller</b>	Select this option to define a log level for forwarding event logs. Log levels include <i>Emergency, Alert, Critical, Error, Warning, Notice, Info</i> and <i>Debug</i> . The default logging level is <i>Error</i> .

- Refer to the **System Event Messages** field to define how system messages are logged and forwarded on behalf of the access point's profile.
- Select the **Enable System Events** radio button to allow the profile to capture system events and append them to a log file. It's important to log individual events to discern an overall pattern that may be negatively impacting the access point's performance. This settings is enabled by default.
- Select the **Enable System Event Forwarding** radio button to enable the forwarding of system events. This setting is enabled by default.
- Refer to the **Events E-mail Notification** field to define how system event notification E-mails are sent on behalf of the access point profile.

<b>SMTP Server</b>	Specify either the <i>Hostname</i> or <i>IP Address</i> of the outgoing SMTP server where notification E-mails are originated.
<b>Port of SMTP</b>	If a non-standard SMTP port is used on the outgoing SMTP server, select this option and specify a port from 1 - 65,535 for the outgoing SMTP server.
<b>Sender E-mail Address</b>	Specify the E-mail address where notification E-mails are originated.
<b>Recipient's E-mail Address</b>	Specify the destination E-mail address where notification E-mails are sent. Multiple E-mail addresses can be specified by typing each address individually and selecting the button next to the E-mail text box to add it to a list.

<b>Username for SMTP Server</b>	Specify the sender's username on the outgoing SMTP server. Many SMTP servers require users to authenticate with a username and password before sending E-mail through the server.
<b>Password for SMTP Server</b>	Specify the sender's username password on the outgoing SMTP server. Many SMTP servers require users to authenticate with a username and password before sending E-mail through the server.

- Use the **Persist Configuration Across Reloads** option to define how the access point saves (in flash memory) the configuration received from its connected Virtual Controller. Stored configurations can be made available to the access point if the access point's connected Virtual Controller were to be unreachable. Options include *Enabled*, *Disabled* and *Secure*.
- Use the **HTTP Analytics** area to configure how analytics is sent to the HTTP analytics server. Select the **Compress** option to send the HTTP analytics compressed. Use the **Update Interval** fields to configure the update interval between two updates to the HTTP analytics server.
- Select **OK** to save the changes made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.
- Select **Firmware** from the Management menu.



**Figure 5-95** Profile Management - Firmware screen

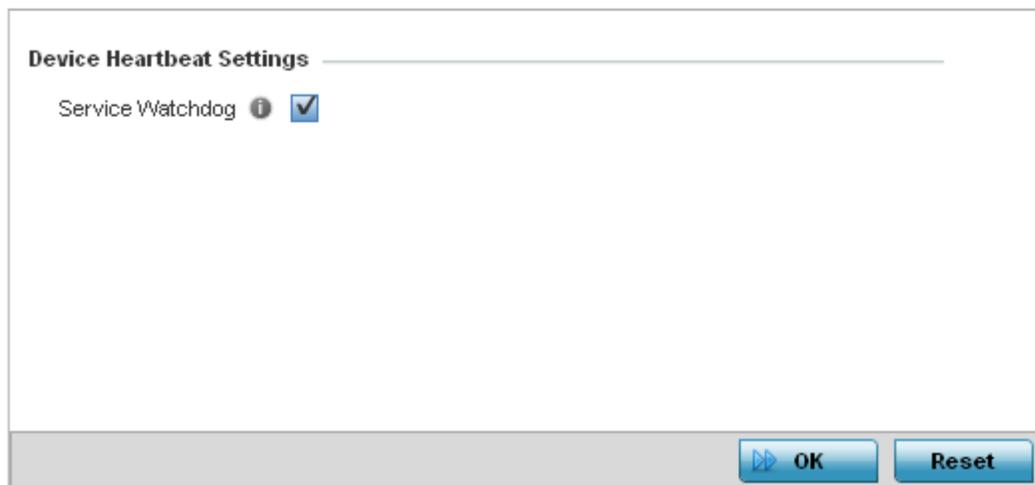
- Refer to the **Auto Install via DHCP** field to define the configuration used by the profile to update firmware using DHCP:

<b>Enable Configuration Update</b>	Select this option to enable automatic configuration file updates for the profile from a location external to the access point. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update. To use this option, first create a Virtual Interface in the Interfaces section and enable the <i>Use DHCP to Obtain Gateway/DNS Servers</i> option for that Virtual Interface.
<b>Enable Firmware Update</b>	Select this option to enable automatic firmware updates (for this profile) from a location external to the access point. To use this option, first create a Virtual Interface in the Interfaces section and enable the <i>Use DHCP to obtain Gateway / DNS Servers</i> option for that Virtual Interface. This value is disabled by default. For information on upgrading an AP6532 from firmware version 5.1, refer to <a href="#">Upgrading AP6532 Firmware from 5.1 on page 5-149</a> .

15. Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware configuration.

<b>Enable Controller Upgrade of AP Firmware</b>	Select the access point model to upgrade to a newer firmware version using its associated Virtual Controller AP's most recent firmware file for that model. The only available option is AP71XX.
<b>Number of Concurrent Upgrades</b>	Use the spinner control to define the maximum number (from 1 - 20) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind, during a firmware upgrade, the access point is offline and unable to perform its normal wireless client support function until the upgrade process is complete.

16. Select **OK** to save the changes made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.
17. Select the **Heartbeat** option from the Management menu.



**Figure 5-96** Profile Management - Device Heartbeat Settings screen

18. Select the **Service Watchdog** option to implement heartbeat messages to ensure other associated devices are up and running. The Service Watchdog is enabled by default.
19. Select **OK** to save the changes made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

### 5.2.11.1 Upgrading AP6532 Firmware from 5.1

#### ► Profile Management Configuration

An existing AP6532 deployment running factory installed 5.1 version firmware can be upgrade to this most recent 5.4 version baseline. To upgrade AP6532 from the 5.1 version baseline:

Ensure you have the following resources:

- A computer with a SSH client and a FTP or TFTP server
- The latest AP6532 5.4 image file in the computer's FTP or TFTP directory
- A PoE hub

1. Calculate the AP6532's IP address.

The AP6532 has an IP of 169.254.<last two digits of its MAC address in decimal>, with subnet mask of 255.255.0.0. For example, if the MAC address is 00-23-68-86-48-18, the last two digits of its IP address will be 72.24 (48 hexadecimal = 72 decimal, 18 hexadecimal = 24 decimal). So the IP address is 169.254.72.24, with subnet mask of 255.255.0.0.

2. Configure the computer with an IP address in the same subnet. For example, 169.254.0.1, and a subnet mask of 255.255.0.0.

3. Ping the AP6532 from the computer to ensure IP connectivity.

4. Open an SSH session on the computer and connect to the AP6532's IP address.

5. Login with a username and password of admin/motorola. The CLI will prompt for a new password. Re-enter the password and confirm.

6. Within the CLI, type **enable**.

7. Enter **commit write memory** to save the new password.

8. To upgrade firmware using a FTP server, use the upgrade command.

```
ftp://<username>:<password>@169.254.0.1/AP6532-5.4.0.0-047R.img.
```

Alternatively, a user can upgrade the AP6532 firmware using a TFTP server using the upgrade command.

```
tftp://169.254.0.1/AP6532-5.4.0.0-047R.img.
```

The AP6532 downloads the firmware from FTP/TFTP server. This process will take a few minutes.

9. When finished, type **reload** to reboot the AP6532. Press 'y' when asked to confirm the reboot.

10. The AP6532 reboots and SSH session is terminated. The reboot takes a couple of minutes.

11. Run a ping from the computer to the AP6532. A ping will be timed out during the reboot.

12. When the ping resumes, start an SSH session again to the AP6532.

13. Login to the AP6532 using the new password and confirm the firmware upgrade is successful by issuing a **show version** command.

### 5.2.11.2 Profile Management Configuration and Deployment Considerations

#### ► Profile Management Configuration

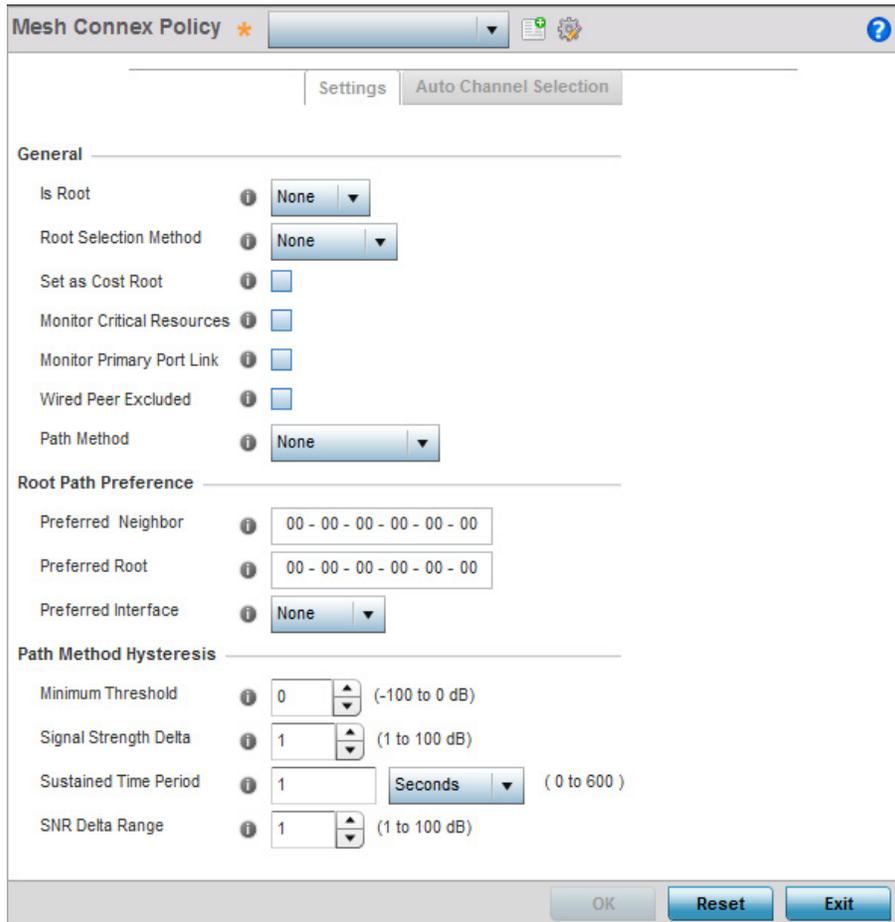
Before defining a access point profile's management configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Define profile management access configurations providing both encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide data privacy and authentication.
- Motorola Solutions recommends SNMPv3 be used for management profile configurations, as it provides both encryption, and authentication.



<b>Monitor Primary Port Link</b>	Displays if this mesh point monitors link status on the primary port.
<b>Path Method</b>	Displays the path selection method used to select the path to the root node.

- Select the **Add** button to create a new Mesh Connex policy.



**Figure 5-98** Mesh Point Configuration - Add Mesh Point Mesh Connex Policy screen

- Refer to the following for more information on the *Mesh Point Mesh Connex Policy* screen:

<b>MeshConnex Policy</b>	Provide a name for the Mesh Connex Policy. Use the <i>Create</i> icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the drop-down and click the <i>Edit</i> icon. For more information on creating or editing a Mesh Connex policy, see <a href="#">MeshConnex Policy on page 6-85</a>
<b>Is Root</b>	From the drop-down menu, select the root behavior of this access point. Select <i>True</i> to indicate this access point is a root node for this mesh network. Select <i>False</i> to indicate this access point is not a root node for this mesh network.

<b>Root Selection Method</b>	<p>Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either <i>None</i>, <i>auto-mint</i> or <i>auto-proximity</i>. The default is <i>None</i>.</p> <p>When <i>auto-mint</i> is selected, root selection is based on the total cost to the root. Cost to the root is measured as total past cost through hops to the root node. Root selection will happen for the root that has the least path cost.</p> <p>When <i>auto-proximity</i> is selected, root selection is based on signal strength of candidate roots.</p> <p><i>None</i> indicates no preference in root selection.</p>
<b>Set as Cost Root</b>	Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default.
<b>Monitor Critical Resource</b>	Select this option to monitor critical resources. If a configured critical resource becomes unavailable, the mesh point is removed from the mesh network.
<b>Monitor Primary Port Link</b>	Select this option to indicate this mesh point monitors the link on the primary port. If the link on the primary port becomes unavailable, the mesh network is brought down.
<b>Wired Peer Exclude</b>	Select this option to exclude wired peers when creating mesh links.
<b>Path Method</b>	<p>From the drop-down menu, select the method to use for path selection in a mesh network. The available options are:</p> <ul style="list-style-type: none"> <li>• <i>None</i> – Select this to indicate no criteria used in root path selection.</li> <li>• <i>uniform</i> – Indicates that the path selection method is uniform. When selected, two paths will be considered equivalent if the average value is the same for these paths.</li> <li>• <i>mobile-snr-leaf</i> – Select this if this access point is mounted on a vehicle or a mobile platform (AP7161 models only). When selected, the path to the route is selected based on the <i>Signal To Noise Ratio</i> (SNR) to the neighbor device.</li> <li>• <i>snr-leaf</i> – Select this to indicate the path with the best signal to noise ratio is always selected.</li> <li>• <i>bound-pair</i> – Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.</li> </ul>
<b>Preferred Neighbor</b>	Enter the MAC address of the mesh point device that is the preferred neighbor.
<b>Preferred Root</b>	Enter the MAC address of the mesh point root that is the preferred root.
<b>Preferred Interface</b>	From the drop-down menu, select the preferred interface for forming a mesh network. Select from <i>None</i> , <i>2.4GHz</i> , <i>4.9GHz</i> or <i>5GHz</i> . The default value is <i>None</i> .
<b>Minimum Threshold</b>	Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered for selection. This field along with <i>Signal Strength Delta</i> and <i>Sustained Time Period</i> are used to dynamically select the next hop in a dynamic mesh network.
<b>Signal Strength Delta</b>	Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value that is higher than the value configured here. This field along with the <i>Minimum Threshold</i> and <i>Sustained Time Period</i> is used to dynamically select the next hop in a dynamic mesh network.
<b>Sustained Time Period</b>	Indicates the duration (in minutes) a signal must sustain the constraints specified in the <i>Minimum Threshold</i> and <i>Signal Strength Delta</i> path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network.

<b>SNR Delta Range</b>	Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB.
------------------------	---



**NOTE:** With this release of Motorola Solutions WiNG software, an AP7161 model access point can be deployed as a *Vehicle Mounted Modem (VMM)* to provide wireless network access to a mobile vehicle (car, train, etc.). A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see [Vehicle Mounted Modem \(VMM\) Deployment Consideration on page 5-158](#).

- Click the **Auto Channel Selection** tab to configure the parameters for the Mesh Connex *Auto Channel Selection* policy. The following screen displays:

**Figure 5-99** Mesh Connex Auto Channel Selection screen

- By default, the **Dynamic Root Selection** screen displays.

This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies. Refer to the following for more information on the *Auto Channel Selection Dynamic Root Selection* screen. These descriptions are common for configuring the 2.4 GHz and 5.0/4.9 GHz frequencies

<b>Channel Width</b>	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
<b>Priority Meshpoint</b>	Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
<b>Off-channel Duration</b>	Configure the duration in the range of 20 - 250 milliseconds for the <i>Off Channel Duration</i> field. This is the duration the scan dwells on each channel when performing an off channel scan.
<b>Off-channel Scan Frequency</b>	Configure the time duration in seconds between two consecutive Off Channel Scans. Set a duration between 1 - 60 seconds.
<b>Meshpoint Root - Sample Count</b>	Configure the number of scans to be performed for data collection before a mesh channel is selected. Set a value between 1 - 10 scans.
<b>Meshpoint Root - Channel Hold Time</b>	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

- Click the **Path Method SNR** tab to configure the signal to noise ratio values when selecting the path to the mesh point root.

**Mesh Point** MeshConnex Policy MeshConnexPolicy\_01

**Settings** **Auto Channel Selection**

**Dynamic Root Selection** **Path Method SNR** **Path Method Root Path Metric**

**For 2.4 GHz**

Channel Width

Priority Meshpoint

SNR Delta  (1 to 100 dB)

SNR Threshold  (-100 to 0 dB)

Off-channel Duration  (20 to 250 milliseconds)

**For 5.0/4.9 GHz**

Channel Width

Priority Meshpoint

SNR Delta  (1 to 100 dB)

SNR Threshold  (-100 to 0 dB)

Off-channel Duration  (20 to 250 milliseconds)

**OK** **Reset** **Exit**

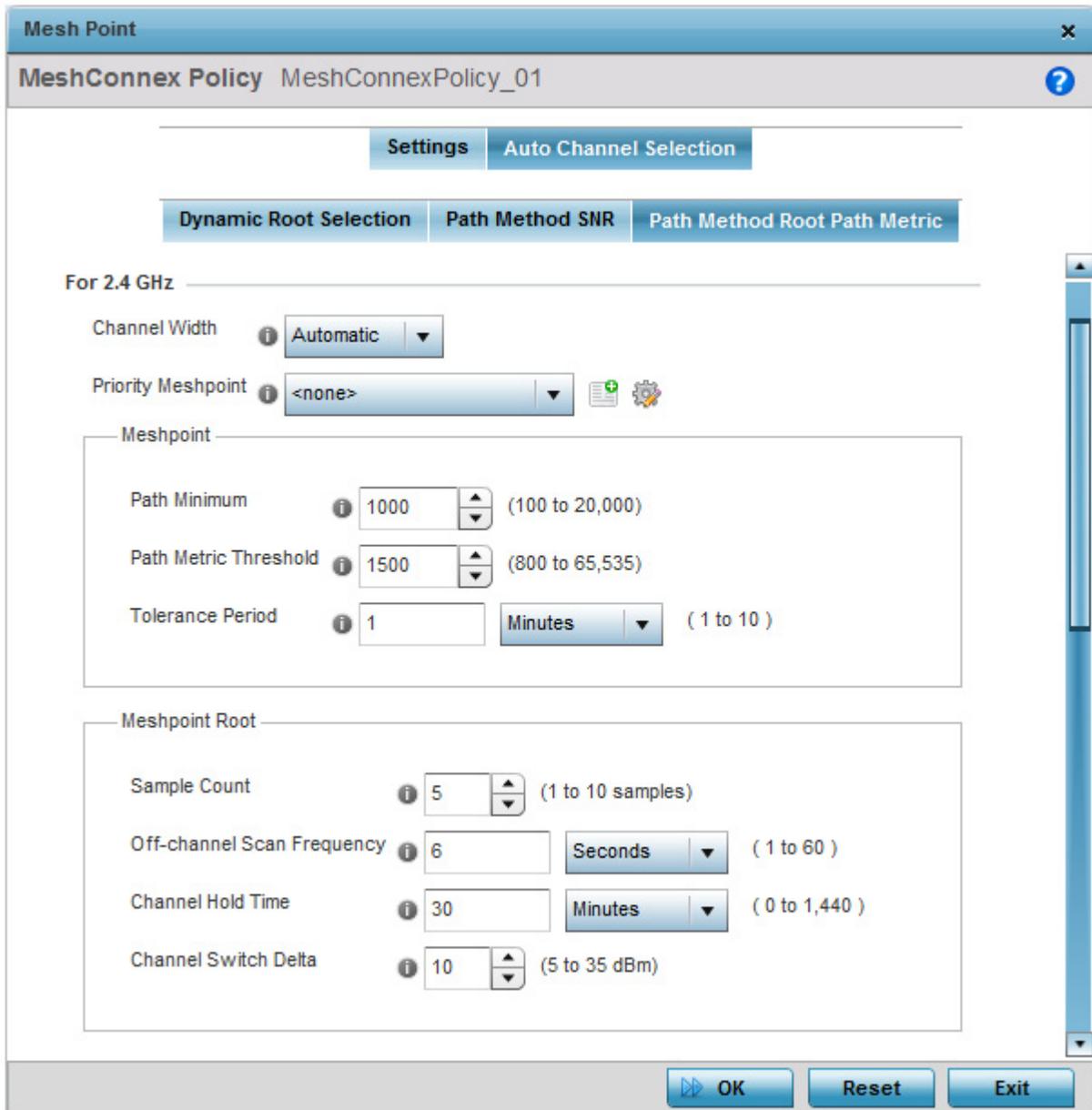
**Figure 5-100** Mesh Point Auto Channel Selection Path Method SNR screen

11. Refer to the following for more information on the *Path Method SNR* screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

<b>Channel Width</b>	<p>Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
<b>Priority Meshpoint</b>	<p>Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.</p>
<b>SNR Delta</b>	<p>Configure the signal to noise ratio delta value for path selection.</p> <p>When path selection happens, this value is considered for selecting the optimal path. A better candidate on a different channel must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network.</p>

<b>SNR Threshold</b>	Configure the signal to noise threshold value for path selection. When the signal strength of the next hop in the mesh network goes below this value, a scan is triggered to select a better next hop.
<b>Off-channel Duration</b>	Configure the duration in the range of 20 - 250 milliseconds for the <i>Off Channel Duration</i> field. This is the duration that the scan dwells on each channel when performing an off channel scan.

- Click the **Path Method Root Path Metric** tab to configure the parameters controlling the calculation of the root path metrics.



**Figure 5-101** Mesh Point Auto Channel Selection Path Method Root Path Metric screen

13. Refer to the following for more information on the *Path Method Root Path Metric* screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

<b>Channel Width</b>	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
<b>Priority Meshpoint</b>	Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
<b>Meshpoint Path Minimum</b>	Configure the minimum path metric value for a mesh connection to be established. Set a value between 100 - 20,000.
<b>Meshpoint Path Metric Threshold</b>	Configure a minimum threshold value for triggering an automatic channel selection for mesh point selection. Set a value in between 800 - 65535.
<b>Meshpoint Tolerance Period</b>	Configure the time duration in seconds to wait before triggering a automatic channel selection for the next hop.
<b>Meshpoint Root Sample Count</b>	Configure the number of scans performed for data collection before a mesh point root is selected. Set a value between 1 - 10 scans.
<b>Meshpoint Root Off-channel Scan Frequency</b>	Configure the time duration in seconds between two consecutive Off Channel Scans for mesh point root. Set a duration between 1 - 60 seconds.
<b>Meshpoint Root Channel Hold Time</b>	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change for mesh point root. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.
<b>Meshpoint Root Channel Switch Delta</b>	Configure the delta value in dBm in the range 5 - 35 dBm which when crossed triggers a mesh point root automatic channel selection.

14. Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this screen.

### 5.2.12.1 Vehicle Mounted Modem (VMM) Deployment Consideration

▶ *Mesh Point Configuration*

Before defining a VMM configuration (mounting an AP7161 mesh point on a moving vehicle), refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Disable layer 2 stateful packet inspection from the firewall policy.
- Set the RTS threshold value to 1 on all mesh devices. The default value is 2347. For more information on defining radio settings, see [Access Point Radio Configuration on page 5-41](#).
- Use *Opportunistic* as the rate selection settings for the AP7161 radio. The default is *Standard*. For more information on defining this settings, see [Radio Override Configuration on page 5-221](#).
- Disable *Dynamic Chain Selection* (radio setting). The default value is enabled. This setting is disabled from the *Command Line Interface* (CLI) using the `dynamic-chain-selection` command, or, in the UI (refer [Radio Override Configuration on page 5-221](#)).
- Disable *A-MPDU Aggregation* if the intended vehicular speed is greater than 30 mph. For more information, see [Radio Override Configuration on page 5-221](#).

## 5.2.13 Advanced Profile Configuration

### ▶ *System Profile Configuration*

An access point profile's advanced configuration is comprised of defining connected client load balance settings, a MINT protocol configuration and miscellaneous settings (NAS ID, access point LEDs and RF Domain Manager).

To set an access point profile's advanced configuration:

1. Select the Configuration tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Expand the **Advanced** menu item.

The following items are available as advanced access point profile configuration options:

- *Advanced Profile Client Load Balancing*
- *Configuring MINT Protocol*
- *Advanced Profile Miscellaneous Configuration*

### 5.2.13.1 Advanced Profile Client Load Balancing

► *Advanced Profile Configuration*

Use the screen to administer the client load across an access point's radios. AP7131 models can have from 1-3 radios depending on the SKU. AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models have 2 radios, while AP6511 and AP6521 models have a single radio.

1. Select **Client Load Balancing** from the expanded **Advanced** menu.

**Figure 5-102** Advanced Profile Configuration - Client Load Balancing screen

2. Use the drop-down menu to define a **SBC strategy**. Options include *Prefer 5GHz*, *Prefer 2.4 GHz*, and *distribute-by-ratio*. The default value is *Prefer 5GHz*.
3. Set the following **Neighbor Selection Strategies**:

<p><b>Use probes from common clients</b></p>	<p>Select this option to use probes from shared clients in the neighbor selection process. This feature is enabled by default, to provide the best common group of available clients amongst access points in neighbor selection.</p>
--	---

<b>Use notifications from roamed clients</b>	Select this option to use roamed client notifications in the neighbor selection process. This feature is enabled by default, allowing access points in the neighbor selection process to consider device roaming counts as selection criteria.
<b>Use smart-rf neighbor detection</b>	Select this option to use SMART RF access point transmission adjustments as criteria in the neighbor selection process. This feature is enabled by default.

- Select the **Balance Band Loads by Ratio** radio button to balance the radio load, by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5.0 GHz band. This setting is enabled by default.
- Set the following **Channel Load Balancing** settings:

<b>Balance 2.4GHz Channel Loads</b>	Select this option to balance loads across channels in the 2.4 GHz radio band. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized. This setting is enabled by default. Selecting this feature enables parameters within the <i>Channel Load Balancing</i> field for assigning weightage and throughput values.
<b>Balance 5GHz Channel Loads</b>	Select this option to balance loads across channels in the 5.0 GHz radio band. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized. This setting is enabled by default. Selecting this feature enables parameters within the <i>Channel Load Balancing</i> field for assigning weightage and throughput values.

- Select the **Balance AP Loads** radio button to distribute this access point's radio load amongst other access point radios. This setting is disabled by default, keeping the load on this access point radio.
- Set the following **Band Control** values within the **Advanced Parameters** field.

<b>Max. Band Load Difference Considered Equal</b>	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing 2.4 and 5GHz radio band load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing 2.4 and 5.0 GHz load balances on this access point. This setting is not available if the <i>Steering Strategy</i> has been set to <i>Disable</i> .
<b>Band Ratio (2.4GHz)</b>	Use the spinner control to set a loading ratio (from 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight the traffic load if wishing to prioritize client traffic on the 2.4 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1. This setting is enabled only when <i>Steer by ratio</i> is selected as the steering strategy.
<b>Band Ratio (5GHz)</b>	Use the spinner control to set a loading ratio (from 0 - 10) the access point 5.0 GHz radio uses in respect to radio traffic on the 5.0 GHz band. This allows an administrator to weight client traffic if wishing to prioritize client traffic on the 5.0 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 5.0 GHz radio band. The default setting is 1. This setting is enabled only when <i>Steer by ratio</i> is selected as the steering strategy.
<b>5 GHz load at which both bands enabled</b>	When the <i>Steering Strategy</i> is set to <i>Steer</i> at 5.0 GHz, use the spinner control to set a value (from 0 - 100%) at which the load on the 2.4 GHz radio is equally preferred to this 5.0 GHz radio load. The default is 10%.

<b>2.4 GHz load at which both bands enabled</b>	When the <i>Steering Strategy</i> is set to Steer at 2.4 GHz, use the spinner control to set a value (from 0 - 100%) at which the load on the 5.0 GHz radio is equally preferred to this 2.4 GHz radio load. The default is 10%.
---	--

8. Set the following **Neighbor Selection** values within the **Advanced Parameters** field:

<b>Minimum signal strength for common clients</b>	When <i>Using probes from common clients</i> is selected as a neighbor selection strategy, use the spinner control to set a value from 0 -100% as signal strength criteria for a client to be regarded as a common client in the neighbor selection process.
<b>Minimum number of clients seen</b>	When <i>Using probes from common clients</i> is selected as a neighbor selection strategy, use the spinner control to set the number of clients (from 0 -256) that must be shared by at least 2 access points to be regarded as neighbors in the neighbor selection process. The default value is 1.
<b>Max confirmed neighbors</b>	Use the spinner control to set the maximum number of access point neighbors (from 0 - 16) of the same model available for load balance distributions. The default setting is 10.
<b>Minimum signal strength for smart-rf neighbors</b>	When <i>Using smart-rf neighbor detection</i> is selected as a neighbor selection strategy, use the spinner control to set a minimum signal strength value (from 0 - 100%) for a SMART RF detected access point to be qualified as a neighbor.

9. Set the following **Channel Load Balancing** values within the **Advanced Parameters** field:

<b>Max. 2.4GHz Load Difference Considered Equal</b>	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing access point 2.4GHz radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances exclusively on the 2.4GHz radio band.
<b>Min. Value to Trigger 2.4GHz Channel Balancing</b>	Use the spinner control to define a threshold (from 1 - 100%) the access point uses (when exceeded) to initiate channel load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within their current channel designations. The default is 5%.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 2.4GHz radio client count in the 2.4GHz radio load calculation. Assign this value higher this 2.4GHz radio is intended to support numerous clients and their throughput is secondary to maintaining association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 2.4 radio throughput in the access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical and more important than a high client connection count. The default setting is 10%.
<b>Max. 5GHz Load Difference Considered Equal</b>	Use the spinner control to set a value (from 0 - 100) considered an adequate discrepancy (or deviation) when comparing access point 5GHz radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances exclusively on the 5GHz radio band.

<b>Min. Value to Trigger 5GHz Channel Balancing</b>	Use the spinner control to define a threshold (from 1 - 100) the access point uses (when exceeded) to initiate channel load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within their current channel designations. The default is 5%.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 5GHz radio client count in the 5GHz radio load calculation. Assign this value higher this 5GHz radio is intended to support numerous clients and their throughput is secondary to maintaining client association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point radio uses to prioritize 5GHz radio throughput in the load calculation. Assign this value higher if throughput and radio performance are considered mission critical and more important than a high client connection count. The default setting is 10%.

10. Set the following **AP Load Balancing** values within the **Advanced Parameters** field:

<b>Min Value to Trigger Load Balancing</b>	Use the spinner control to set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other radios. When the radio load exceeds the defined threshold, load balancing is initiated. The default is 5%.
<b>Max. AP Load Difference Considered Equal</b>	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize client count in the radio load calculation (on both the 2.4 and 5.0 GHz radio bands). Assign this value higher if this radio is intended to support numerous clients and their throughput is secondary to maintaining client association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (from 0 - 100%) the access point radio uses to prioritize radio throughput in the load calculation (on both the 2.4 and 5.0 GHz radio bands). Assign this value higher if throughput and radio performance are considered mission critical and of more importance than a high client connection count. The default setting is 10%.

11. Select **OK** to save the changes made to the Client Load Balancing configuration. Select **Reset** to revert to the last saved configuration.

## 5.2.13.2 Configuring MINT Protocol

### ► *Advanced Profile Configuration*

MINT provides the means to secure access point profile communications at the transport layer. Using MINT, an access point can be configured to only communicate with other authorized (MINT enabled) access points of the same model.

Virtual Controller AP managed access points can communicate with each other exclusively over a MINT security domain. Keys can also be generated externally using any application (like openssl). These keys must be present on the access point managing the domain for key signing to be integrated with the UI. A MAP device that needs to communicate with another first negotiates a security context with that device. The security context contains the transient keys used for encryption and authentication. A secure network requires users know about certificates and PKI. However, administrators do not need to define security parameters for access points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MINT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

To define an access point profile's MINT configuration:

1. Select **MINT Protocol** from the expanded **Advanced** menu. The **Settings** tab displays by default.

The screenshot shows the MINT Protocol configuration screen in the Settings tab. The screen is divided into several sections:

- Area Identifier:** Level 1 Area ID is set to 1 (range: 1 to 16,777,215).
- Priority Adjustment:** Designated IS Priority Adjustment is set to 0 (range: -255 to 255).
- Shortest Path First (SPF):** Latency of Routing Recalculation is set to 0 (range: 0 to 60 seconds).
- MINT Link Settings:**
  - MLCP IP:
  - MLCP VLAN:
  - Tunnel MINT across extended VLAN:
- Tunnel Controller Load Balancing:** Tunnel Controller Load Balancing (Level1):
- Preferred Tunnel Controller Group:** Preferred Tunnel Controller Name:

At the bottom right, there are buttons for **OK** and **Reset**.

**Figure 5-103** Advanced Profile Configuration - MINT Protocol screen - Settings tab

2. Refer to the **Area Identifier** field to define the Level 1 Area IDs used by the profile's MINT configuration.

<b>Level 1 Area ID</b>	Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 4,294,967,295. The default value is disabled.
------------------------	---



**Figure 5-105** Advanced Profile Configuration- MINT Protocol screen - Add IP MiNT Link field

11. Set the following **Link IP** parameters to complete the MINT network address configuration:

<b>IP</b>	Define the IP address used by peer access points for interoperation when supporting the MINT protocol.
<b>Port</b>	Select this option to specify a custom port for MiNT links. Use the spinner control to define the port number (from 1 - 65,535).
<b>Routing Level</b>	Use the spinner control to define a routing level of either 1 or 2.
<b>Listening Link</b>	Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted.
<b>Forced Link</b>	Select this option to specify the MiNT link as a forced link.
<b>Link Cost</b>	Use the spinner control to define a link cost from 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
<b>Adjacency Hold Time</b>	Set a hold time interval in either <i>Seconds</i> (2 - 600) or <i>Minutes</i> (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.
<b>IPsec Secure</b>	Select this option to use a secure link for IPsec traffic. This setting is disabled by default. When enabled, both the header and the traffic payload are encrypted.



**Figure 5-107** Advanced Profile Configuration - MINT Protocol screen - Add/edit VLAN field

14. Set the following parameters to add or modify MINT VLAN configuration:

<b>VLAN</b>	If adding a new VLAN, define a VLAN ID from 1 - 4,094 used by peers for interoperation when supporting the MINT protocol.
<b>Routing Level</b>	If adding a new VLAN, use the spinner control to define a routing level of either 1 or 2.
<b>Link Cost</b>	Use the spinner control to define a link cost from 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 4 seconds.
<b>Adjacency Hold Time</b>	Set a hold time interval in either <i>Seconds</i> (2 - 600) or <i>Minutes</i> (1 - 10) for the transmission of hello packets. The default interval is 13 seconds.

15. Select **OK** to save the updates to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.13.3 Advanced Profile Miscellaneous Configuration

► *Advanced Profile Configuration*

Refer to the advanced profile's *Miscellaneous* menu item to set the profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When the wireless controller authorizes users, it queries the user profile database using a username representative of the physical NAS port making the connection.

1. Select **Miscellaneous** from the expanded **Advanced** menu.

The screenshot shows the 'Advanced Profile Configuration - Miscellaneous' screen. It is organized into several sections, each with a title bar and a horizontal separator line:

- Device RADIUS Authentication Parameters:** Contains two text input fields. The first is labeled 'NAS-Identifier Attribute' and the second is 'NAS-Port-Id Attribute'. Both have an information icon (i) to their left.
- LEDs (Light Emitting Diodes):** Contains a section titled 'Turn on LEDs' with three radio button options: 'Off (0)', 'On (1)' (which is selected), and 'Flash Pattern (2)'. An information icon (i) is to the left of the radio buttons.
- MeshConnex Parameters:** Contains a 'Root Path Monitor Interval' field with a value of '30', a unit dropdown menu set to 'Seconds', and a range '( 1 to 65,535 )'. An information icon (i) is to the left.
- RADIUS Dynamic Authorization:** Contains an 'Additional Port' field with a value of '3799', a unit dropdown menu set to 'Minutes', and a range '( 1 to 65,535 ) (Cisco ISE:1700)'. An information icon (i) is to the left.
- Client Bridge:** Contains an 'Aging Time' field with a value of '10', a unit dropdown menu set to 'Minutes', and a range '( 1 to 10,923 )'. An information icon (i) is to the left.

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

**Figure 5-108** Advanced Profile Configuration - Miscellaneous screen

2. Set a **NAS-Identifier Attribute** up to 253 characters.  
This is the RADIUS NAS-Identifier attribute that typically identifies the access point where a RADIUS message originates.
3. Set a **NAS-Port-Id Attribute** up to 253 characters.  
This is the RADIUS NAS port ID attribute which identifies the port where a RADIUS message originates.
4. Select the **Turn on LEDs** radio button to ensure this access point's LED remain continuously illuminated. Deployments such as hospitals prefer to keep their wireless devices from having illuminating LEDs, as they have been reported to disturb their patients. this setting, however, is enabled by default.  
  
Select the **Flash Pattern** radio button to enable the access point to blink in a manner that is different from its operational LED behavior. Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate that the initial configuration is complete.
5. Set the appropriate **Meshpoint Behavior** value by selecting either *external* (Fixed) or *vehicle-mounted* from the drop-down menu. The value vehicle-mounted indicates that the mesh point is mobile. This feature is only available on an AP7161 model access point.

6. Set the appropriate **Root Path Monitor Interval** value. This setting configures the frequency at which the path to the root mesh point is monitored.
7. Set the **Additional Port** value for **RADIUS Dynamic Authorization** field. Set this value to 1700 to enable a CISCO *Identity Services Engine (ISE) Authentication, Authorization and Accounting (AAA)* server, when deployed in the network, to dynamically authenticate a client.

When a client requests access to the network, the CISCO ISE RADIUS server presents the client with a URL where the device's compliance to the networks security such as validity of anti-virus or anti-spyware software is checked for the validity of their definition files (this checking is called posture). If the client device complies, then it is allowed access to the network.

8. Set the **Aging Time** value for **Client Bridge**. Use the spinner control to set a value in *days, hours, minutes* and *seconds*.
9. Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

### 5.2.14 Environmental Sensor Configuration

#### ▶ System Profile Configuration

---

---



**NOTE:** This feature is available on the AP8132 model only.

---

---

An AP8132 sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the access point's radio coverage area. The output of the sensor's detection mechanisms are viewable using the *Environmental Sensor* screen.

To set an environmental sensor configuration for an AP8132 model access point:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **System Profile** from the options on left-hand side of the UI.
4. Select **Environmental Sensor**. The *Environmental Sensor* screen displays.

**Light Sensor**

Enable Light Sensor

Polling Time to Determine if Light is On/Off  Seconds ( 2 to 201 )

Shutdown WLAN Radio at Low Limit of Light Threshold

Low Limit of Light Threshold  (0 to 1,000 lux)

High Limit of Light Threshold  (100 to 10,000 lux)

**Environmental Sensors**

Enable Temperature Sensor

Enable Motion Sensor

Enable Humidity Sensor

**Shared Configuration**

Polling Interval for All Sensors  Seconds ( 1 to 100 )

OK Reset Exit

**Figure 5-109** Profile - Environmental Sensor screen

5. Set the following **Light Sensor** settings for the access point's sensor module:.

<b>Enable Light Sensor</b>	Select this option to enable the light sensor on the module. This setting is enabled by default. The light sensor reports whether the access point has its light sensor powered on or off.
<b>Polling Time to Determine if Light is On/ Off</b>	Define an interval in <i>Seconds</i> (2 - 201) or <i>Minutes</i> (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 10 seconds. Light intensity is used to determine whether the access point's deployment location is currently populated with clients.
<b>Shutdown WLAN Radio at Low Limit of Light Threshold</b>	Select this option to power off the access point's radios if the light intensity falls below the set threshold. If enabled, select <i>All</i> (both radios), <i>radio-1</i> or <i>radio-2</i> .
<b>Low Limit of Light Threshold</b>	Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the access point's deployment location. The default is 100.
<b>High Limit of Light Threshold</b>	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the access point's deployment location. The default is 500.

6. Enable or disable the following **Environmental Sensors**:

<b>Enable Temperature Sensor</b>	Select this option to enable the module's temperature sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
----------------------------------	---

<b>Enable Motion Sensor</b>	Select this option to enable the module's motion sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
<b>Enable Humidity Sensor</b>	Select this option to enable the module's humidity sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.

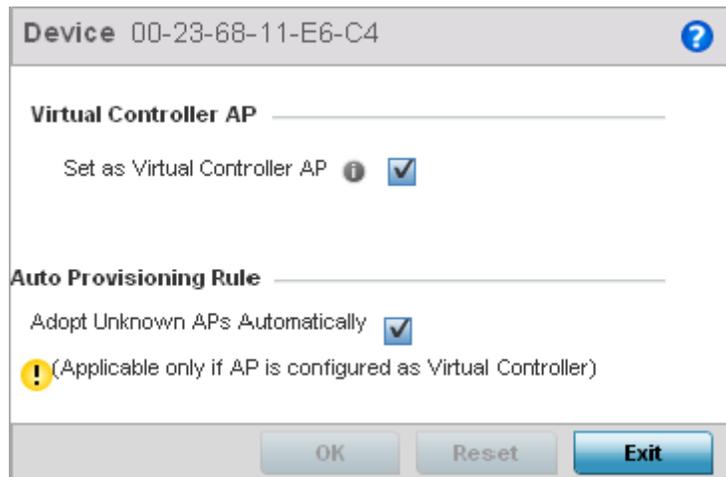
7. Define or override the following **Shared Configuration** setting:

<b>Polling Interval for All Sensors</b>	Set an interval in either <i>Seconds</i> (1 - 100) or <i>Minutes</i> (1 - 2) for the time between all environmental polling (both light and environment). The default setting is 5 seconds.
---	---

8. Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.



4. The **Virtual Controller AP** screen lists all peer access points within this Virtual Controller's radio coverage area. Each listed access point is listed by its assigned System Name, MAC Address and Virtual Controller designation. Only Standalone APs of the same model can have their Virtual Controller AP designation changed.
5. Either select an access point from those displayed and select **Edit**, or use the device browser in the lower left-hand side of the UI to select an access point.



**Figure 5-111** Managing Virtual Controller - AP Designation screen

6. Select the **Set as Virtual Controller AP** radio button to change the selected access point's designation from Standalone to Virtual Controller AP. Remember, a Virtual Controller can manage (up to) 24 access points of the same model. Thus, an administrator should take care to change the designation of a Virtual Controller AP to Standalone AP to compensate for a new Virtual Controller AP designation.
7. Select the **Adopt Unknown APs Automatically** option to allow a Virtual Controller to adopt APs it does not recognize. While this option may help in the administration and management of all the APs in the network, it introduces the risk of allowing device association to a potential rogue device. Consequently, this setting is disabled by default.
8. Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Delete** to remove obsolete rows as needed.

## 5.4 Overriding a Device Configuration

### ► [Device Configuration](#)

Devices within the access point managed network can have an override configuration defined and applied. New devices can also have an override configuration defined and applied once



---

**NOTE:** The best way to administer a network populated by numerous access points is to configure them directly from the designated Virtual Controller AP. If an access point's configuration requires an exception from the Virtual Controller AP's assigned profile configuration the administrator should apply a Device Override to change just that access point's configuration. For more information on applying an override to an access point's Virtual Controller AP assigned configuration profile, see [Device Overrides on page 5-195](#).

---

Refer to the following configuration overrides, applicable to devices within a access point managed network:

- [Basic Configuration](#)
- [Certificate Management](#)
- [RF Domain Overrides](#)
- [Wired 802.1X Overrides](#)
- [Device Overrides](#)

### 5.4.1 Basic Configuration

#### ► [Overriding a Device Configuration](#)

Applying a basic configuration override to a device entails changing (overriding) the device's system name, deployment area, building floor and system clock.

When a device is initially deployed, it requires several basic configuration parameters be set and its deployment location defined. Additionally, the number of permitted licenses needs to be accessed to determine whether new devices can be adopted (if in Virtual Controller AP mode).

To override a managed device's basic configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **Device Overrides**.
4. Select a target device MAC address from either the device browser in the lower, left-hand side of the UI or within the *Device Overrides* screen.

The *Basic Configuration* screen displays by default.

**Configuration**

System Name

Latitude Coordinate  (-90.0000 - 90.0000)

Longitude Coordinate  (-180.0000 - 180.0000)

**Location**

Area

Floor

**Device Overrides**

**Set Clock**

Device Time 2012-04-12 01:17:55 UTC

New Time    :   AM  PM

Setting the clock may logout the current session.

**Figure 5-112** Device Overrides - Basic Configuration screen

5. Set the following **Configuration** settings for the target device:

<b>System Name</b>	Provide the selected device a system name up to 64 characters in length. This is the device name that appears within the RF Domain or Profile the access point supports and is identified by.
<b>Latitude Coordinate</b>	Optionally provide the latitude coordinate where the device is located. The valid value for this field is in the range -90.0000 degrees to +90.0000 degrees. When provided, this enables the device to be mapped on the geolocation map.
<b>Longitude Coordinate</b>	Optionally provide the longitude coordinate where the device is located. The valid value for this field is in the range -180.0000 degrees to +180.0000 degrees. When provided, this enables the device to be mapped on the geolocation map.
<b>Area</b>	Assign the access point an <i>Area</i> representative of the location the access point is physically deployed. The name cannot exceed 64 characters. Assigning an area is helpful when grouping access points in profiles, as access points in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.
<b>Floor</b>	Assign the target access point a building <i>Floor</i> name representative of the location the access point was physically deployed. The name cannot exceed 64 characters. Assigning a building floor name is helpful when grouping devices in profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

6. Refer to the **Device Overrides** field to assess whether overrides have been applied to the device's configuration. Use the **Clear Overrides** button to clear all device overrides and reset the configuration to its default values.
7. Refer to the **Set Clock** field to update the system time.

Refer to the **Device Time** parameter to assess the device's current time. If the device's time has not been set, the device time is displayed as unavailable. Select **Refresh** to update the device's system time.

Use the **New Time** parameter to set the calendar day, hour and minute. Use the AM and PM radio buttons to refine whether the updated time is for the AM or PM. This time can be synchronized with the use of an external NTP resource.

When completed, select **Update Clock** to commit the updated time to the device.

8. Select **OK** to save the changes to the basic configuration. Selecting **Reset** reverts the screen to its last saved configuration.

## 5.4.2 Certificate Management

### ► *Overriding a Device Configuration*

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a client to access resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides with the licensed device, while the private portion remains on the client.

The certificate configuration used by an access point managed device can be changed (overridden) as changes in security credentials require modification in the management of the device.

To override a managed device's certificate configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **Device Overrides**.
4. Select a target device's MAC address from the device browser in the lower, left-hand side of the UI.
5. Select **Certificates** from the **Device** menu.

**Management Security**

HTTPS Trustpoint Pending    
 Stored  default-trustpoint ▼ Launch Manager

SSH RSA Key Pending    
 Stored  default\_rsa\_key ▼ Launch Manager

**RADIUS Security**

RADIUS Certificate Authority Pending    
 Stored  default-trustpoint ▼ Launch Manager

RADIUS Server Certificate Pending    
 Stored  default-trustpoint ▼ Launch Manager

**Information**

"Pending" Trustpoints and RSA Keys have not been verified to exist on the device.

OK Reset Exit

**Figure 5-113** Device Overrides - Certificates screen

6. Set the following **Management Security** certificate configurations:

<b>HTTPS Trustpoint</b>	Either use the default-trustpoint or select the <i>Stored</i> radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To leverage an existing device certificate for use with this target device, select the <i>Launch Manager</i> button. For more information, see <a href="#">Manage Certificates on page 5-179</a> .
<b>SSH RSA Key</b>	Either use the default_rsa_key or select the <i>Stored</i> radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing key, select the <i>Launch Manager</i> button. For more information, see <a href="#">RSA Key Management on page 5-183</a> .

7. Set the **RADIUS Security** certificate configuration. Select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To leverage an existing device certificate for use with this target device, select the **Launch Manager** button.



**NOTE:** Pending trustpoints and RSA keys are typically not verified as existing on a device.

8. Select **OK** to save the changes made to the certificate configurations. Selecting **Reset** reverts the screen to its last saved configuration.



2. Select a device from amongst those displayed to review its certificate information.  
Refer to **Certificate Details** to review the certificate's properties, self-signed credentials, validity period and CA information.
3. To optionally import a certificate, select the **Import** button from the **Certificate Management** screen. The **Import New Trustpoint** screen displays.

**Import New Trustpoint**

Import ⓘ  
 Import CA ⓘ  
 Import CRL ⓘ  
 Import Signed Cert ⓘ

Trustpoint Name \*

**Location of Trustpoint**

From Network

Protocol: ftp Port: 21 **Basic**

Host: 0 . 0 . 0 . 0 IP Address

User Name:

Password:

Path/File:

OK Cancel

**Figure 5-115** Certificate Management - Import New Trustpoint screen

4. Define the following configuration parameters required for the Import of the trustpoint:

<b>Import</b>	Select the type of Trustpoint to import. The following Trustpoints can be imported: <ul style="list-style-type: none"> <li>• <i>Import</i> – Select to import any trustpoint.</li> <li>• <i>Import CA</i> – Select to import a <i>Certificate Authority</i> (CA) certificate on to the access point.</li> <li>• <i>Import CRL</i> – Select to import a <i>Certificate Revocation List</i> (CRL), CRLs are used to identify and remove those installed certificates that have been revoked or are no longer valid.</li> <li>• <i>Import Signed Cert</i> – Select to import a self signed certificate.</li> </ul>
<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a *CA certificate*.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A *certificate revocation list* (CRL) is a list of revoked certificates, or certificates no longer valid. A certificate can be revoked if the CA improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

*Signed certificates* (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

5. Define the following configuration to import the Trustpoint from a location on the network. To do so, select **From Network** and provide the following information.

<b>URL</b>	Provide the complete URL to the location of the trustpoint. This option is available by default. Click the <i>Advanced</i> link next to this field to display more fields to provide detailed trustpoint location information.
<b>Protocol</b>	If using <i>Advanced</i> settings, select the protocol used for importing the target trustpoint. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If using <i>Advanced</i> settings, use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>IP Address</b>	If using <i>Advanced</i> settings, enter IP address of the server used to import the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .

<b>Host</b>	If using <i>Advanced</i> settings, provide the hostname of the server used to import the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If using <i>Advanced</i> settings, specify the path to the trustpoint. Enter the complete path to the file on the server.

6. Select the **Cut and Paste** option to paste the trustpoint information in text. When this option is selected, the text box next to it is enabled. Paste the trustpoint details into the text box.
7. Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
8. To optionally export a trustpoint to a remote location, select the **Export** button from the **Certificate Management** screen. Once a certificate has been generated on the authentication server, export the self-signed certificate.

A digital CA certificate is different from a self-signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an Active Directory Group Policy for automatic root-certificate deployment.

Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

**Figure 5-116** Certificate Management - Export Trustpoint screen

9. Define the following configuration parameters to export a trustpoint:

<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
<b>URL</b>	Provide the complete URL to the location of the trustpoint. If needed, select <i>Advanced</i> to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol.
<b>Protocol</b>	Select the protocol used for exporting the target trustpoint. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If using <i>Advanced</i> settings, use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>IP Address</b>	If using <i>Advanced</i> settings, enter IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	If using <i>Advanced</i> settings, provide the hostname of the server used to export the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If using <i>Advanced</i> settings, specify the path to the trustpoint. Enter the complete relative path to the file on the server.

10. Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

To optionally delete a trustpoint, select the **Delete** button from within the **Certificate Management** screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select the **Delete RSA Key** option to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the *Certificate Management* screen.

#### 5.4.2.1.1 RSA Key Management

##### ► *Certificate Management*

Refer to the RSA Keys screen to review existing RSA key configurations applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import or export an existing key to and from a remote location.

*Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1. Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).
2. Select **RSA Keys** from the upper, left-hand side of the **Certificate Management** screen.

The screenshot displays the 'RSA Keys' management interface. At the top, there are four tabs: 'Manage Certificates', 'RSA Keys', 'Create Certificate', and 'Create CSR'. Below the tabs is a header 'RSA Keys' with a help icon. The main content area is titled 'All Certificates Details' and contains a table with the following data:

RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDks5UoQxrpQFuq5sVJBPrLAp4/ EUyIDrG2FaphnqYSbbZlifoL4pMiS81bRk8pr7gMz0BK9Cg3TH/QsNaqRKWJVkZd OAsn1wOvOpTwHNsdLMWuGLgT3L2Oe2QaNIAdiOAlyW8lu79jnUM7but5ApPd4uZK L90Ls+tenw9t/st1XwIDAQAB -----END PUBLIC KEY-----

Below the table, the 'Certificate Details' section is expanded for the selected key, showing the following information:

- RSA Name: default\_rsa\_key
- Size: 1024
- RSA Public Key: -----BEGIN PUBLIC KEY-----  
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDks5UoQxrpQFuq5sVJBPrLAp4/  
EUyIDrG2FaphnqYSbbZlifoL4pMiS81bRk8pr7gMz0BK9Cg3TH/QsNaqRKWJVkZd  
OAsn1wOvOpTwHNsdLMWuGLgT3L2Oe2QaNIAdiOAlyW8lu79jnUM7but5ApPd4uZK  
L90Ls+tenw9t/st1XwIDAQAB  
-----END PUBLIC KEY-----

At the bottom of the interface, there are four buttons: 'Generate Key', 'Import', 'Export', and 'Delete'.

**Figure 5-117** Certificate Management - RSA Keys screen

3. Select a listed device to review its current RSA key configuration.  
Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.
4. Select the **Generate Key** button to create a new key.

**Figure 5-118** Certificate Management - Generate RSA Key screen

5. Define the following configuration parameters required to generate a key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Size</b>	Use the spinner control to set the size of the key (from 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality.

6. Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.  
 7. To optionally import a CA certificate, select the **Import** button from the RSA Keys screen.

**Figure 5-119** Certificate Management - Import New RSA Key screen

8. Define the following configuration parameters required to import a RSA key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key
-----------------	---

<b>Key Passphrase</b>	Define the key used by both the access point and the server (or repository) of the target RSA key. Select the <i>Show</i> option to expose the actual characters used in the passphrase. Leaving the <i>Show</i> option unselected displays the passphrase as a series of asterisks "***".
<b>URL</b>	Provide the complete URL to the location of the RSA key.
<b>Protocol</b>	If selecting <i>Advanced</i> , select the protocol used for importing the target key. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If selecting <i>Advanced</i> , use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>IP Address</b>	If selecting <i>Advanced</i> , enter IP address of the server used to import the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	If selecting <i>Advanced</i> , provide the hostname of the server used to import the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If selecting <i>Advanced</i> , specify the path to the RSA key. Enter the complete relative path to the key on the server.

9. Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.
10. To optionally export a **RSA key** to a remote location, select the **Export** button from the RSA Keys screen.
11. Export the key to a RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

**Figure 5-120** Certificate Management - Export RSA Key screen

12. Define the following configuration parameters required to export a RSA key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Passphrase</b>	Define the key passphrase used by both the access point and the server. Select the <i>Show</i> option to expose the actual characters used in the passphrase. Leaving the <i>Show</i> option unselected displays the passphrase as a series of asterisks "*".
<b>URL</b>	Provide the complete URL to the location of the key.
<b>Protocol</b>	If selecting <i>Advanced</i> , select the protocol used for exporting the RSA key. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If selecting <i>Advanced</i> , use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .

<b>IP Address</b>	If selecting <i>Advanced</i> , enter the IP address of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	If selecting <i>Advanced</i> , provide the hostname of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If selecting <i>Advanced</i> , specify the path to the key. Enter the complete relative path to the key on the server.

13. Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.
14. To optionally delete a key, select the **Delete** button from within the RSA Keys screen. Provide the key name within the **Delete RSA Key** screen and select the **Delete Certificates** option to remove the certificate and the supported key. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

#### 5.4.2.1.2 Certificate Creation

##### ▶ *Certificate Management*

The *Certificate Management* screen provides the facility for creating new self-signed certificates. Self-signed certificates (often referred to as root certificates) do not use public or private CAs. A self-signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate:

1. Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).
2. Select **Create Certificate** from the upper, left-hand, side of the **Certificate Management** screen.

**Figure 5-121** Certificate Management - Create Certificate screen

3. Set the following **Create New Self-Signed Certificate** configuration parameters:

<b>Certificate Name</b>	Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
<b>Use Existing</b>	Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key.
<b>Create New</b>	Select this option to create a new RSA key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting (1024) to ensure optimum functionality. For more information on creating a new RSA key, see <a href="#">RSA Key Management on page 5-183</a> .

4. Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

<b>Certificate Subject Name</b>	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-configured</i> to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
<b>Country (C)</b>	Define the Country of deployment for the certificate. The field can be modified by the user. This is a required field and must not exceed 2 characters.

<b>State (ST)</b>	Enter a State for the state or province name used in the certificate. This is a required field.
<b>City (L)</b>	Enter a City to represent the city name used in the certificate. This is a required field.
<b>Organization (O)</b>	Define an Organization for the organization used in the certificate. This is a required field.
<b>Organizational Unit (OU)</b>	Enter an Organizational Unit for the name of the organization unit used in the certificate. This is a required field.
<b>Common Name (CN)</b>	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Set the following **Additional Credentials** required for the generation of the self-signed certificate:

<b>Email Address</b>	Provide an E-mail address used as the contact address for issues relating to this certificate request.
<b>Domain Name</b>	Enter a <i>fully qualified domain name</i> (FQDN) as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
<b>IP Address</b>	Specify the IP address used as the destination for certificate requests.

6. Select the **Generate Certificate** button at the bottom of the screen to generate the certificate.

### 5.4.2.1.3 Generating a Certificate Signing Request

#### ► *Certificate Management*

A *certificate signing request* (CSR) is an application from a requestor to a certificate authority to issue a digitally signed identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1. Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).
2. Select **Create CSR** from the upper, left-hand, side of the **Certificate Management** screen.

**Figure 5-122** Certificate Management - Create CSR screen

3. Set the following **Create New Certificate Signing Request (CSR)** configuration parameters:

<b>Create New</b>	Select this option to create a new RSA Key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting (1024) to ensure optimum functionality. For more information on creating a new RSA key, see <a href="#">RSA Key Management on page 5-183</a> .
<b>Use Existing</b>	Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key.

4. Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

<b>Certificate Subject Name</b>	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-defined</i> to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
<b>Country (C)</b>	Define the Country used in the CSR. The field can be modified by the user. This is a required field and must not exceed 2 characters.
<b>State (ST)</b>	Enter a State for the state or province name used in the CSR. This is a required field.
<b>City (L)</b>	Enter a City to represent the city name used in the CSR. This is a required field.
<b>Organization (O)</b>	Define an Organization for the organization used in the CSR. This is a required field.

<b>Organizational Unit (OU)</b>	Enter an Organizational Unit for the name of the organization unit used in the CSR. This is a required field.
<b>Common Name (CN)</b>	If there's a Common Name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Select the following **Additional Credentials** required for the generation of the CSR:

<b>Email Address</b>	Provide an E-mail address used as the contact address for issues relating to this CSR.
<b>Domain Name)</b>	Enter a FQDN as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
<b>IP Address</b>	Specify the IP address used as the destination for certificate requests.

6. Select the **Generate CSR** button at the bottom of the Create CSR screen to generate the CSR.

### 5.4.3 RF Domain Overrides

#### ► *Overriding a Device Configuration*

Use *RF Domain Overrides* to define settings overriding a target device's original RF Domain configuration.

An RF Domain allows an administrator to assign configuration data to multiple access points (of the same model) deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement from their original RF Domain administered design. Unlike a RFS series controller, an access point supports a single RF domain. An access point RF Domain cannot be used on a different model access point. For example, an AP6532 RF Domain override can only be applied to another AP6532 model access point.

To define a device's RF Domain override configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the **Configuration** tab.
3. Select **Device Overrides**.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **RF Domain Overrides**.

**Figure 5-123** Device Overrides -RF Domain Overrides screen



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove a device's override, go to the *Basic Configuration* screen's *Device Overrides* field, and then select the *Clear Overrides* button.

- Refer to the **Basic Configuration** field to review the basic settings defined for the target device's RF Domain configuration, and optionally assign/remove overrides to and from specific parameters.

<b>Location</b>	Set the deployment location for the access point as part of its RF Domain configuration.
<b>Contact</b>	Set the administrative contact for the access point. This should reflect the administrator responsible for the access point's configuration and wireless network.
<b>Time Zone</b>	Use the drop-down menu to select the geographic time zone supporting its deployment location.
<b>Country Code</b>	Use the drop-down menu to select the country code supporting its deployment location.

- Refer to the **Statistics** field to set the following:

<b>Window Index</b>	Use the spinner control to set a numerical index used as an identifier for each RF Domain statistics configuration defined.
<b>Sample Interval</b>	Use the spinner control to define the interval (in seconds) used to capture statistics supporting the listed RF Domain configuration. The default is 5 seconds.
<b>Window Size</b>	Use the spinner control to set the number of samples used to define RF Domain statistics. The default value is 3 samples.

- Click **+ Add Row** button to add up to two (2) rows to the **Statistics** field.

9. Select **OK** to save the changes and overrides made to the RF Domain configuration. Selecting **Reset** reverts the screen to its last saved configuration.

## 5.4.4 Wired 802.1X Overrides

### ► *Overriding a Device Configuration*

802.1X provides administrators secure, identity based access control as another data protection option to utilize with a device profile.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the user or device.

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **Device Overrides** from the options on left-hand side of the UI.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **Wired 802.1x**.

The screenshot shows the 'Wired 802.1X Settings' configuration page. It includes the following elements:

- Dot1x Authentication Control:** A checkbox that is currently unchecked.
- Dot1x AAA Policy:** A dropdown menu with a downward arrow.
- Dot1x Guest VLAN Control:** A checkbox that is currently unchecked.
- MAC Authentication AAA Policy:** A dropdown menu with a downward arrow, and two small icons (a green plus sign and a gear) to the right.
- Buttons:** 'OK' and 'Reset' buttons are located at the bottom right of the configuration area.

**Figure 5-124** Profile Wired 802.1X screen

6. Set the following **Wired 802.1x Settings**:

<b>Dot1x Authentication Control</b>	Select this option to globally enable 802.1x authentication for the <i>access point</i> . This setting is disabled by default.
<b>Dot1x AAA Policy</b>	Use the drop-down menu to select an AAA policy to associate with the wired 802.1x traffic. If a suitable AAA policy does not exist, click the <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.
<b>Dot1x Guest VLAN Control</b>	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
<b>MAC Authentication AAA Policy</b>	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.

7. Select **OK** to save the changes to the 802.1x override configuration. Select **Reset** to revert to the last saved configuration.

## 5.4.5 Device Overrides

### ► Overriding a Device Configuration

A profile enables an administrator to assign a common set of configuration parameters and policies to another access point of the same model. Profiles can be used to assign shared or unique network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

However, device profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could require modification from a profile configuration shared amongst numerous devices deployed within a particular site.

Use device overrides to define configurations overriding the parameters set by the target device's original profile configuration.

To define a general profile override configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the **Configuration** tab.
3. Select **Device Overrides**.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **Device Overrides** from the Device menu to expand it into sub menu options.
6. Select **General** if it does not display by default.

**Network Time Protocol (NTP)**

Autokey	Key	Preferred	Server IP	Version	

**RF Domain Manager**

Capable

Priority  (1 to 255)

**Buttons:** + Add Row, OK, Reset, Exit

**Figure 5-125** Device Overrides - General screen



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

7. Select **+ Add Row** below the **Network Time Protocol (NTP)** table to define (or override) the configurations of NTP server resources used to obtain system time. Set the following parameters to define the NTP configuration:

<b>AutoKey</b>	Select this option to enable an autokey configuration for the NTP resource. This is a key randomly generated for use between the access point and its NTP resource. The default setting is disabled.
<b>Key</b>	If an autokey is not being utilized, you must manually enter a 64 character maximum key shared for interoperation.
<b>Prefer</b>	Select this option to designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources will be given first opportunity to connect to and provide NTP calibration.
<b>Server IP</b>	Set the IP address of each server added as a potential NTP resource.
<b>Version</b>	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.

8. Refer to the **RF Domain Manager** field to configure this device as a RF Domain manager.
9. Select the **Capable** option to enable or disable this device as a RF Domain manager.
10. Select the **Priority** option to enable configuring a priority value for this device when election to become a Domain Manager is conducted. Set a value using the spinner control. Setting a low value increases the chance of this device becoming the RF Domain manager.
11. Select **OK** to save the changes and overrides made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

Refer to the following to complete the override of the access point's entire profile configuration:

- [Radio Power Overrides](#)
- [Adoption Overrides](#)
- [Profile Interface Override Configuration](#)
- [Overriding the Network Configuration](#)
- [WAN Backhaul Overrides](#)
- [Overriding a Security Configuration](#)
- [Overriding a Services Configuration](#)
- [Overriding a Management Configuration](#)
- [Overriding an Advanced Configuration](#)
- [Overriding Mesh Point Configuration](#)
- [Overriding Environmental Sensor Configuration](#)

### 5.4.5.1 Radio Power Overrides

#### ▶ *Device Overrides*

Use the *Power* screen to set or override one of two power modes (*3a* for *Auto*) for an access point. When *Automatic* is selected, the access point safely operates within available power. Once the power configuration is determined, the access point configures its operating power characteristics based on its model and power configuration.

An access point uses a *complex programmable logic device* (CPLD). The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the maximum power budget. When an access point is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the access point. The CPLD also determines the access point hardware SKU (model) and the number of radios. If the access point's POE resource cannot provide sufficient power to run the access point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- *The access point's transmit and receive algorithms could be negatively impacted*
- *The access point's transmit power could be reduced due to insufficient power*
- *The access point's WAN port configuration could be changed (either enabled or disabled)*

To define an access point's power configuration or apply an override to an existing parameter:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the **Configuration** tab.
3. Select **Device Overrides**.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **Device Overrides** from the Device menu to expand it into sub-menu options.
6. Select **Power**.

A screen displays where an access point's power configuration can be defined or overridden.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

---

---

**Power Mode Configuration on this AP**

Power Mode i Automatic ▼

! AP must be restarted for power-management change to take effect.

**802.3af Power Mode**

802.3af Mode i Throughput ▼

**802.3at Power Mode**

802.3at Mode i Throughput ▼

OK Reset Exit

**Figure 5-126** Device Overrides - Power screen

7. Use the **Power Mode** drop-down menu to set or override the Power Mode Configuration on this AP.



**NOTE:** Single radio model access point's always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models.

When an access point is powered on for the first time, the system determines the power budget available. Using the Automatic setting, the access point automatically determines the best power configuration based on the available power budget. Automatic is the default setting.

If 802.3af is selected, the access point assumes 12.95 watts are available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts are available.

8. Set or override the access point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

Use the drop-down menu to define a mode of either *Range* or *Throughput*.

Select *Throughput* to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance. Select *Range* when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. Throughput is the default setting for both 802.3af and 802.3at.

9. Select **OK** to save the changes and overrides made to the access point power configuration. Select **Reset** to revert to the last saved configuration

## 5.4.5.2 Adoption Overrides

### ▶ *Device Overrides*

Use the *Adoption* screen to define the configuration of a preferred Virtual Controller, wireless controller, or service platform resource used for access point adoption. A Virtual Controller can adopt up to 24 access points of the same model. The Virtual Controller must also share its VLAN to peer access points wishing to adopt to it. The Virtual Controllers IP address (or hostname), pool and routing level must also be defined and made available to connecting peers.

Adoption is the process an access point uses to discover Virtual Controllers available in the network, pick the most desirable Virtual Controller, establish an association, obtain its configuration and consider itself provisioned.

At adoption, an access point solicits and receives adoption responses from Virtual Controllers available on the network.

To define an access point's Virtual Controller configuration or apply an override to an existing parameter:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the Configuration tab.
3. Select **Device Overrides**.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **Device Overrides** from the Device menu to expand it into sub menu options.
6. Select **Adoption**.

A screen displays where an access point's Virtual Controller group, VLAN and network address information can be defined or overridden for the preferred Virtual Controller resource.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

---

---

The screenshot shows the 'Device Overrides - Adoption' configuration screen. It includes the following sections:

- Controller Group:** A text input field for 'Preferred Group' with an information icon.
- Controller VLAN:** A spinner control for 'VLAN' set to 1, with a range of (1 to 4,094).
- Controller Hello Interval:** A spinner control for 'Hello Interval' set to 1, with a range of (1 to 120).
- Adjacency Hold Time:** A spinner control for 'Adjacency Hold Time' set to 2, with a range of (2 to 600).
- Controller Hostnames:** A table with columns: Host, Pool, Routing Level, IPsec Secure, IPsec GW, Force, and a delete icon. The table is currently empty. An 'Add Row' button is located below the table.

At the bottom, there is a warning icon and text: 'Auto IPsec Tunnel parameters need to be configured when IPsec Secure is selected'. At the very bottom are 'OK' and 'Reset' buttons.

**Figure 5-127** Device Overrides - Adoption screen

7. Define a 64 character maximum **Preferred Group**.  
The preferred group is the controller group the access point would prefer to connect upon adoption.
8. Define the **Hello Interval** value for this device. This is the interval between hello keep alive messages exchanged with the wireless controller that has adopted this access point. These messages serve as a connection validation mechanism to keep the access point adopted to its wireless controller. Set a value from 1-120 seconds.
9. Define the **Adjacency Hold Time** value for this device. This is the amount of time before the preferred controller group is considered down and unavailable to provide services. Set a value from 2-600 seconds.
10. Use the spinner control to set the **Controller VLAN**.  
This is the VLAN the Virtual Controller is reachable on. Select from 1 - 4094. There is no default value for this setting.
11. Use the **+ Add Row** button to populate the **Controller Hostnames** table with the following host, pool and routing parameters for defining the preferred adoption resource.

<b>Host</b>	Use the drop-down menu to specify whether the controller adoption resource is defined as a (non DNS) IP address or a hostname. Once defined, provide the numerical IP or hostname. A hostname cannot exceed 64 characters.
<b>Pool</b>	Use the spinner controller to set a pool of either 1 or 2. This is the pool the target Virtual Controller belongs to. The default setting is 1.
<b>Routing Level</b>	Use the spinner controller to set the routing level for the Virtual Controller link. The default setting is 1.

<b>IPSec Support</b>	Select to enable secure communication between the access point and the wireless controllers.
<b>IPSec GW</b>	Use the drop-down menu to specify if the IPSec Gateway resource is defined as a (non DNS) IP address or a hostname. Once defined, provide the numerical IP or hostname. A hostname cannot exceed 64 characters.
<b>Force</b>	Select to enable the link to the adopting controller or the controller group to be created even when not required.

12. Select **OK** to save the changes and overrides made to the access point adoption configuration. Select **Reset** to revert to the last saved configuration

### 5.4.5.3 Profile Interface Override Configuration

#### ▶ *Device Overrides*

An access point requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each connected VLAN ID.

An interface configuration can have overrides applied to customize the configuration to a unique deployment objective. For more information, refer to the following:

- [Ethernet Port Override Configuration](#)
- [Virtual Interface Override Configuration](#)
- [Port Channel Override Configuration](#)
- [Radio Override Configuration](#)
- [WAN Backhaul Overrides](#)
- [PPPoE Configuration](#)

#### 5.4.5.3.1 Ethernet Port Override Configuration

##### ▶ *Profile Interface Override Configuration*

Use an Ethernet Port override to change (modify) parameters of an access point's Ethernet Port configuration.

The following ports are available on supported access point models:

- AP6511 - fe1, fe2, fe3, fe4, up1
- AP6521 - GE1/POE (LAN)
- AP6522/AP6522M - GE1/POE (LAN)
- AP6532 - GE1/POE (LAN)
- AP6562 - GE1/POE (LAN)
- AP7131 - GE1/POE (LAN), GE2 (WAN)
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7181 - GE1/POE (LAN), GE2 (WAN)
- AP8122/AP8132 - GE1/POE (LAN), GE2 (WAN)
- AP8222/AP8232 - GE1/POE (LAN), GE2 (WAN)

To define an Ethernet port configuration override:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the **Configuration** tab.
3. Select **Device Overrides**.
4. Select a target device from the device browser in the lower, left-hand, side of the UI.
5. Select **Interface** to expand its sub menu options.
6. Select **Ethernet Ports**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

---

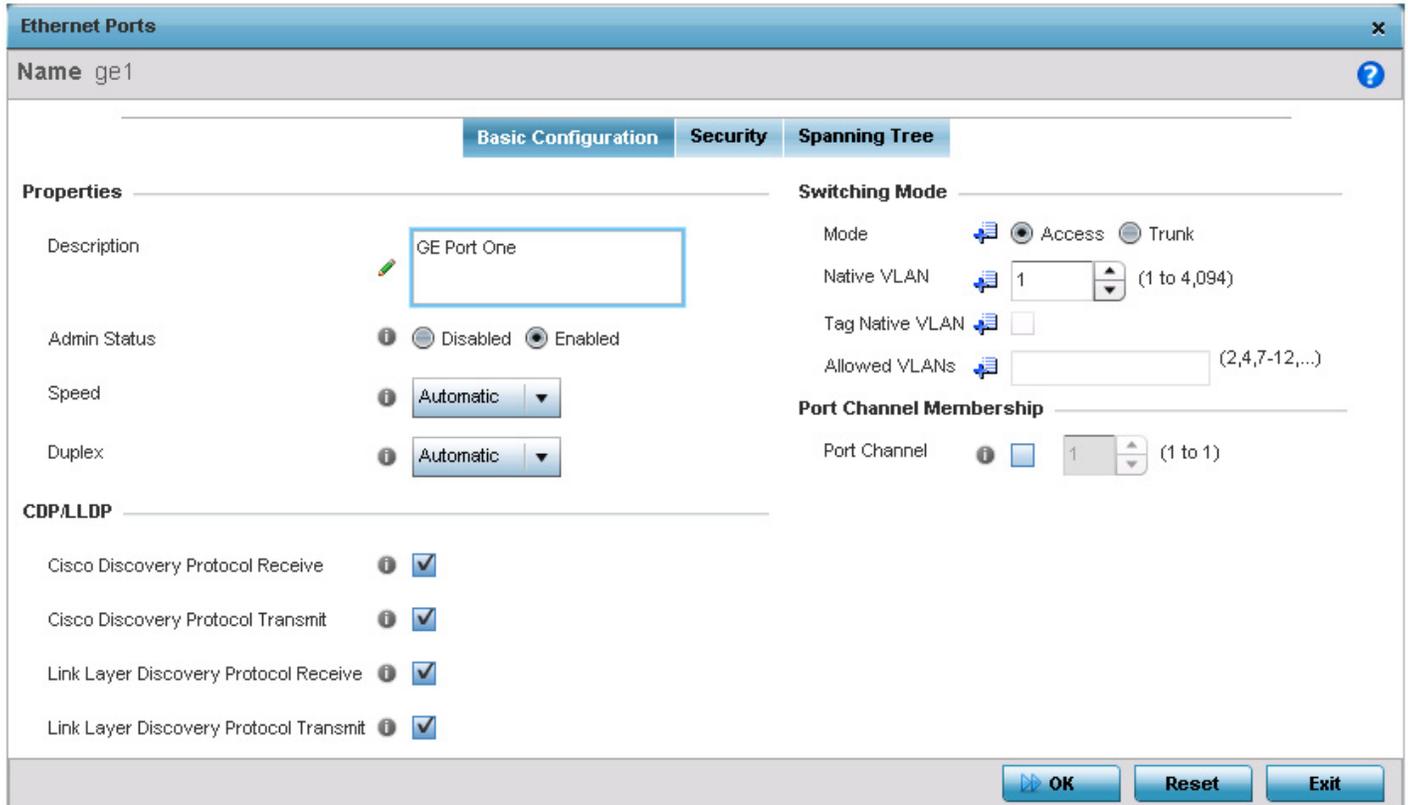


---



<b>Overrides</b>	Click <i>Clear</i> to clear overrides made to this interface. This field is blank if there are no overrides for this configuration.
------------------	---

- To edit (or override) the configuration of an existing port, select it from amongst those displayed and select the **Edit** button. The *Ethernet Port Basic Configuration* screen displays by default.



**Figure 5-129** Ethernet Ports - Basic Configuration screen

- Set (or override) the following Ethernet port Properties and CDP/LLDP settings:

<b>Description</b>	Provide a brief description for the access point's port (64 characters maximum).
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port as active to the profile it supports. Select the <i>Disabled</i> radio button to disable this physical port in the profile. It can be activated at any future time when needed.
<b>Speed</b>	Set the speed at which the port can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> , <i>1000 Mbps</i> . Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select <i>Automatic</i> to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.

<b>Duplex</b>	Select either <i>half</i> , <i>full</i> or <i>automatic</i> as the duplex option. Select Half duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port performance needs dictate. Automatic is the default setting.
<b>Cisco Discover Protocol Receive</b>	Select this option to allow the Cisco discovery protocol for receiving data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.
<b>Cisco Discover Protocol Transmit</b>	Select this option to allow the Cisco discovery protocol for transmitting data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.
<b>Link Layer Discovery Protocol Receive</b>	Select this option to allow the Link Layer discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
<b>Link Layer Discovery Protocol Transmit</b>	Select this option to allow the Link Layer discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.

10. Set (or override) the following **Switching Mode** parameters to apply to the Ethernet port configuration:

<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port. If Access is selected, the port accepts packets only from the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode.
<b>Native VLAN</b>	Use the spinner control to define a numerical Native VLAN ID from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.
<b>Tag Native VLAN</b>	Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.

**Allowed VLANs**

Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the listed port.

11. Optionally select the **Port Channel Membership** option and define (or override) a setting from 1 - 8 using the spinner control. This sets the channel group for the port.
12. Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.
13. Select the **Security** tab.

The screenshot shows the 'Ethernet Ports' configuration window for port 'ge1'. The 'Security' tab is active. The 'Access Control' section has two dropdown menus for 'IP Inbound Firewall Rules' and 'MAC Inbound Firewall Rules', both set to '<none>'. The 'Trust' section has five checkboxes: 'Trust ARP Responses' (unchecked), 'Trust DHCP Responses' (checked), 'Trust 802.1p COS values' (checked), and 'Trust IP DSCP' (checked). The '802.1X supplicant (client) feature' section has an 'Enable' checkbox (unchecked), a 'Username' text field, and a 'Password' text field with a 'Show' checkbox.

**Figure 5-130** Ethernet Ports - Security screen

14. Refer to the **Access Control** field. As part of the port's security configuration, Inbound IP and MAC address firewall rules are required. The configuration can be optionally overridden if needed.
15. Use the **IP Inbound Firewall Rules** and **MAC Inbound Firewall Rules** drop-down menus to select the firewall rules to apply to this profile's Ethernet port configuration.  
The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.
16. If a firewall rule does not exist suiting the data protection needs of the target port configuration, select the **Create** icon to define a new rule configuration. For more information, see [Wireless Firewall on page 8-2](#).
17. Refer to the **Trust** field to define the following:

**Trust ARP Responses**

Select this option to enable ARP trust on this port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled.

<b>Trust DHCP Responses</b>	Select this option to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
<b>ARP header Mismatch Validation</b>	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
<b>Trust 802.1p COS values</b>	Select this option to enable 802.1p COS values on this port. The default value is enabled.
<b>Trust IP DSCP</b>	Select this option to enable IP DSCP values on this port. The default value is enabled.



**NOTE:** Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, despite a conflict existing.

18. Refer to the **802.1X Settings** field to define the following:

<b>Host Mode</b>	Select the port mode for 802.1X authentication. Select <i>single-host</i> to bridge traffic from a single authenticated host. Select <i>multi-host</i> to bridge traffic from any host to this port.
<b>Guest VLAN</b>	Set the Guest VLAN on which traffic is bridged from a wired port when the selected port is considered unauthorized.
<b>Port Control</b>	Set how the port bridges traffic. Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Automatic</i> – The port is set to the state as received from the authentication server.</li> <li>• <i>force-authorized</i> – Any traffic on the port is considered authenticated and is bridged as configured.</li> <li>• <i>force-unauthorized</i> – Any traffic on the port is considered unauthenticated and is not bridged.</li> </ul>
<b>Re Authenticate</b>	Select to <i>enable</i> or <i>disable</i> reauthentication. Reauthentication is primarily used to refresh the current state of the selected port. When enabled the device is forced to reauthenticate. When this happens, the port is still considered authenticated. If reauthentication fails, the port is considered unauthorized and devices using the port are denied access.
<b>Max Reauthenticate Count</b>	Set the number of reauthentication attempts when a port tries to reauthenticate and fails. Once this count exceeds, the port is considered unauthorized.
<b>Maximum Request</b>	Set the number of times an attempt is made to authenticate with an EAP server before returning an 'Authentication Failed' message to the device seeking to authenticate using the controlled port.
<b>Quiet Period</b>	Set the duration in seconds where no attempt is made to reauthenticate a controlled port. Set a value from 0 - 65535 seconds.
<b>Reauthenticate Period</b>	Set the duration after which a controlled port is forced to reauthenticate. Set a value from 0 - 65535 seconds.

19. Select the **Enable** option within the **802.1x supplicant (client) feature** field to enable a username and password pair used when authenticating users on this port. Select **Show** to expose the characters comprising the password in the **Password** field.

20. Select the **Spanning Tree** tab.

**Figure 5-131** Ethernet Ports – Spanning Tree Configuration

*Spanning Tree Protocol* (STP) (IEEE 802.1D standard) configures a meshed network for robustness by eliminating loops within the network and calculating and storing alternate paths to provide fault tolerance.

STP calculation happens when a port comes up. As the port comes up and STP calculation happens, the port is set to Blocked state. In this state, no traffic can pass through the port. Since STP calculations take up to a minute to complete, the port is not operational thereby affecting the network behind the port. Once the STP calculation is complete, the port's state is changed to Forwarding and traffic is allowed.

*Rapid Spanning Tree Protocol* (RSTP) (IEEE 802.1w standard) is an evolution over the standard STP where the primary aim was to reduce the time taken to respond to topology changes while being backward compatible with STP. PortFast enables quickly changing the state of a port from Blocked to Forwarding to enable the port to allow traffic while the STP calculation happens.

*Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there is just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI

messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

21. Select the **Enable as Edge Port** option to enable or disable the port as an edge port. An edge port is a port that is known to connect to a LAN which has no other bridges connected or is directly connected to a user device.
22. Select either the **Point-to-Point** or **Shared** radio button for the **Link Type** field. When Point-to-Point is selected, it indicates that the port should be treated as connected to a point-to-point link. Selecting Shared indicates that the port is shared between multiple devices. An example for Shared connection would be when the port is connected to a hub. Similarly, an example for a Point-to-Point connection would be when the port is connected to an access point.
23. Select either the **Enable** or **Disable** radio button for the **CISCO MSTP Interoperability** field. This enables or disables interoperability with CISCO's implementation of the *Multiple Spanning Tree Protocol* (MSTP) which is incompatible with the standard MSTP implementation.
24. Select one of the available choices for **Force Protocol Version** field. Select *STP* to use the standard Spanning Tree Protocol. Select *RSTP* to use Rapid Spanning Tree Protocol. Select *MSTP* to use Multiple Spanning Tree Protocol.  
Select **Not Supported** to disable spanning tree protocol for this interface.
25. Select either the **None** or **Root** radio button for the **Guard field**. Root guard is a mechanism to prevent election of roots other than those designated as roots in a network. When this port receives a better (superior) BPDU, the port state becomes Blocked. It retains this state till the port no longer receives the better (superior) BPDU and then the state is changed to Forwarding. Select *Root* to enable this feature. Select *None* to disable.
26. Select the **Enable Port Fast** option to enable or disable PortFast. PortFast enables reducing the time taken for a port to complete the MSTP state changes from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller which are directly connected to a Server/Workstation and not to another hub or controller. PortFast can be left unconfigured on an access point.
27. Set the **Enable PortFast BPDU Filter** value from the drop-down list. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports do not transmit BPDU messages. When set to 'Default' sets the PortFast BPDU Filter value to the bridge's BPDU filter value.
28. Set the **Enable PortFast BPDU Guard** value from the drop-down list. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports are forced to shut down when they receive BPDU messages. When set to 'Default' sets the PortFast BPDU Guard value to the bridge's BPDU guard value.
29. Configure the **Spanning Tree Port Cost** value. Select the **+ Add Row** button to add a row to the table. Configure an **Instance Index** value and its corresponding cost in the **Cost** column. This is the cost for a packet to traverse the current network segment. The cost of a path is the sum of all costs of traversal from the source to the destination. The default rule for the cost of a network segment is, the faster the media, the lower the cost.
30. Configure the **Spanning Tree Port Priority** value. Select the **+ Add Row** to add a row to the table. Configure an **Instance Index** value and its corresponding priority in the **Priority** column. This is the priority for this port becoming a designated root. The default rule is, the lower this value, the higher the chance that the port is assigned as a designated root.
31. Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration if you do not wish to commit the overrides.

### 5.4.5.3.2 Virtual Interface Override Configuration

#### ▶ [Profile Interface Override Configuration](#)

A *Virtual Interface* is required for layer 3 (IP) access or provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each VLAN ID. A Virtual Interface is created for the default VLAN (VLAN 1) to enable remote





11. Define or override the following parameters from within the Properties field:

<b>Description</b>	Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Either select the <i>Disabled</i> or <i>Enabled</i> radio button to define this interface's current status within the network. When set to Enabled, the Virtual Interface is operational and available. The default value is disabled.

12. Set or override the following network information from within the IP Addresses field:

<b>Enable Zero Configuration</b>	Zero Configuration (or Zero Config) is a wireless connection utility included with Microsoft Windows XP and later as a service that dynamically selects a network to connect based on a user's preference and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device.  The access point can use Zero Config for IP assignments on an individual virtual interface basis. Select <i>Primary</i> to use Zero Config as the designated means of providing an IP address, this eliminates the means to assign one manually. Selecting <i>Secondary</i> is preferred when wanting the option to either use Zero Config or manual assignments. Selecting <i>None</i> disables using Zero Config for IP assignments. None is the default setting.
<b>Primary IP Address</b>	Define the IP address for the VLAN associated Virtual Interface.
<b>Use DHCP to Obtain IP</b>	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
<b>Use DHCP to obtain Gateway/DNS Servers</b>	Select this option to allow DHCP to obtain a default gateway address, and DNS resource for one virtual interface. This setting is disabled by default and only available when the <i>Use DHCP to Obtain IP</i> option is selected.
<b>Secondary Addresses</b>	Use the <i>Secondary Addresses</i> parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

13. Define or override the **Network Address Translation** (NAT) direction.

Select either the *Inside*, *Outside* or *None* radio buttons.

- *Inside* - The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
- *Outside* - Packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. There the destination IP address is changed back to the specific private class IP address in order to reach the LAN over the switch managed network.
- *None* - No NAT activity takes place. This is the default setting.



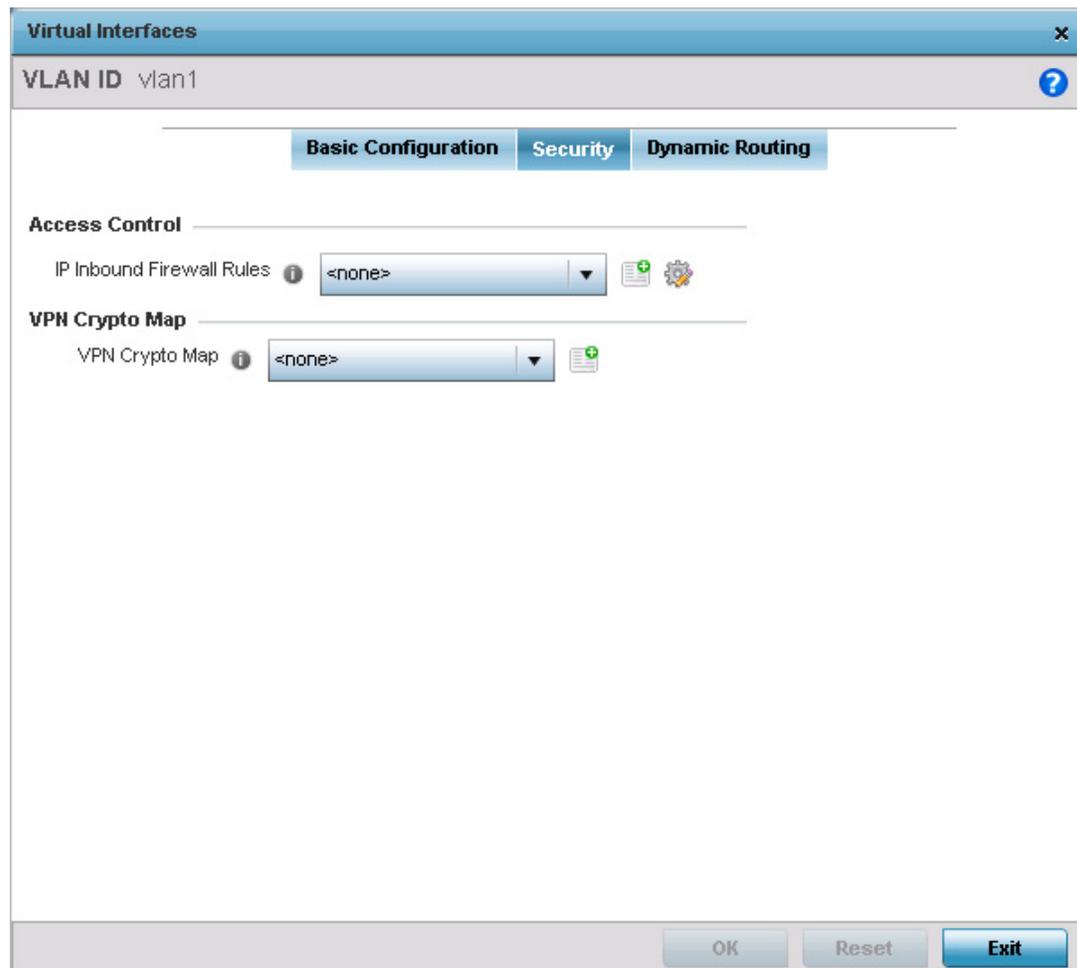
**NOTE:** Refer to [Setting the Profile's NAT Configuration on page 5-123](#) for instructions on creating a profile's NAT configuration.

14. Select **OK** button to save the changes and overrides to the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.

15. Select the **Security** tab.

The firewall inspects and packet traffic to and from connected clients.

If a firewall rule does not exist suiting the data protection needs of this Virtual Interface, select the **Create** icon to define a new firewall rule configuration or the **Edit** icon to modify or override an existing configuration. For more information, see [Wireless Firewall on page 8-2](#).



**Figure 5-134** Device Overrides - Virtual Interfaces Security screen

16. Use the **IP Inbound Firewall Rules** drop-down menu to select the firewall rule configuration to apply to this Virtual Interface.
17. Use the **VPN Crypto Map** drop-down menu to define the cryptography map to use with this virtual interface. The VPN Crypto Map entry defines the type of VPN connection and its parameters. For more information see [Defining Profile VPN Settings on page 5-104](#).
18. Select the **Dynamic Routing** tab.

**Figure 5-135** Device Overrides – Virtual Interfaces Dynamic Routing screen

19. Refer to the following to configure **OSPF Settings**.

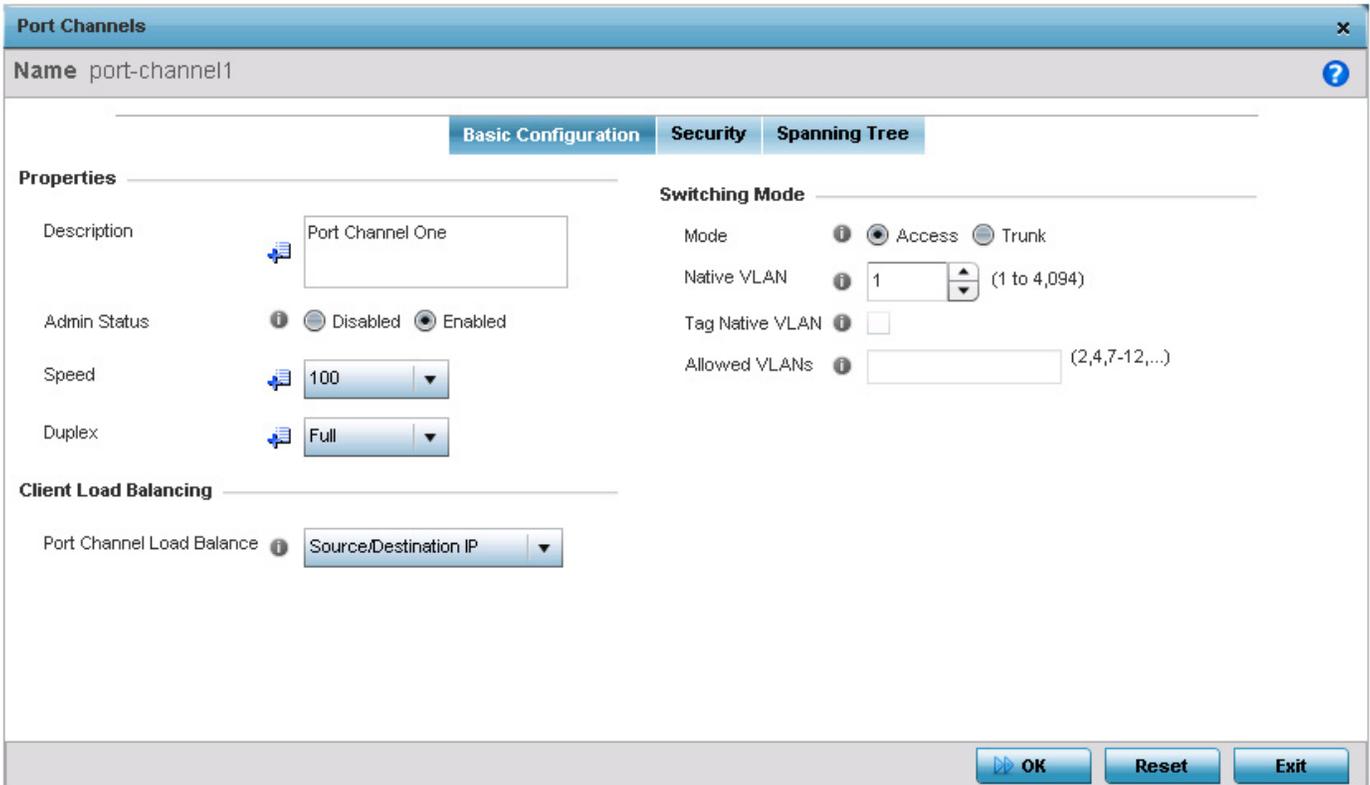
<b>Priority</b>	Select this option to enable or disable OSPF priority settings. Use the spinner to configure a value from 0 - 255. This option sets the priority of this interface becoming the <i>Designated Router</i> (DR) for the network. DRs provide routing updates to the network by maintaining a complete topology table of the network and sends the updates to the other routers in the network using multicast. Setting a high value increases the chance of this interface becoming a DR. Setting this value to Zero (0) prevents this interface from being elected a DR.
<b>Cost</b>	Select this option to enable or disable OSPF cost settings. Use the spinner to configure a cost value from 1 - 65535. Use this option to set the OSPF cost of this interface. OSPF cost is the overhead required to send a packet over this interface.
<b>Bandwidth</b>	Select this option to enable or disable OSPF bandwidth settings. Use the spinner to configure a bandwidth settings from 1 - 10,000,000 KBps. Use this option to set the bandwidth of this interface in KBps.

20. Configure the **OSPF Authentication Type** settings by selecting from the drop-down list. The available options are *None*, *null*, *simple-password* and *message-digest*.



<b>Admin Status</b>	A green check mark defines the listed port channel as active and currently enabled with the access point's profile. A red "X" defines the port channel as currently disabled and not available for use. The interface status can be modified with the port channel configuration as required
---------------------	--

- To edit the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. The Port Channel **Basic Configuration** screen displays by default.



**Figure 5-137** Device Overrides - Port Channels - Basic Configuration tab

- Set the following port channel **Properties**:

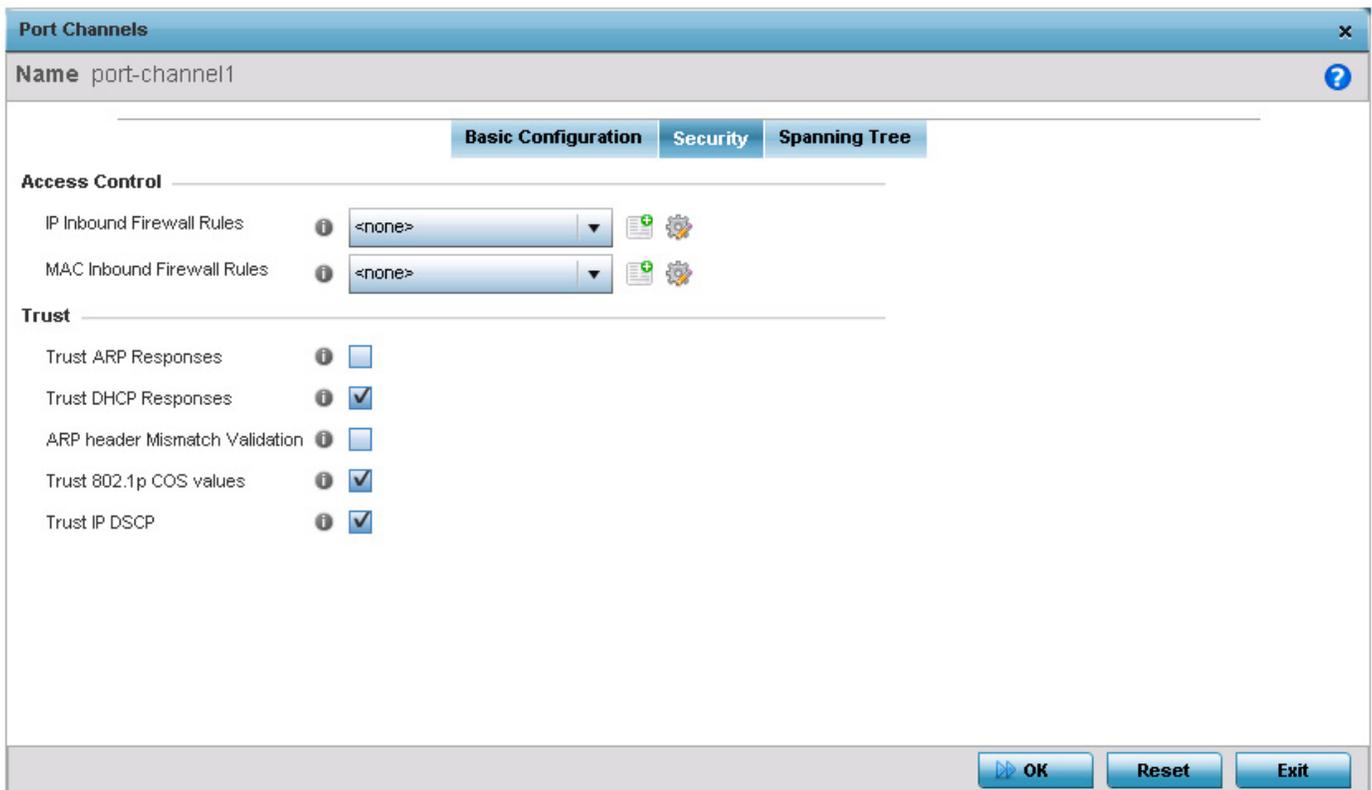
<b>Description</b>	Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port channel as active to the profile it supports. Select the <i>Disabled</i> radio button to disable this port channel configuration within the profile. It can be activated at any future time when needed. The default setting is disabled.
<b>Speed</b>	Select the speed at which the port channel can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> , <i>1000 Mbps</i> . Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select Automatic to enable the port channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.

<b>Duplex</b>	Select either <i>Half</i> , <i>Full</i> or <i>Automatic</i> as the duplex option. Select <i>Half</i> duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a Full duplex transmission, a Half duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port channel at the same time. Using Full duplex, the port channel can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.
---------------	---

9. Use the **Port Channel Load Balance** drop-down menu within the **Client Load Balancing** field to define whether port channel load balancing is conducted using a *Source/Destination IP* or a *Source/Destination MAC* as criteria. *Source/Destination IP* is the default setting.
10. Define the following **Switching Mode** parameters to apply to the port channel configuration:

<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port channel. If <i>Access</i> is selected, the port channel accepts packets only from the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to <i>Trunk</i> , the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. <i>Access</i> is the default setting.
<b>Native VLAN</b>	Use the spinner control to define a numerical ID from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using trunk mode. The default value is 1.
<b>Tag the Native VLAN</b>	Select this option to tag the native VLAN. Access points support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
<b>Allowed VLANs</b>	Selecting <i>Trunk</i> as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the port channel.

11. Select **OK** to save the changes made to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.
12. Select the **Security** tab.



**Figure 5-138** Device Overrides - Port Channels - Security tab

13. Refer to the **Access Control** field. As part of the port channel's security configuration, Inbound IP and MAC address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **Inbound MAC Firewall Rules** drop-down menus to select firewall rules to apply to this profile's port channel configuration.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

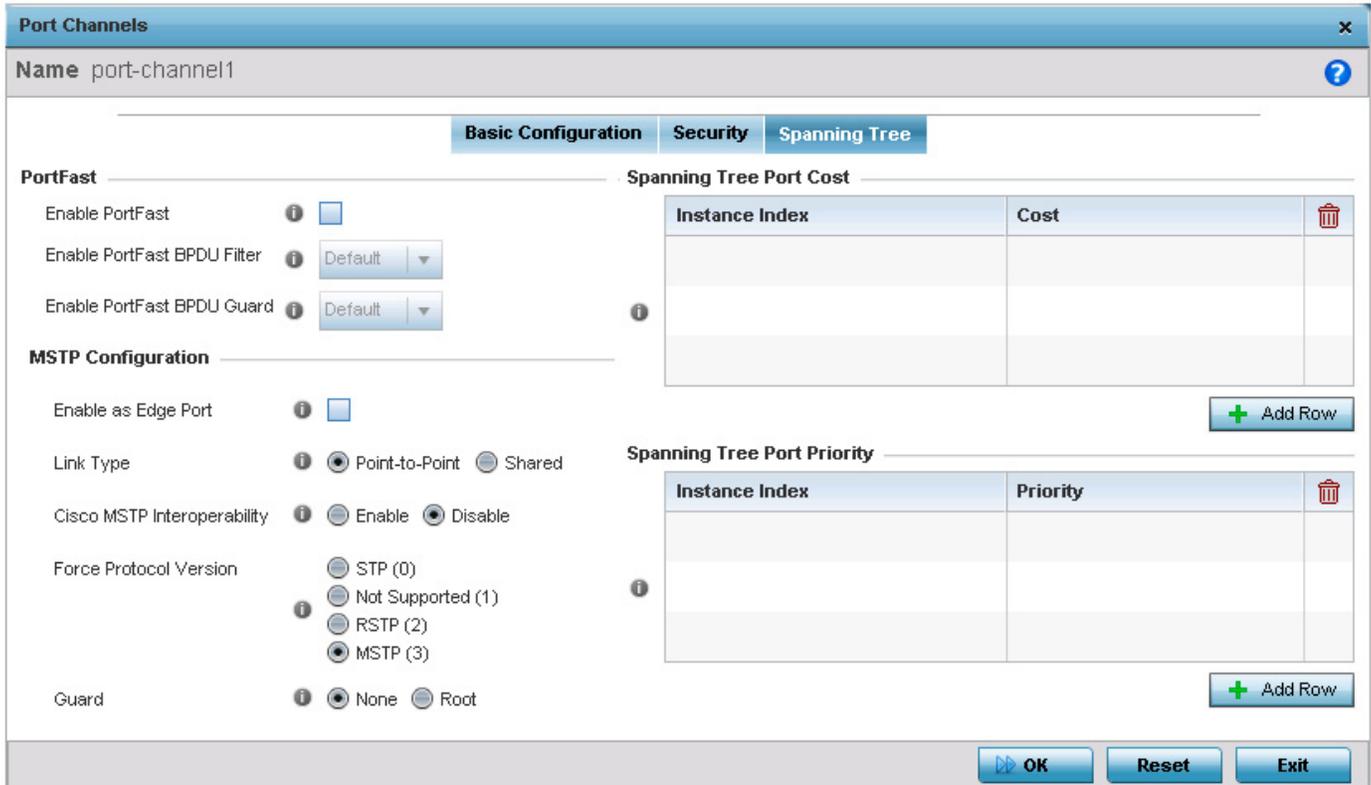
If a firewall rule does not exist suiting the data protection needs of the target port channel configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing firewall rule configuration. For more information, see [Wireless Firewall on page 8-2](#).

14. Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	Select this option to enable ARP trust on this port channel. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the managed network. The default value is disabled.
<b>Trust DHCP Responses</b>	Select this option to enable DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
<b>ARP header Mismatch Validation</b>	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
<b>Trust 802.1p COS values</b>	Select this option to enable 802.1p COS values on this port channel. The default value is enabled.

<b>Trust IP DSCP</b>	Select this option to enable IP DSCP values on this port channel. The default value is enabled.
----------------------	---

15. Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.
16. Select the **Spanning Tree** tab.



**Figure 5-139** Port Channels - Spanning Tree tab

17. Define the following **PortFast** parameters for the port channel's MSTP configuration:

<b>Enable PortFast</b>	PortFast reduces the time required for a port to complete a MSTP state change from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller directly connected to a server/workstation and not another hub or controller. PortFast can be left unconfigured on an access point. Select this option to enable drop-down menus for both the <i>Enable PortFast BPDU Filter</i> and <i>Enable PortFast BPDU Guard</i> options. This setting is disabled by default.
<b>Enable PortFast BPDU Filter</b>	Select <i>Enable</i> to invoke a BPDU filter for this PortFast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. The default setting is None.
<b>Enable PortFast BPDU Guard</b>	Select <i>Enable</i> to invoke a BPDU guard for this PortFast enabled port channel. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. The default setting is None.

18. Set the following **MSTP Configuration** parameters for the port channel:

<b>Enable as Edge Port</b>	Select this option to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port channel. This setting is disabled by default.
<b>Link Type</b>	Select either the <i>Point-to-Point</i> or <i>Shared</i> radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point is a point-to-point link. Point-to-Point is the default setting.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
<b>Force Protocol Version</b>	Sets the protocol version to either <i>STP(0)</i> , <i>Not Supported(1)</i> , <i>RSTP(2)</i> or <i>MSTP(3)</i> . MSTP is the default setting.
<b>Guard</b>	Determines whether the port channel enforces root bridge placement. Setting the guard to <i>Root</i> ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.

19. Refer to the **Spanning Tree Port Cost** table.

Define an Instance Index using the spinner control and then set the cost. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

<b>Speed</b>	<b>Default Path Cost</b>
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000
<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

20. Select **+ Add Row** as needed to include additional indexes.

21. Refer to the **Spanning Tree Port Priority** table.

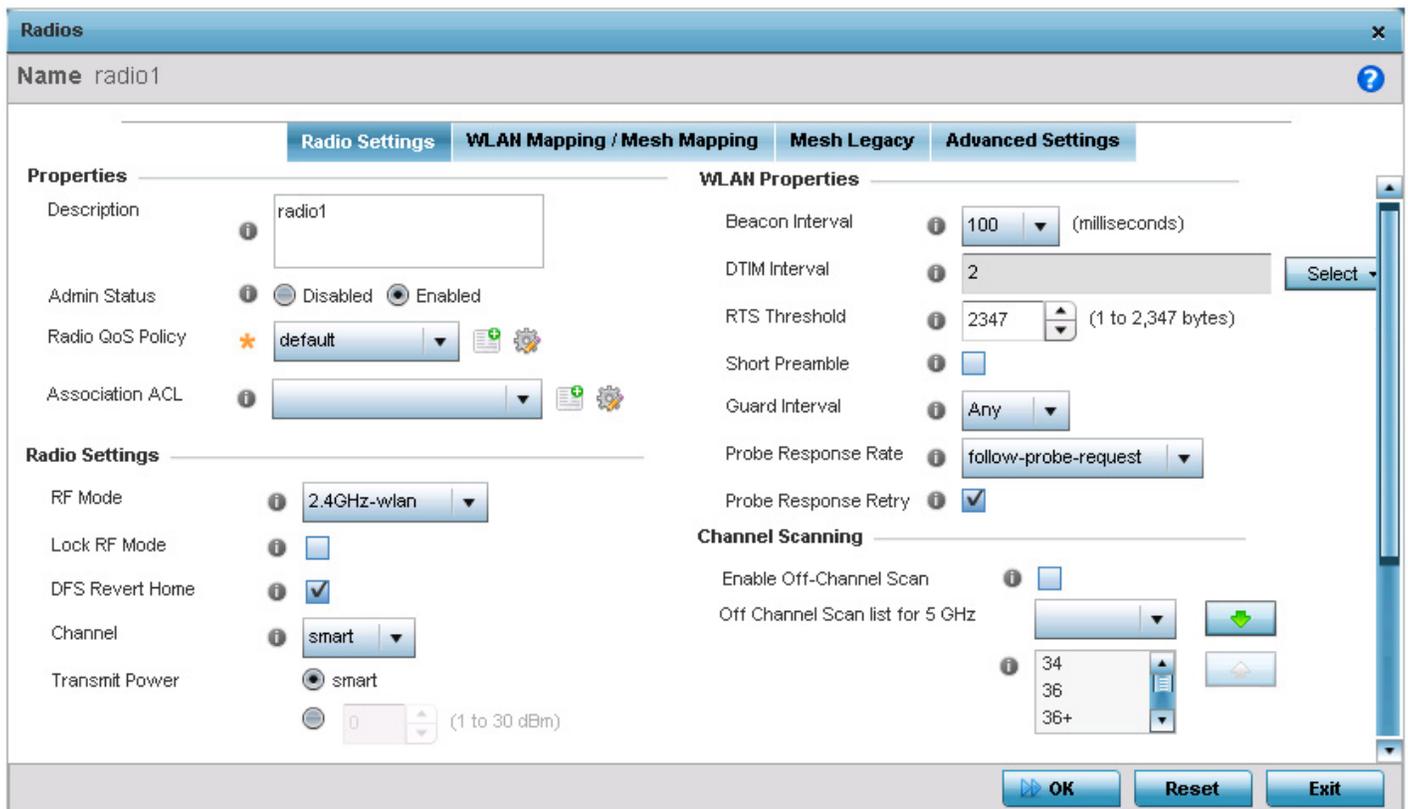
Define an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, a greater likelihood of the port becoming a designated port.



7. Review the following radio configuration data to determine whether a radio configuration requires modification or override:

<b>Name</b>	Displays whether the reporting radio is the access point's radio1, radio2 or radio3. AP7131 models can support up to 3 radios. AP6522, AP6522M, AP6532, AP6562, AP7161, AP7181, AP81XX and AP82XX models support 2 radios and AP6511 and AP6521 models support a single radio.
<b>Type</b>	Displays the type as either <i>Radio</i> (for typical client support) or <i>sensor</i> . If setting an AP6511 or AP6521 model access point to function as a sensor, the access point must be rebooted before it can begin to operate as a sensor.
<b>Description</b>	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
<b>Admin Status</b>	Defines the radio as either enabled or disabled for client or sensor support.
<b>RF Mode</b>	Displays whether each listed radio is operating in the 802.11a/n or 802.11b/g/n radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client bridge, it will be listed as a client bridge and does not provide typical WLAN support. The radio band is set from within the <i>Radio Settings</i> tab.
<b>Channel</b>	Lists the channel setting for the radio. <i>Smart</i> is the default setting. If set to <i>smart</i> , the access point scans non-overlapping channels listening for beacons from other access points. After the channels are scanned, it selects the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level.
<b>Transmit Power</b>	Lists the transmit power for each radio.
<b>Overrides</b>	Click <i>Clear</i> to clear overrides made to this radio interface. This field is blank if there are no overrides for this radio.

8. If required, select a radio configuration and select the **Edit** button to modify or override portions of its configuration.



**Figure 5-141** Device Overrides - Access Point Radio Settings tab

9. The **Radio Settings** tab displays by default.
10. Define or override the following radio configuration **Properties**:

<b>Description</b>	Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Either select the <i>Active</i> or <i>Shutdown</i> radio button to define this radio's availability. When defined as Active, the access point is operational and available for client support, Shutdown renders it unavailable.
<b>Radio QoS Policy</b>	Use the drop-down menu to specify an existing QoS policy to apply to the access point radio in respect to its intended radio traffic. If there's no existing QoS policy suiting the radio's intended operation, select the <i>Create</i> icon.
<b>Association ACL</b>	Use the drop-down menu to specify an existing Association ACL policy to apply to the radio. An Association ACL is a policy-based <i>Access Control List</i> (ACL) that either prevents or allows wireless clients from connecting to an access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the fields in the packet are compared to applied ACLs to verify the packet has the required permissions needed to be forwarded. If a packet does not meet any of the ACL criteria, the packet is dropped. Select the <i>Create</i> icon to define a new Association ACL.

11. Set or override the following profile **Radio Settings** for the selected radio:

<b>RF Mode</b>	Set the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio's intended client support. Set the mode to <i>sensor</i> if using the radio for rogue device detection. Set the mode to <i>client-bridge</i> to configure the radio as a client bridge. A client bridge enables the access point to connect to a 3rd party access point and bridge frames to it.
<b>Lock RF Mode</b>	Select this option to lock Smart RF calibration functions for this radio. The default setting is disabled.
<b>Channel</b>	Use the drop-down menu to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select <i>Smart</i> for the radio to scan non-overlapping channels to listen for beacons from other access points. Once channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it will select the channel with the lowest average power level. The default value is Smart.  Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, only appear when using an AP8232, and are unique to the 80 MHz band.
<b>DFS Revert Home</b>	Select this option to enable a radio to return back to its original channel. <i>Dynamic Frequency Selection</i> (DFS) prevents a radio from operating in a channel where radar signals are present. When radar signals are detected in a channel, the radio changes its channel of operation to another channel. The radio cannot use the channel it has moved from for the next thirty (30) minutes. When selected, the radio can return back to its original channel of operation once the thirty minute period is over. When not selected, the radio cannot return back to its original channel of operation ever after the mandatory thirty minute evacuation period is over.
<b>Transmit Power</b>	Set the transmit power of the selected access point radio. If using a dual or a three radio model AP7131, each radio should be configured with a unique transmit power in respect to its intended client support function. Select <i>smart</i> to use Smart RF to determine output power. <i>smart</i> is the default value.
<b>Antenna Gain</b>	Set the antenna from 0.00 - 30.00 dBm. The access point's <i>Power Management Antenna Configuration File</i> (PMACF) automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Motorola Solutions recommends only a professional installer set the antenna gain. The default value is 0.00.
<b>Antenna Mode</b>	Set the number of transmit and receive antennas on the access point. 1x1 is used for transmissions over just a single "A" antenna, 1x3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. The default setting is dynamic based on the access point model deployed and its transmit power settings.

<b>Enable Antenna Diversity</b>	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.
<b>Wireless Client Power</b>	Select this option to enable a spinner control for client radio power transmissions in dBm. The available range is 0 - 20 dBm.
<b>Dynamic Chain Selection</b>	Select this option to allow the access point radio to dynamically change the number of transmit chains. This setting is disabled by default. The radio uses a single chain/antenna for frames at non 802.11n data rates.
<b>Data Rate</b>	Once the radio band is provided, the <i>Rate</i> drop-down menu populates with rate options depending on the 2.4 or 5.0 GHz band selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates define how they are used together. When using 802.11n (in either the 2.4 or 5.0 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). For more information on 802.11n MCS rates, see <a href="#">MCS Data Rates on page 5-51</a> .
<b>Radio Placement</b>	Use the drop-down menu to specify whether the radio is located Indoors or Outdoors. The placement should depend on the selected country of operation and its regulatory domain requirements for radio emissions. The default setting is Indoors.
<b>Max Clients</b>	Use the spinner control to set the maximum permissible client connections for this radio. Set a value from 0 - 256. AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 clients per access point or radio. AP6511 and AP6521 model access points can support up to 128 clients per access point or radio.
<b>Rate Selection Methods</b>	Use the drop-down menu to specify the algorithm to use for rate selection. Select <i>Standard</i> to use the standard rate selection algorithm. Select <i>Opportunistic</i> to use the Opportunistic rate selection algorithm.



**NOTE:** AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 client connections to a single access point radio. AP6511 and AP6521 model access points (both single radio models) can support up to 128 client connections to a single radio.

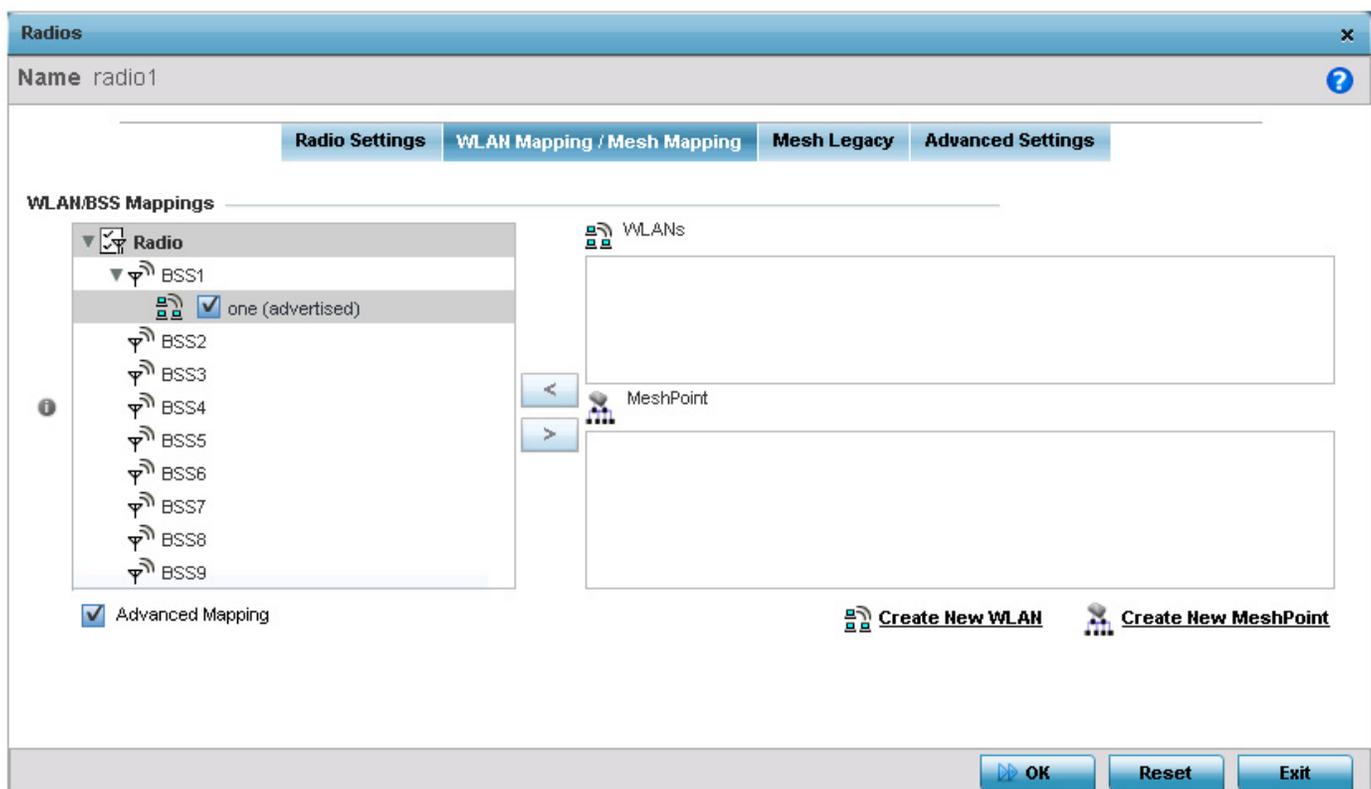
12. Set or override the following profile WLAN Properties for the selected access point radio.

<b>Beacon Interval</b>	Set the interval between radio beacons in milliseconds (either <i>50</i> , <i>100</i> or <i>200</i> ). A beacon is a packet broadcast by adopted radios to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds.
<b>DTIM Interval</b>	Set a DTIM Interval to specify a period for <i>Delivery Traffic Indication Messages</i> (DTIM). A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM indicates broadcast and multicast frames (buffered at the access point) are soon to arrive. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.
<b>RTS Threshold</b>	<p>Specify a <i>Request To Send</i> (RTS) threshold (from 1 - 2,347 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a <i>Clear To Send</i> (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.</p> <p>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.</p> <p>Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.</p>
<b>Short Preamble</b>	If using an 802.11bg radio, select this option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. The default value is disabled.

<b>Guard Interval</b>	Use the drop-down menu to specify a <i>Long</i> or <i>Any</i> guard interval. The guard interval is the space between symbols (characters) being transmitted. The guard interval eliminates <i>inter-symbol interference</i> (ISI). ISI occurs when echoes or reflections from one symbol interfere with another symbol. Adding time between transmissions allows echo's and reflections to settle before the next symbol is transmitted. A shorter guard interval results in a shorter symbol times which reduces overhead and increases data rates by up to 10%.The default value is Long.
<b>Probe Response Rate</b>	Use the drop-down menu to specify the data transmission rate used for the transmission of probe responses. Options include, <i>highest-basic</i> , <i>lowest-basic</i> and <i>follow-probe-request</i> (default setting).
<b>Probe Response Retry</b>	Select this option to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

13. Use the **Feed WLAN Packets to Sensor** drop-down menu to allow the radio to send WLAN packet to the sensor radio. Options include Off, Inline and Promiscuous. The default setting is off.

14. Select the **WLAN Mapping/Mesh Mapping** tab.



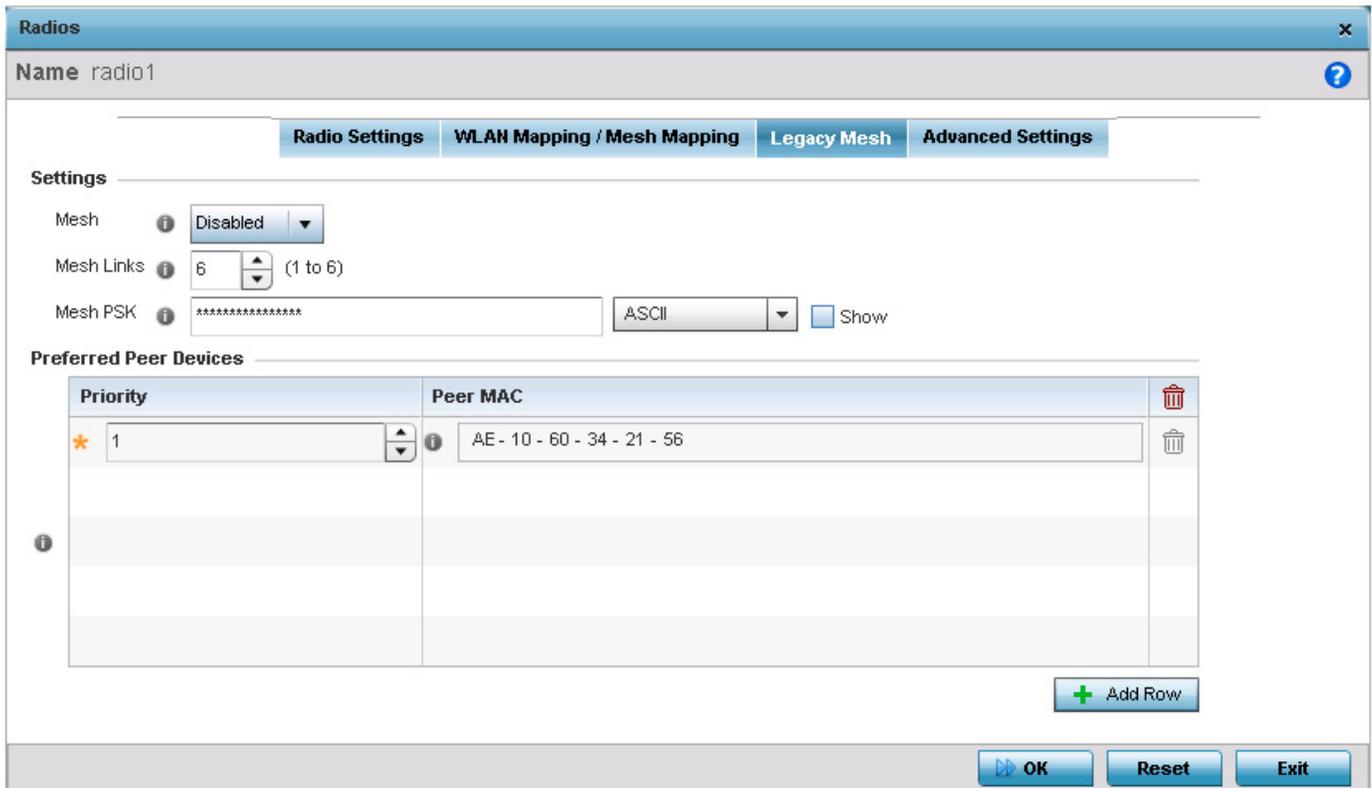
**Figure 5-142** Device Overrides - WLAN Mapping tab

Refer to the **WLAN/BSS Mappings** field to set or override WLAN BSSID assignments for an existing access point deployment. Use the '*<*' or '*>*' buttons to assign WLANs and mesh points to the available BSSIDs.

Administrators can assign each WLAN its own BSSID. If using a single-radio AP6511 or AP6521 access point, there are 8 BSSIDs available. If using a dual-radio AP6532, AP6522, AP6522M, AP6562, AP71XX, AP75XX, AP81XX or AP82XX model access point, there are 16 BSSIDs for the 802.11b/g/n radio and 16 BSSIDs for the 802.11a/n/c radio.

15. Select **OK** to save the changes and overrides to the WLAN Mapping. Select Reset to revert to the last saved configuration.

16. Select the **Legacy Mesh** tab.



**Figure 5-143** Device Overrides - Access Point Radio - Mesh tab

17. Use the **Mesh Legacy** screen to define or override how mesh connections are established and the number of links available amongst access points within the Mesh network.
18. Define the following **Mesh Legacy** settings:

<b>Mesh</b>	Options include <i>Client</i> , <i>Portal</i> and <i>Disabled</i> . Select <i>Client</i> to scan for mesh portals, or nodes that have connection to portals, and connect through them. <i>Portal</i> operation begins beaconing immediately and accepts connections from other mesh supported nodes. In general, the portal is connected to the wired network. The default value is <i>Disabled</i> .
<b>Mesh Links</b>	Use the spinner control to define the number of mesh links (1 -6) an access point radio will attempt to create. The default settings is 3 links.
<b>Mesh PSK</b>	Use the field to define the shared key for mesh. From the drop-down, select the type of the key. Click <i>Show</i> to display the actual characters comprising the key.

19. Refer to the **Preferred Peer Devices** table and select **+ Add Row** to define MAC addresses representing peer devices for preferred mesh connection. Use the Priority spinner control to set a priority (1 -6) for connection preference.
20. Select the **OK** button located at the bottom right of the screen to save the changes to the Mesh configuration. Select **Reset** to revert to the last saved configuration.
21. Select the **Advanced Settings** tab.

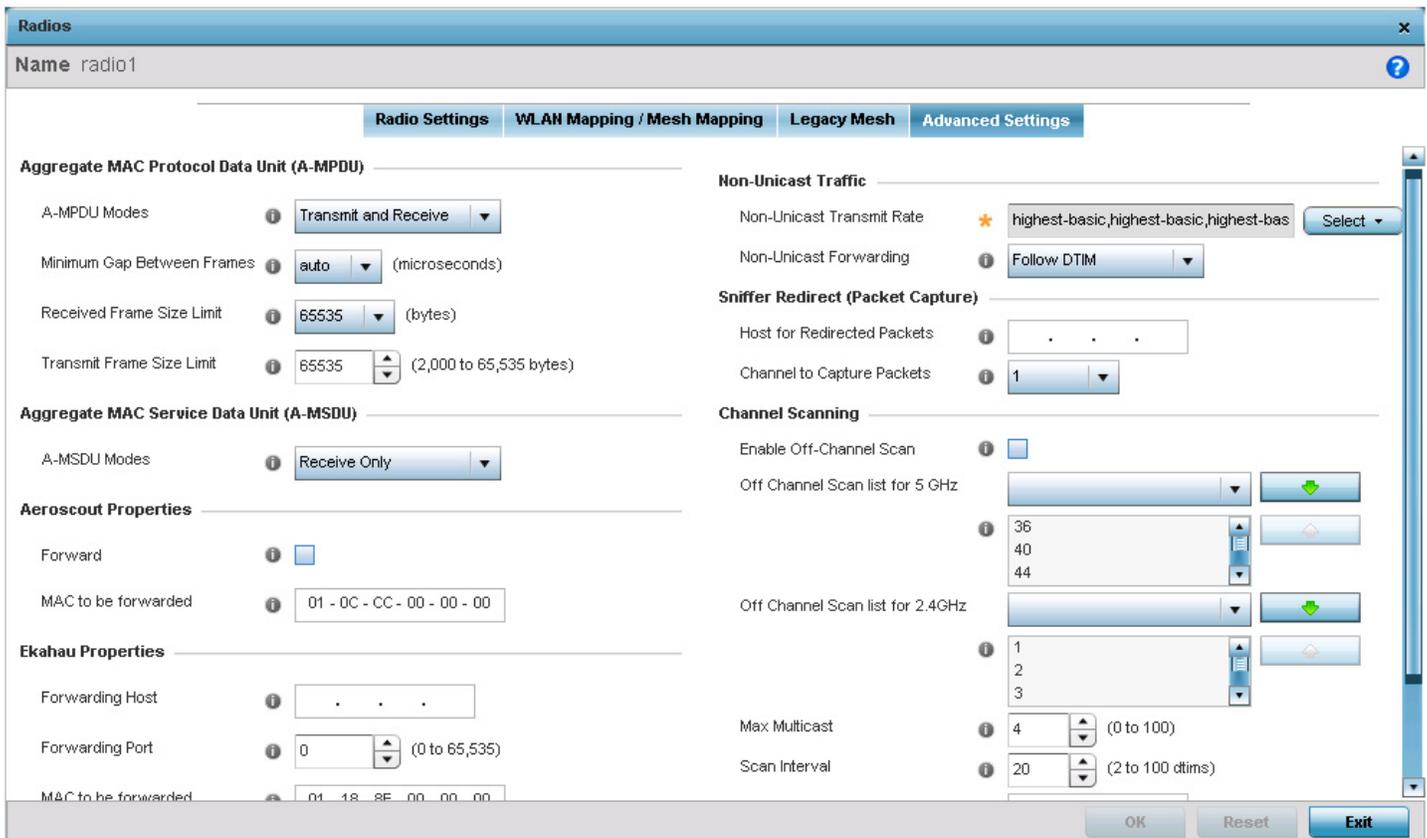


Figure 5-144 Device Overrides - Access Point Radio Advanced Settings tab

- Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** field to define or override how MAC service frames are aggregated by the access point radio.

<b>A-MPDU Modes</b>	Use the drop-down menu to define the A-MPDU mode. Options include <i>Transmit Only</i> , <i>Receive Only</i> , <i>Transmit and Receive</i> and <i>None</i> . The default value is <i>Transmit and Receive</i> . Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit (or both).
<b>Minimum Gap Between Frames</b>	Use the drop-down menu to define the minimum gap between A-MPDU frames (in microseconds). The default value is 4 microseconds.
<b>Received Frame Size Limit</b>	If a support mode is enable allowing A-MPDU frames to be received, define an advertised maximum limit for received A-MPDU aggregated frames. Options include 8191, 16383, 32767 or 65535 bytes. The default value is 65535 bytes.
<b>Transmit Frame Size Limit</b>	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is from 0 - 65,535 bytes). The default value is 65535 bytes.

- Use the **Aggregate MAC Service Data Unit (A-MSDU)** drop-down menu to set or override the supported A-MSDU mode. Available modes include *Receive Only* and *Transmit and Receive*. Using *Transmit and Receive*, frames up to 4 KB can be sent and received. The buffer limit is not configurable.

- Set or override the following profile **Aeroscout** Properties for the selected access point radio.

<b>Forward</b>	Select to enable forwarding of Aeroscout packets
<b>MAC to be forwarded</b>	Enter the MAC address that is incorporated in the Aeroscout packets that are forwarded.

25. Set or override the following profile **Ekahau Properties** for the selected access point radio.

<b>Forwarding host</b>	Provide the IP address of the host to which Ekahau packets are forwarded to.
<b>Forwarding Port</b>	Use the spinner to provide the Ekahau forwarding port number.
<b>MAC to be forwarded</b>	Enter the MAC address that is incorporated in the Ekahau packets that are forwarded.

26. Define a *Reduced Interframe Spacing* (RIFS) mode using the drop-down menu. This value determines whether interframe spacing is applied to transmissions or received packets, or both or none. The default mode is Transmit and Receive. Consider setting this value to *None* for high priority traffic to reduce packet delay.
27. Set or override the following **Non-Unicast Traffic** values for the profile's supported access point radio and its connected wireless clients:

<b>Non-Unicast Transmit Rate</b>	Use the <i>Select</i> drop-down menu to launch a sub screen to define the data rate broadcast and multicast frames are transmitted. Seven different rates are available if the not using the same rate for each BSSID, each with a separate menu.
<b>Non-Unicast Forwarding</b>	Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is Follow DTIM.

28. Refer to the **Sniffer Redirect (Packet Capture)** field to define or override the radio's captured packet configuration.

<b>Host for Redirected Packets</b>	If packets are re-directed from a access point radio, define an IP address of a resource (additional host system) used to capture the re- directed packets. This address is the numerical (non DNS) address of the host used to capture the re-directed packets.
<b>Channel to Capture Packets</b>	Use the drop-down menu to specify the channel used to capture re-directed packets. The default value is channel 1.

29. Select the **Enable Off-Channel Scan** radio button to scan across other channels in the radio band. This setting is disabled by default.
30. Select the **Off-Channel Scan list for 5GHz** field and enter the channels on which off channel scan has to be performed for the 5.0 GHz radio. Similarly select the channels for the **Off Channel Scan list for 2.4 GHz** radio.
31. Use the **Max Multicast** spinner to set the maximum number of multicast channels on which to do off channel scan.
32. Use the **Scan Interval** spinner to set the time duration in DTIM period between 2 off channel scans.
33. Use the **Sniffer Redirect** field to provide the IP address of the device to which the captured off-channel scan packets are redirected to.
34. Select **OK** to save or override the changes to the Advanced Settings screen. Select **Reset** to revert to the last saved configuration.

### 5.4.5.3.5 WAN Backhaul Overrides

#### ▶ *Device Overrides*

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a Cellular Wide Area Network. Certain AP7131N model access points have a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses *Point to Point Protocol* (PPP) to connect to the Internet Service Provider (ISP) and gain access to the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol used on various physical media,

including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation. For a list of supported 3G cards, see [WAN Backhaul Configuration on page 5-53](#).

To define a WAN Backhaul configuration override for a supported access point:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the **Device** menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Interface** to expand its submenu items.
5. Select **WAN Backhaul**.

**WAN (3G) Backhaul**

WAN Interface Name wwan1

Enable WAN (3G)  Disabled  Enabled Reset WAN Card

**Basic Settings**

Username

Password  Show

Access Point Name (APN)

Authentication Type CHAP

**Network Address Translation (NAT)**

NAT Direction  Inside  Outside  None

**Security Settings**

IP Inbound Firewall Rules  + ⚙

VPN Crypto Map  + ⚙

**Default Route Priority**

WWAN Default Route Priority  (1 to 8,000)

OK Reset Exit

**Figure 5-145** Device Overrides - WAN Backhaul screen



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

6. Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	
	Displays the WAN Interface name for the WAN 3G Backhaul card.

<b>Reset WAN Card</b>	If the WAN card becomes unresponsive or is experiencing other errors click the <i>Reset WAN Card</i> button to power cycle and reboot the WAN card.
<b>Enable WAN (3G)</b>	Select this option to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work.

7. Define or override the following authentication parameters from within the **Basic Settings** field:

<b>Username</b>	Provide your username for authentication support by your cellular data carrier.
<b>Password</b>	Provide your password for authentication support by your cellular data carrier.
<b>Access Point Name (APN)</b>	Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols such as Europe, the middle east and Asia.
<b>Authentication Type</b>	Use the drop-down menu to specify authentication type used by your cellular data provider. Supported authentication types are <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

8. Use the **NAT Direction** field to specify the NAT direction used with the access point's WAN card. Options include *Inside*, *Outside* or *None*. The default is *None*.
9. Configure the **Inbound IP Firewall Rules**. Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing rule.
10. Select the **VPN Crypto Map** to use with this WWAN configuration. Use the drop-down menu to apply an existing crypt map configuration to this WWAN interface.
11. Configure the **WWAN Default Route Priority**. Use the spinner control to set the Default Route Priority for the WWAN default route. Select from 1 - 8,000. The default setting is 3,000.
12. Select **OK** to save or override the changes to the *Advanced Settings* screen. Select **Reset** to revert to the last saved configuration.

### 5.4.5.3.6 PPPoE Configuration

#### ► Profile Interface Configuration

*PPP over Ethernet* (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG supported controllers and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN were to fail.



**NOTE:** Access points with PPPoE enabled continue to support VPN, NAT, PBR and 3G failover over the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

---



**NOTE:** PPPoE is supported on AP6522, AP6522M, AP6532, AP6562, AP71XX, AP7522, AP7532, AP81XX and AP82XX models and is not available on AP6511 and AP6521 model access points.

---

---

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic flow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

To create a PPPoE point-to-point configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Interface** to expand its submenu items.
5. Select **PPPoE**.

**Basic Settings**

**Enable PPPoE**  Disabled  Enabled

**Service**

**DSL Modem Network (VLAN)**  (1 to 4,094)

**Client IP Address**   .  .

**Authentication**

**Username**

**Password**   Show

**Authentication Type**

**Connection**

**Maximum Transmission Unit (MTU)**  (500 to 1,492)

**Client Idle Timeout**   (1 to 1,093)

**Keep Alive**

**Network Address Translation (NAT)**

**NAT Direction**  Inside  Outside  None

**Security Settings**

**Inbound IP Firewall Rules**

**VPN Crypto Map**

**Default Route Priority**

**PPPoE Default Route Priority**  (1 to 8,000)

**Figure 5-146** Device Overrides - PPPoE screen

6. Use the **Basic Settings** field to enable PPPoE and define a PPPoE client:

<b>Enable PPPoE</b>	Select <i>Enable PPPoE</i> to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled.
<b>Service</b>	Enter the 128 character maximum PPPoE client service name provided by the service provider.
<b>DSL Modem Network (VLAN)</b>	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 - 4,094. The default VLAN is VLAN1
<b>Client IP Address</b>	Provide the numerical (non hostname) IP address of the PPPoE client.

7. Define the following **Authentication** parameters for PPPoE client interoperation:

<b>Username</b>	Provide the 64 character maximum username used for authentication support by the PPPoE client.
<b>Password</b>	Provide the 64 character maximum password used for authentication by the PPPoE client. Select <i>Show</i> to display the actual characters comprising the password.
<b>Authentication Type</b>	Use the drop-down menu to specify authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

8. Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

<b>Maximum Transmission Unit (MTU)</b>	Set the PPPoE client <i>Maximum Transmission Unit</i> (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
<b>Client Idle Timeout</b>	Set a timeout in either <i>Seconds</i> (1 - 65,535), <i>Minutes</i> (1 - 1,093) or <i>Hours</i> . The access point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes.
<b>Keep Alive</b>	Select this option to ensure the point-to-point connect to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

9. Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

*Network Address Translation* (NAT) converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point router maps its local (*Inside*) network addresses to WAN (*Outside*) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is None (neither inside or outside).

10. Define the following **Security Settings** for the PPPoE configuration:

<b>Inbound IP Firewall Rules</b>	Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the <i>Create</i> icon to define a new rule configuration or the <i>Edit</i> icon to modify an existing rule. For more information, see <a href="#">Wireless Firewall on page 8-2</a> .
<b>VPN Crypto Map</b>	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

11. Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

12. Select **OK** to save the changes to the PPPoE screen. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

#### 5.4.5.4 Overriding the Network Configuration

##### ▶ *Device Overrides*

Setting a network configuration is a large task comprised of numerous administration activities. Each of the configuration activities described can have an override applied to the original configuration. Applying an override differentiates the device from the profile's configuration and requires careful administration to ensure this one device still supports the deployment requirements within the network.

A profile's network configuration process consists of the following:

- *Overriding the DNS Configuration*
- *Overriding an ARP Configuration*
- *Overriding a L2TPv3 Profile Configuration*
- *Overriding IGMP Snooping Configuration*
- *Overriding a Quality of Service (QoS) Configuration*
- *Overriding a Spanning Tree Configuration*
- *Overriding a Routing Configuration*
- *Overriding a Dynamic Routing (OSPF) Configuration*
- *Overriding a Forwarding Database Configuration*
- *Overriding a Bridge VLAN Configuration*
- *Overriding a Cisco Discovery Protocol Configuration*
- *Overriding a Link Layer Discovery Protocol Configuration*
- *Overriding a Miscellaneous Network Configuration*
- *Overriding Alias Configuration*

##### 5.4.5.4.1 Overriding the DNS Configuration

###### ▶ *Overriding the Network Configuration*

*Domain Naming System (DNS)* DNS is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS you need to remember a series of numbers (123.123.123.123) instead of a domain name (www.domainname.com).

To define the DNS configuration or apply overrides to an existing configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **DNS**.

**Domain Name System (DNS)**

Domain Name

Enable Domain Lookup

Enable DNS Server Forwarding

**DNS Servers**

Name Servers

IP Address	
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>

OK Reset Exit

**Figure 5-147** Device Overrides - Network DNS screen



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's Device Overrides field and select **Clear Overrides**. This removes all overrides from the device.

6. Provide or override the default Domain Name used when resolving DNS names. The name cannot exceed 64 characters.
7. Set or override the following *Domain Name System* (DNS) settings:

<b>Enable Domain Lookup</b>	Select this option to enable DNS on the access point. When enabled, human friendly domain names can be converted into numerical IP destination addresses. The radio button is selected by default.
<b>Enable DNS Server Forwarding</b>	Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by the access point's own DNS resources. This feature is disabled by default.

8. Provide a list of up to three DNS servers to forward DNS queries if DNS resources are unavailable. The DNS name servers are used to resolve IP addresses. Use the Clear link next to each DNS server to clear the DNS name server's IP address from the list.
9. Select **OK** to save the changes and overrides made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.2 Overriding an ARP Configuration

##### ► *Overriding the Network Configuration*

*Address Resolution Protocol* (ARP) is a protocol for mapping an IP address to a hardware MAC address. ARP provides protocol rules for making this correlation and providing address conversion in both directions. This ARP assignment can be overridden

as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

When an incoming packet destined for a host arrives at the access point, the access point's gateway uses ARP to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to the destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply indicating as such. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To define an ARP supported configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **ARP**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

**Address Resolution Protocol (ARP)**

Switch VLAN Interface	IP Address	MAC Address	Device Type	
1	192.168.13.2	00-43-8D-62-71-AB	DHCP Server	

+ Add Row

▶ OK
Reset

**Figure 5-148** Device Overrides - Network ARP screen

6. Set or override the following parameters to define the ARP configuration:

<b>Switch VLAN Interface</b>	Use the spinner control to select a VLAN (1 - 4094) for an address requiring resolution.
<b>IP Address</b>	Define the IP address used to fetch a MAC address.
<b>MAC Address</b>	Displays the target MAC address that's subject to resolution. This is the MAC used for mapping an IP address to a MAC address that's recognized on the network.

<b>Device Type</b>	Specify the device type the ARP entry supports (either Host, Router or DHCP Server). Host is the default setting.
--------------------	---

7. Select the OK button to save the changes and overrides to the ARP configuration. Select Reset to revert to the last saved configuration.

### 5.4.5.4.3 Overriding a L2TPv3 Profile Configuration

#### ► *Overriding the Network Configuration*

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports.

Multiple pseudowires can be created within an L2TP V3 tunnel. WING supported access points support an Ethernet VLAN pseudowire type exclusively.



**NOTE:** A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.



**NOTE:** If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

To define or override an L2TPV3 configuration for an access point profile:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.

5. Select **L2TP V3**.

**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

The screenshot shows the 'General Settings' section of the L2TPv3 Tunnel configuration. It includes the following fields and controls:

- Host Name:** A text input field with a pencil icon.
- Router ID:** A numeric input field containing '0 . 0 . 0 . 0' with a blue override icon and an 'IP Address' dropdown menu.
- UDP Listen Port:** A numeric input field containing '1024' with a blue override icon and a range indicator '(1,024 to 65,535)'.
- Tunnel Bridging:** A checkbox with a blue override icon.

At the bottom right, there are 'OK' and 'Reset' buttons.

**Figure 5-149** Device Overrides - Network - L2TPv3 screen, General tab

6. Set the following **General Settings** for an L2TPv3 profile configuration:

<b>Host Name</b>	Define a 64 character maximum hostname to specify the name of the host that sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRQ and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
<b>Router ID</b>	Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunnelled peer.
<b>UDP Listen Port</b>	Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,353.
<b>Tunnel Bridging</b>	Select this option to enable or disable bridge packets between two tunnel end points. This setting is disabled by default.

7. Select the **L2TP Tunnel** tab.



**Figure 5-151** Device Overrides - Network - L2TPv3 screen, Add T2TP Tunnel Configuration

10. If creating a new tunnel configuration, assign it a 31 character maximum **Name**.
11. Define the following **Settings** required for the L2TP tunnel configuration:

<b>Local IP Address</b>	Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests.
<b>MTU</b>	Set the <i>maximum transmission unit</i> (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU from 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data.

<b>Use Tunnel Policy</b>	Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available a new policy can be created or an existing one can be modified. For more information, refer to <a href="#">Configuring Captive Portal Policies on page 9-2</a> .
<b>Local Hostname</b>	Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages.
<b>Local Router ID</b>	Specify the router ID sent in tunnel establishment messages with a potential peer device.
<b>Establishment Criteria</b>	Specify the establishment criteria for creating a tunnel. The tunnel is only created if this device is one of the following: <ul style="list-style-type: none"> <li>• <i>vrp-master</i></li> <li>• <i>cluster-master</i></li> <li>• <i>rf-domain-manager</i></li> </ul> The tunnel is always created if <i>Always</i> is selected. This indicates that the device need not be any one of the above three (3) to establish a tunnel.
<b>VRRP Group</b>	Set the VRRP group value. This is only applicable if the <i>Establishment Criteria</i> specifies <i>vrp-master</i> .
<b>Critical Resource</b>	This table lists the critical resources defined for this system. The tunnel is created and maintained if the critical resources are available. The tunnel is brought down if any one of the defined critical resource goes down or is unreachable.

- Refer to the **Peer table** to review the configurations of the peers available for tunnel connection.
- Select **+ Add Row** to populate the table with a maximum of two peer configurations.

The screenshot shows a dialog box titled "Add Row" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Peer ID:** A numeric input field containing "1" with up and down arrow buttons and a range indicator "(1 to 2)".
- Peer IP Address:** A text input field with a blue information icon (i) to its left.
- Host Name:** A text input field with a blue information icon (i) to its left.
- Router ID:** A text input field containing "any" with a blue information icon (i) to its left and a dropdown arrow on the right.
- Encapsulation:** A dropdown menu currently showing "IP" with a blue information icon (i) to its left.
- UDP Port:** A numeric input field containing "1701" with up and down arrow buttons and a range indicator "(1,024 to 65,535)".
- Ipsec Secure:** A checkbox that is currently unchecked with a blue information icon (i) to its left.
- Ipsec Gateway:** A text input field with a blue information icon (i) to its left.

At the bottom of the dialog, there are two buttons: "OK" and "Exit".

**Figure 5-152** Device Overrides - Network - L2TPv3 screen, Add L2TP Peer Configuration

14. Define the following **Peer** parameters:

<b>Peer ID</b>	Define the primary peer ID used to set the primary and secondary peer for tunnel failover. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or router ID matches.
<b>Peer IP Address</b>	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment.
<b>Host Name</b>	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process.
<b>Router ID</b>	Specify the router ID sent in tunnel establishment messages with this specific peer.
<b>Encapsulation</b>	Select either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port.
<b>IPSec Secure</b>	Enables or disable IPSec security for the tunnel.
<b>IPSec Gateway</b>	If <i>IPSec Secure</i> is enabled, provide the IPSec gateway device's IP address.

15. Select **OK** to save the peer configuration and overrides.

16. Refer to the Session table to review the configurations of the peers available for tunnel connection.

17. Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

18. Define the following **Session** parameters:

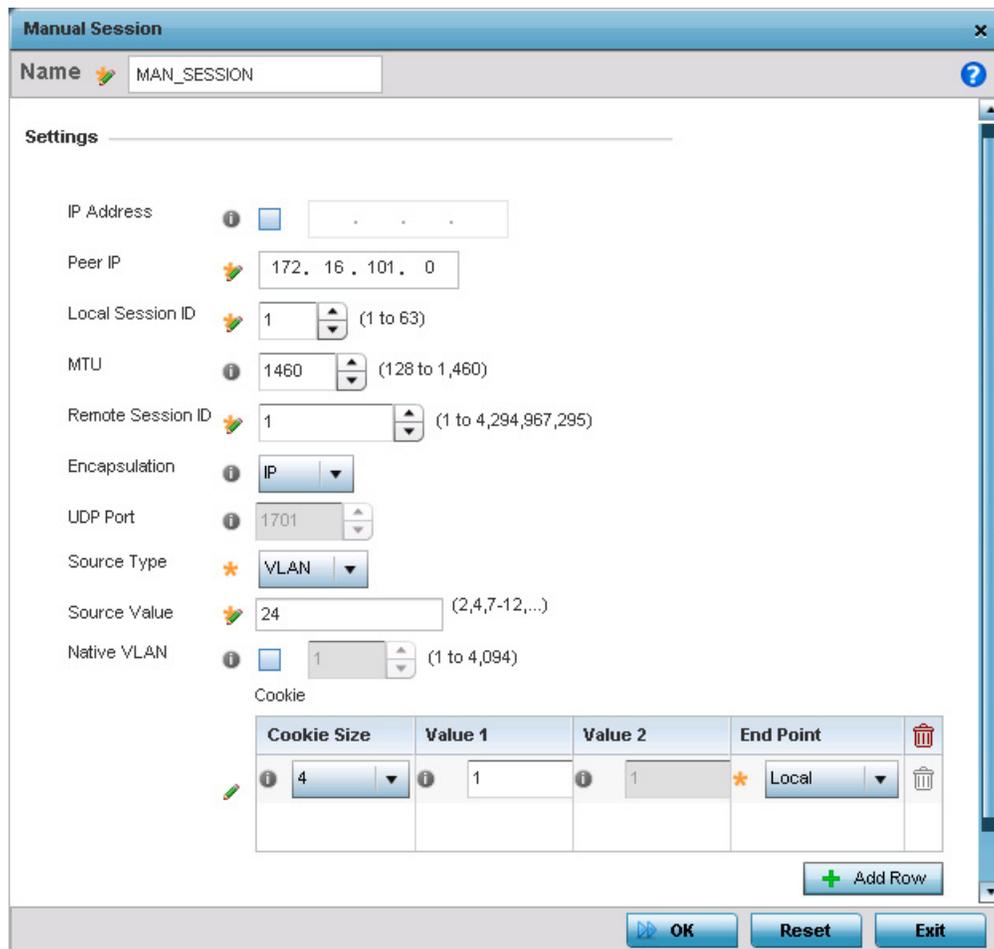
<b>Name</b>	Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed.
<b>Pseudowire ID</b>	Define a pseudowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a <i>packet-switching network</i> (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.
<b>Traffic Source Type</b>	Lists the type of traffic tunnelled in this session.
<b>Traffic Source Value</b>	Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 - 4,094.
<b>Native VLAN</b>	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer.

19. Select **OK** to save the changes and overrides to the T2TP Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.

20. Select the **Manual Session** tab.

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.





**Figure 5-154** Device Overrides - Network - L2TPv3 screen, Add T2TP Peer Configuration

23. Set the following **Session** parameters:

<b>Name</b>	Define a 31 character maximum name of this tunnel session. After a successful tunnel connection and establishment, the session is created. Each session name represents a single data stream.
<b>IP Address</b>	Specify the IP address used to be as tunnel source ip address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, it would use the IP address on which it had received the tunnel create request.
<b>IP</b>	Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel.
<b>Local Session ID</b>	Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in session establishment message to the L2TP peer.
<b>MTU</b>	Define the session <i>maximum transmission unit</i> (MTU) as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
<b>Remote Session ID</b>	Use the spinner control to set the remote session ID passed in the establishment of the tunnel session. Assign an ID from 1 - 4,294,967,295.

<b>Encapsulation</b>	Select either <i>IP</i> or <i>UDP</i> as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running.
<b>Source VLAN</b>	Define the VLAN range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames.
<b>Native VLAN</b>	Select this option to define the native VLAN that will not be tagged

24. Select the **+ Add Row** button to set the following:

<b>Cookie Size</b>	Set the size of the cookie field within each L2TP data packet. Options include 0, 4 and 8. The default setting is 0.
<b>Value 1</b>	Set the cookie value first word.
<b>Value 2</b>	Set the cookie value second word.
<b>End Point</b>	Define whether the tunnel end point is local or remote.

25. Select **OK** to save the changes and overrides to the session configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.4 Overriding IGMP Snooping Configuration

##### ► *Overriding the Network Configuration*

*Internet Group Management Protocol* (IGMP) is a protocol to establish and maintain multicast group memberships to interested members. Multicasting allows a computer on a network to send content to multiple computers who have registered to receive the content. IGMP Snooping is the term for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.

To configure IGMP Snooping:

1. Select the **Configuration** tab from the Web UI.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **IGMP Snooping**.

**General**

Enable IGMP Snooping

Forward Unknown Multicast Packets

**IGMP Querier**

Enable IGMP Querier

IGMP Version  (1 to 3)

IGMP Query Interval  Minutes (1 to 300)

IGMP Robustness Variable  (1 to 7)

Maximum Response Time  seconds (1 to 25)

Other Querier Time Expiry  Minutes (1 to 5)

OK Reset Exit

**Figure 5-155** Device Overrides - Network - IGMP Snooping Screen

6. Set the following parameters to configure general IGMP Snooping values.

<b>Enable IGMP Snooping</b>	Select the box to enable IGMP Snooping on the access point. This feature is enabled by default.
<b>Forward Unknown Multicast Packets</b>	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the <i>Unknown Multicast Forward</i> feature is also disabled for the selected VLANs. This is enabled by default.

7. Set the following for **IGMP Querier** configuration:

<b>Enable IGMP Querier</b>	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then forwarded on that port. An AP71XX model access point can also be an IGMP querier.
<b>IGMP Version</b>	Use the spinner control to set the IGMP version compatibility to one of IGMP version 1,2 or 3. The default IGMP version is 3.
<b>IGMP Query Interval</b>	Sets the IGMP query interval. This parameter will be used only when the querier functionality is enabled. Define an interval value in <i>Seconds</i> (1 - 18,000), <i>Minutes</i> (1 - 300) or <i>Hours</i> (1 - 5) up to maximum of 5 hours. The default value is 60 seconds.
<b>IGMP Robustness Variable</b>	Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value is 2.

<b>Maximum Response Time</b>	Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
<b>Other Querier Time Expiry</b>	Specify an interval in either <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

8. Select **OK** to save the changes and overrides to the session configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.5 Overriding a Quality of Service (QoS) Configuration

##### ► *Overriding the Network Configuration*

QoS values are required to provide service priority to packets. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit *Differentiated Service Code Point* (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet. This QoS assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar access point models.

To define an QoS configuration for DSCP mappings:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Quality of Service**.

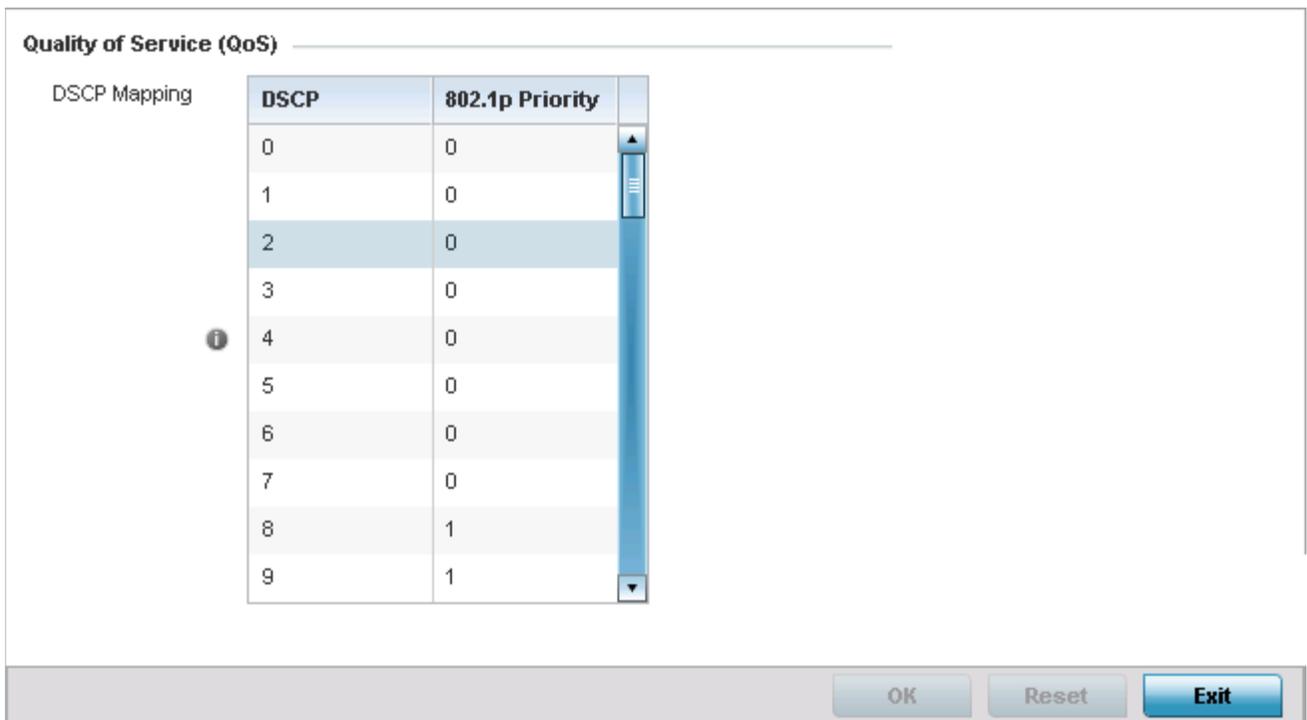


**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

---



---



**Figure 5-156** Device Overrides - Network QoS screen

6. Set or override the following parameters for the IP DSCP mappings for untagged frames:

<b>DSCP</b>	Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification.
<b>802.1p Priority</b>	Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: <i>0 – Best Effort</i> <i>1 – Background</i> <i>2 – Spare</i> <i>3 – Excellent Effort</i> <i>4 – Controlled Load</i> <i>5 – Video</i> <i>6 – Voice</i> <i>7 – Network Control</i>

7. Use the spinner controls within the 802.1p Priority field for each DSCP row to change or override the priority value.  
 8. Select the **OK** button located to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.6 Overriding a Spanning Tree Configuration

##### ► *Overriding the Network Configuration*

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with multiple *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To override a profile's spanning tree configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Spanning Tree**.

**MSTP Configuration**

MSTP Enable

Max Hop Count  (7 to 127)

MST Config Name

MST Revision Level  (0 to 255)

Cisco MSTP Interoperability

Hello Time  (1 to 10)

Forward Delay  (4 to 30)

Maximum Age  (6 to 40)

**PortFast**

PortFast BPDU Filter

PortFast BPDU Guard

**Error Disable**

Enable Recovery

**Spanning Tree Instance**

Instance	Priority	

+ Add Row

**Spanning Tree Instance VLANs**

Instance	VLANs	

+ Add Row

OK Reset Exit

**Figure 5-157** Device Overrides - Network - Spanning Tree screen

6. Set the following **MSTP Configuration** parameters:

<b>MSTP Enable</b>	Select this option to enable MSTP for this profile. MSTP is disabled by default, so if requiring different (groups) of VLANs with the profile supported network segment.
<b>Max Hop Count</b>	Define the maximum number of hops the BPDU will consider valid in the spanning tree topology. The available range is from 7 - 127. The default setting is 20.
<b>MST Config Name</b>	Define a 64 character maximum name for the MST region as an identifier.
<b>MST Revision Level</b>	Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
<b>Hello Time</b>	Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and star/stop port forwarding as required.

<b>Forward Delay</b>	Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately start to forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay of while it goes through the listening and learning states. The time spent in the listening and learning states is defined by the forward delay (15 seconds by default).
<b>Maximum Age</b>	Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40. The default setting is 20.

7. Define the following **PortFast** parameters for the profile configuration:

<b>PortFast BPDU Filter</b>	Select Enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is disabled.
<b>PortFast BPDU Guard</b>	Select Enable to invoke a BPDU guard for the portfast enabled port. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly and enable the access point to keep track of network changes and to start and stop port forwarding as required. The default setting is disabled.

8. Define the following **Error Disable** settings:

<b>Enable Recovery</b>	Select this option to enable a error disable timeout resulting from a BPDU guard. This setting is disabled by default.
<b>Recovery Interval</b>	Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds with a default setting of 300.

9. Use the **Spanning Tree Instance** table to add indexes to the spanning tree topology.
10. Add up to 16 indexes and use the Priority setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.
11. Use the **Spanning Tree Instance VLANs** table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.
12. Select the **OK** button located at the bottom right of the screen to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.7 Overriding a Routing Configuration

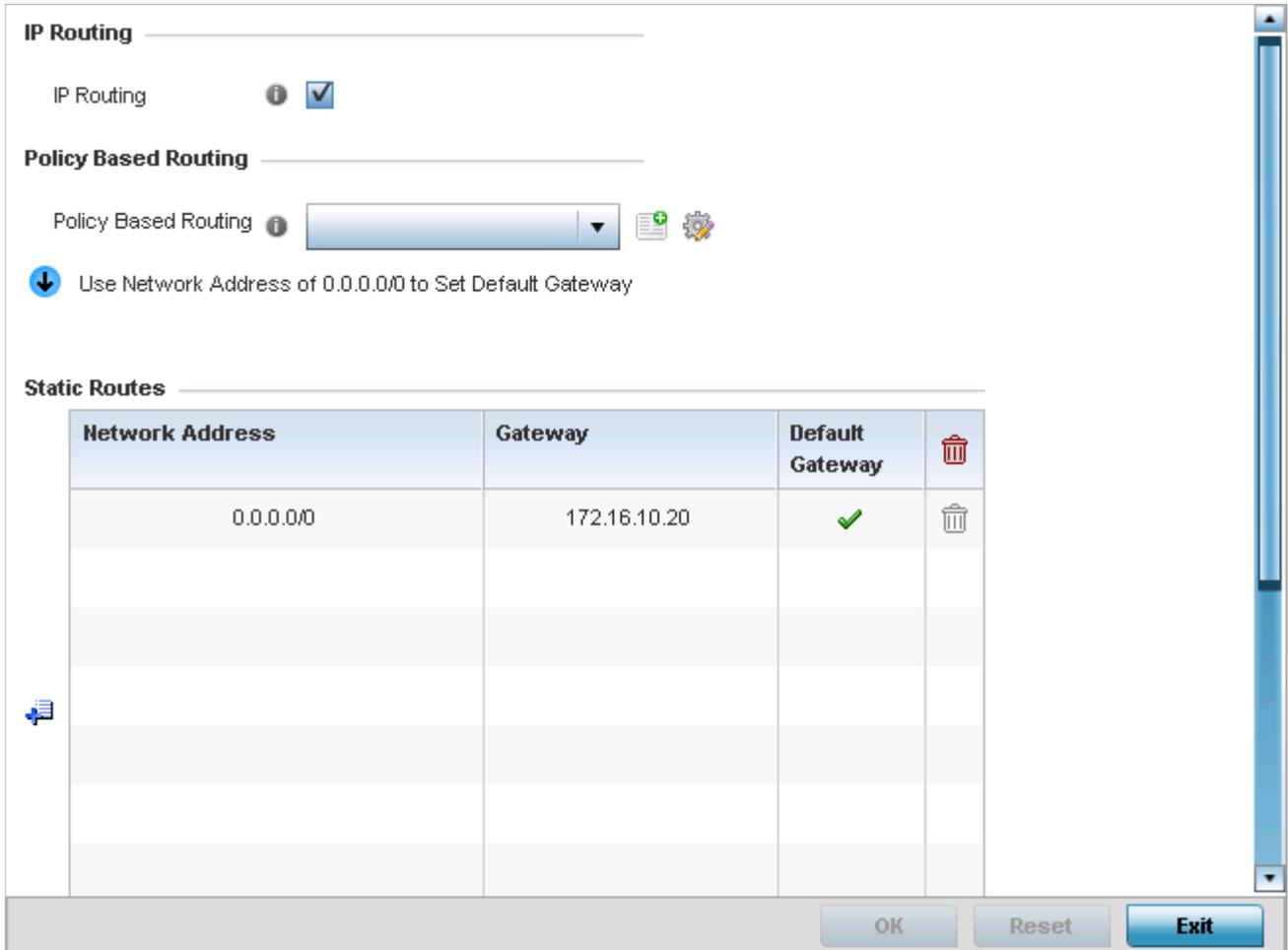
##### ► *Overriding the Network Configuration*

Routing is the process of selecting IP paths in a network to send access point managed network traffic. Use the *Routing* screen to set destination IP and gateway addresses enabling assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the resource space required to maintain address pools.

To override a profile's route configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.

3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Routing**.



**Figure 5-158** Device Overrides - Network - Network Routing screen

6. Select the **IP Routing** option to enable IP routing using static routes provided in the route table. This option is enabled by default.
7. Select the **Policy Based Routing** policy to apply to this profile. Click the **Create** icon to create a policy based route or click the **Edit** to edit an existing policy after selecting it in the drop-down list. For more information on policy based routing, see [Policy Based Routing \(PBR\) on page 7-2](#).
8. Select **Add Row +** as needed to include single rows with in the static IPv4 route table.
9. Add IP addresses and network masks in the **Network** column.
10. Provide the **Gateway** used to route traffic.
11. Refer to the **Default Route Priority** field and set the following parameters:

<b>Static Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default static route. The default setting is 100.
<b>DHCP Client Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000.

**Enable Routing Failure**

When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default.

12. Select the **OK** button located at the bottom right of the screen to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.8 Overriding a Dynamic Routing (OSPF) Configuration

##### ► *Overriding the Network Configuration*

*Open Shortest Path First* (OSPF) is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers.

OSPF uses a route table managed by the link *cost* (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability. Setting a cost value provides a dynamic way to load balancing traffic between routes of equal cost.

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can be defined as:

- *stub area* - A stub area is an area which does not receive route advertisements external to the autonomous system (AS) and routing from within the area is based entirely on a default route.
- *totally-stub* - A totally stubby area does not allow summary routes and external routes. that is, The only way for traffic to get routed outside of the area is. A default route is the only way to route traffic outside of the area. When there's only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- *non-stub* - An area that imports autonomous system external routes and send them to other areas. However. it still cannot receive external routes from other areas.
- *nssa* - NSSA is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- *totally nssa* - This is an NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an autonomous system boundary router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a *point-to-point* link, OSPF knows it is sufficient, and the link stays *up*. If on a *broadcast* link, the router waits for election before determining if the link is functional.

To override a profile's dynamic routing configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.

5. Select **OSPF**.

**Figure 5-159** Device Overrides - Network - OSPF Settings screen

## 6. Enable/disable OSPF and provide the following dynamic routing settings:

<b>Enable OSPF</b>	Select this option to enable OSPF for this access point. OSPF is disabled by default.
<b>Router ID</b>	Select this option to define a router ID (numeric IP address) for this access point. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
<b>Auto-Cost</b>	Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1.
<b>Passive Mode on All Interfaces</b>	When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default.
<b>Passive Removed</b>	If enabling <i>Passive Mode on All Interfaces</i> , use the spinner control to select VLANs (by numeric ID) as OSPF non passive interfaces. Multiple VLANs can be added to the list.
<b>Passive Mode</b>	If disabling <i>Passive Mode on All Interfaces</i> , use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list.

<b>VRRP Mode Check</b>	Select this option to enable checking VRRP state. If the interface's VRRP state is not <i>Backup</i> , then the interface is published via OSPF.
------------------------	--

7. Set the following **OSPF Overload Protection** settings:

<b>Number of Routes</b>	Use the spinner controller to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295.
<b>Retry Count</b>	Set the maximum number of retries (OSPF resets) permitted before the OSPS process is shut down. The available range is from 1 - 32. The default setting is 5.
<b>Retry Time Out</b>	Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds.
<b>Reset Time</b>	Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds.

8. Set the following **Default Information**:

<b>Originate</b>	Select this option to make the default route a distributed route. This setting is disabled by default.
<b>Always</b>	Enabling this setting continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default.
<b>Metric Type</b>	Select this option to define the exterior metric type (1 or 2) used with the default route.
<b>Route Metric</b>	Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting given route.

9. Refer to the **Route Redistribution** table to set the types of routes that can be used by OSPF.
10. Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include *connected*, *kernel* and *static*.
11. Select the **Metric Type** option to define the exterior metric type (1 or 2) used with the route redistribution. Select the **Metric** option to define route metric used with the redistributed route.
12. Use the **OSPF Network** table to define networks (IP addresses) to connect using dynamic routes.
13. Select the **+ Add Row** button to populate the table. Add the IP address and mask of the network(s) participating in OSPF. Additionally, define the OSPF area (IP address) to which the network belongs.
14. Set an OSPF Default Route Priority (1 - 8,000) as the priority of the default route learnt from OSPF.
15. Click the **Clear** button next to the **Clear OSPF Process** field to clear all OSPF routing entries.
16. Select the **Area Settings** tab.

An OSPF Area contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.



The screenshot shows the 'OSPF Area' configuration window. The 'Area ID' is set to 3892748394 with a dropdown menu set to 'Integer'. The 'Authentication Type' is 'simple-password', 'Type' is 'nssa', 'Default Cost' is checked and set to 600 (range 1 to 16,777,215), 'Translate Type' is 'translate-candidate', and 'Range' is empty. At the bottom are 'OK', 'Reset', and 'Exit' buttons.

**Figure 5-161** Device Overrides - Network - OSPF Area Configuration screen

19. Set the **OSPF Area** configuration.

<b>Area ID</b>	Use the drop-down menu and specify either an IP address or Integer for the OSPF area.
<b>Authentication Type</b>	Select either <i>None</i> , <i>simple-password</i> or <i>message-digest</i> as credential validation scheme used with the OSPF dynamic route. The default setting is None.
<b>Type</b>	Set the OSPF area type as either <i>stub</i> , <i>totally-stub</i> , <i>nssa</i> , <i>totally-nssa</i> or <i>non-stub</i> .
<b>Default Cost</b>	Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16,777,215.
<b>Translate Type</b>	Define how messages are translated. Options include <i>translate-candidate</i> , <i>translate-always</i> and <i>translate-never</i> . The default setting is <i>translate-candidate</i> .
<b>Range</b>	Specify a range of addresses for routes matching address/mask for OSPF summarization.

20. Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

21. Select the **Interface Settings** tab.

<span>OSPF Settings</span> <span>Area Settings</span> <span>Interface Settings</span>						
Name	Type	Description	Admin Status	VLAN	IP Address	
vlan1	VLAN		Enabled	1	172.16.10.23/24	

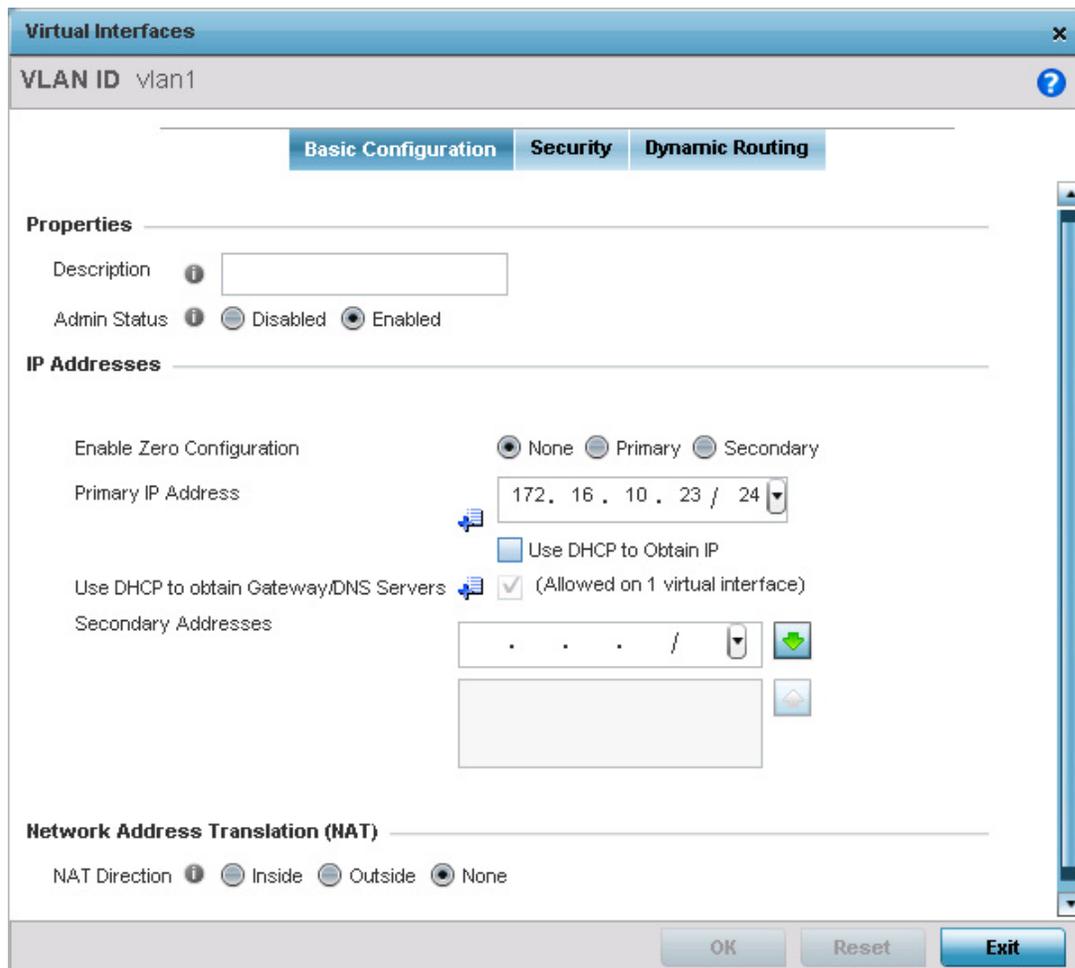
Type to search in tables Row Count: 1

**Figure 5-162** Device Overrides - Network - OSPF Interface Settings screen

22. Review existing **Interface Settings** using:

<b>Name</b>	Displays the name defined for the interface configuration.
<b>Type</b>	Displays the type of interface.
<b>Description</b>	Lists each interface's 32 character maximum description.
<b>Admin Status</b>	Displays whether Admin Status privileges have been enabled or disabled for the OSPF route's virtual interface connection.
<b>VLAN</b>	Lists the VLAN IDs set for each listed OSPF route virtual interface.
<b>IP Address</b>	Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.

23. Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.



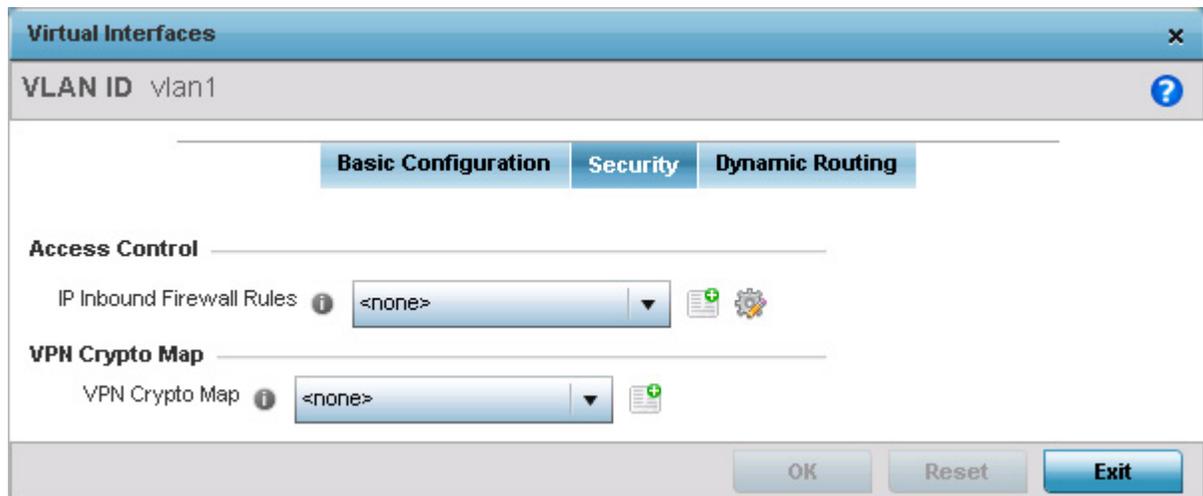
**Figure 5-163** Device Overrides - Network - OSPF Virtual Interface - Basic Configuration screen

24. Within the **Properties** field, enter a 32 character maximum Description to help differentiate the virtual interface configuration used with this OSPF route. Enable/disable admin privileges as need. They're disabled by default.
25. Use the **IP Addresses Area** to set how route addresses are created for the virtual configuration.

Zero Configuration can be enabled and set as the *Primary* or *Secondary* means of providing IP addresses for the OSPF virtual route. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. The drivers for the wireless adapter query the NDIS Object IDs and pass the available network names (SSIDs) to the service. The service then lists them in the user interface on the **Wireless Networks** tab in the connection's Properties or in the *Wireless Network Connection* dialog box accessible from the notification area. A checked build version of the WZC service can be used by developers to obtain additional diagnostic and tracing information logged by the service.

26. Select **Use DHCP to Obtain IP** to use the access point's DHCP server resource as the means of providing requested IP addresses to the OSPF route's virtual interface.
27. Select **Use DHCP to Obtain Gateway/DNS Servers** to learn default gateway, name servers and the domain name on just this interface. Once selected, specify an IP address and mask in dot decimal format.
28. Define the **NAT Direction** as either *Inside*, *Outside* or *None*.
  - *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.

- *Outside* - Packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.
  - *None* - No NAT activity takes place. This is the default setting.
29. Select **OK** to save the changes to the basic configuration. Select **Reset** to revert to the last saved configuration.
  30. Select the **Security** tab.



**Figure 5-164** OSPF Virtual Interface - Security screen

31. Use the **Inbound IP Firewall Rules** drop-down menu to select the IP access and deny rules to apply to the OSPF dynamic route.
32. Either select an existing IP firewall policy or use the default set of IP firewall rules. The firewall inspects OSPF route traffic flows and detects potential attacks on the dynamic route not visible to traditional wired firewall appliances. Select the **Create** icon to define a new set of IP firewall rules that can be applied to the OSPF route configuration. Selecting **Edit** allows for the modification of an existing IP firewall rules configuration. For more information, see [Wireless Firewall on page 8-2](#).
33. Select the **VPN Crypto Map** to use with this VLAN configuration. Use the drop-down menu to apply an existing crypto map configuration to this VLAN interface. Use the **Create** icon to create a new VPN Crypto Map or use the **Edit** icon to edit an existing VPN Crypto Map configuration before applying it to this VLAN.  
Crypto Map entries are sets of configuration parameters for encrypting packets passing through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration.
34. Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.
35. Select the **Dynamic Routing** tab.

The screenshot shows the 'Virtual Interfaces' configuration window for 'vlan1'. The 'Dynamic Routing' tab is active, displaying the following settings:

- OSPF Settings:**
  - Priority: 0 (range 0 to 255)
  - Cost: 1 (range 1 to 65,535)
  - Bandwidth: 1 (range 1 to 10,000,000)
- OSPF Authentication:**
  - Chosen Authentication Type: None
- MD5 Authentication:**
  - Table with columns: Key ID, Password, and a delete icon.

Buttons at the bottom include 'OK', 'Reset', and 'Exit'.

**Figure 5-165** OSPF Virtual Interface - Dynamic Routing screen

36. Refer to the following to configure **OSPF Settings**:

<b>Priority</b>	Select to enable or disable OSPF priority settings. Use the spinner to configure a value in the range 0-255. This option sets the priority of this interface becoming the <i>Designated Router</i> (DR) for the network. DRs provide routing updates to the network by maintaining a complete topology table of the network and sends the updates to the other routers in the network using multicast. Setting a high value increases the chance of this interface becoming a DR. Setting this value to Zero (0) prevents this interface from being elected a DR.
<b>Cost</b>	Select to enable or disable OSPF cost settings. Use the spinner to configure a cost value in the range 1-65535. Use this option to set the OSPF cost of this interface. OSPF cost is the overhead required to send a packet over this interface.
<b>Bandwidth</b>	Select to enable or disable OSPF bandwidth settings. Use the spinner to configure a bandwidth settings in the range 1-10,000,000 KBps. Use this option to set the bandwidth of this interface in KBps.

37. Configure the **OSPF Authentication Type** settings by selecting from the drop-down list. The available options are *None*, *Null*, *simple-password* and *message-digest*.
38. Refer the following to configure **MD5 Authentication** keys. Click the **+ Add Row** button to add a row to the table.

<b>Key ID</b>	Set the unique MD5 Authentication key ID. The available key ID range is 1-255.
<b>Password</b>	Set the OSPF password. This value is displayed as "asterisk" (*). Select <i>Show</i> to display the actual characters comprising the password.

39. Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.9 Overriding a Forwarding Database Configuration

##### ► *Overriding the Network Configuration*

A *Forwarding Database* is used by a bridge to forward or filter packets. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

This forwarding database assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

To define or override a forwarding database configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Forwarding Database**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

---



---

**Aging Time**

Bridge Aging Time ⓘ  (0,10-1000000 seconds)

**Static Forwarding Table**

MAC Address	VLAN Id	Interface Name	
* <input type="text" value="0E - FD - 08 - 16 - 32 - 64"/>	* <input type="text" value="1"/> <input type="button" value="▲"/> <input type="button" value="▼"/>	ⓘ <input type="text" value="TO_HQ"/>	<input type="button" value="🗑"/>

**Figure 5-166** Device Overrides - Network Forwarding Database screen

- Define or override a **Bridge Aging Time** from 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry will remain in the a bridge's forwarding table before being deleted due to lack of activity. If an entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

- Define or override the **L3e Lite Entry Aging Time** from 10 - 1,000,000 seconds.
- Use the **+ Add Row** button to create a new row within the MAC address table.
- Set or override a destination MAC Address address. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).
- Define or override the target VLAN ID if the destination MAC is on a different network segment.
- Provide an **Interface Name** used as the target destination interface for the target MAC address.
- Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.10 Overriding a Bridge VLAN Configuration

##### ▶ *Overriding the Network Configuration*

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical. VLANs are broadcast domains to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

For example, say several computers are used into conference room X and some into conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The creation of a VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single entity, but ignore the systems that aren't using same VLAN ID.



<b>Edge VLAN Mode</b>	Defines whether the VLAN is currently in edge VLAN mode. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is defined with wireless clients and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't be marked as an edge VLAN. When defining a VLAN as edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active.
<b>Trust ARP Response</b>	When ARP trust is enabled, a green check mark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks.
<b>Trust DHCP Responses</b>	When DHCP trust is enabled, a green check mark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.

7. Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify or override an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

The screenshot shows the 'Bridge VLAN' configuration window for 'VLAN 1'. The window is divided into two tabs: 'General' and 'IGMP Snooping'. The 'General' tab is active. The 'Description' field contains 'engineering vlan1'. Under the 'Extended VLAN Tunnel' section, 'Bridging Mode' is set to 'Automatic', 'IP Outbound Tunnel ACL' is '<none>', and 'MAC Outbound Tunnel ACL' is '<none>'. Under the 'Layer 2 Firewall' section, 'Trust ARP Responses' is checked, 'Trust DHCP Responses' is unchecked, and 'Edge VLAN Mode' is checked. At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 5-168** Device Overrides - Add Network Bridge VLAN screen

8. If adding a new bridge VLAN configuration, use the spinner control to define or override a VLAN ID from 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined.

9. If creating a new Bridge VLAN, provide a Description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
10. Select the **Per VLAN Firewall** option to enable firewall on this interface. Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate a large amount of flow tables that store information on the traffic that is allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory on the device that could be used for other critical purposes. With the Per VLAN firewall feature enabled on an interface, flow tables are only generated for that interface, Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory that can be used for other purposes.

Firewall can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network.

11. Select the **L2 Tunnel Broadcast Optimization** option to prevent flooding of ARP packets on this bridge interface. Broadcast optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered.
12. Set or override the following **Extended VLAN Tunnel** parameters:

<b>Bridging Mode</b>	Specify one of the following bridging mode for use on the VLAN. <ul style="list-style-type: none"> <li>• <i>Automatic</i>: Select Automatic mode to let the controller determine the best bridging mode for the VLAN.</li> <li>• <i>Local</i>: Select Local to use local bridging mode for bridging traffic on the VLAN.</li> <li>• <i>Tunnel</i>: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. Tunnel must be selected to successfully create a mesh connection between two Standalone APs.</li> <li>• <i>isolated-tunnel</i>: Select isolated-tunnel to use a dedicated tunnel for bridging traffic on the VLAN.</li> </ul>
<b>IP Outbound Tunnel ACL</b>	Select an <i>IP Outbound Tunnel ACL</i> for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available click the create button to make a new one.
<b>MAC Outbound Tunnel ACL</b>	Select a <i>MAC Outbound Tunnel ACL</i> for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available click the create button to make a new one.



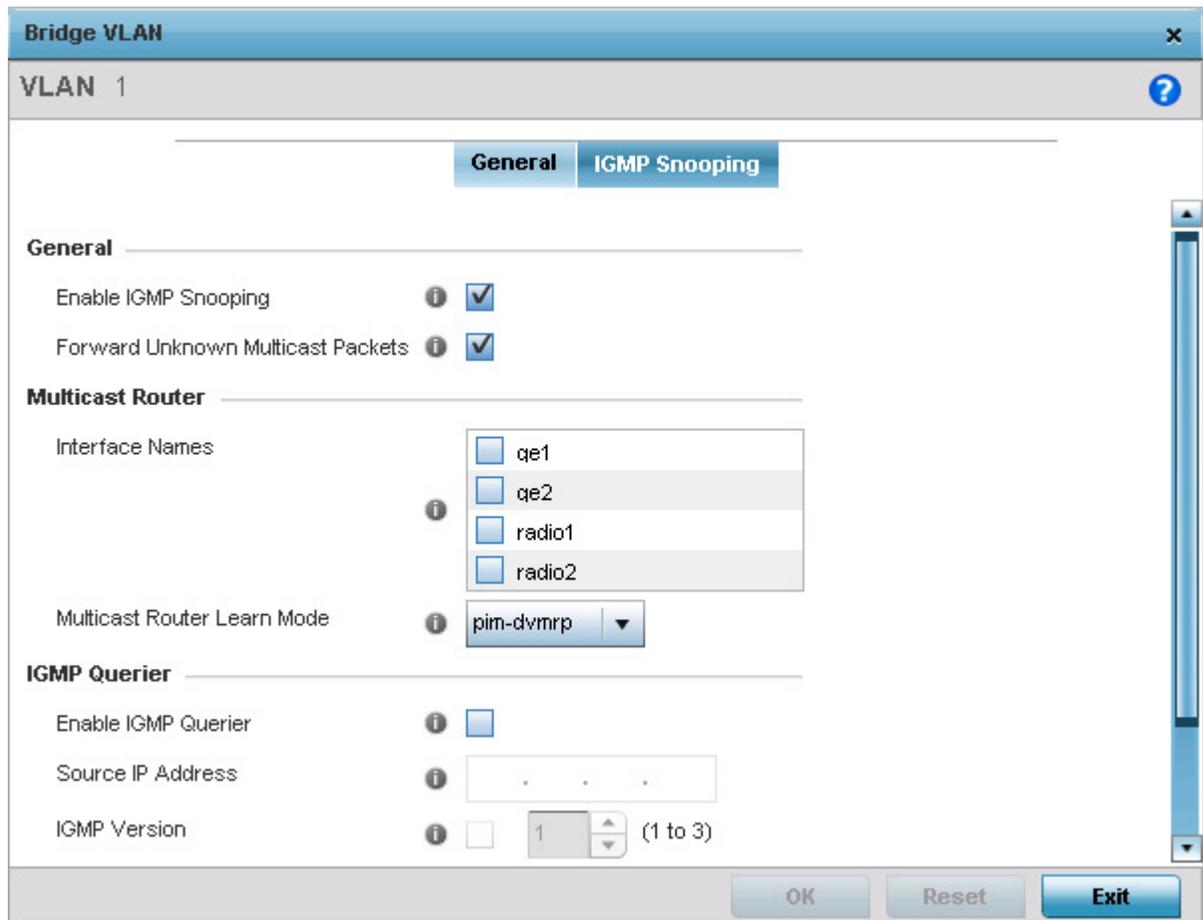
**NOTE:** If creating a mesh connection between two access points in Standalone AP mode, *Tunnel* must be selected as the bridging mode to successfully create the mesh link between the two access points.

13. Select **Tunnel Over Level 2** to tunnel extended VLAN traffic over level 2 links.
14. Set or override the following **Layer 2 Firewall** parameters:

<b>Trust ARP Responses</b>	Select this option to use trusted ARP packets to update the DHCP snoop table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default.
<b>Trust DHCP Responses</b>	Select this option to use DHCP packets from a DHCP server as trusted and permissible within the network. DHCP packets are used to update the DHCP snoop table to prevent IP spoof attacks. This feature is disabled by default.

<b>Edge VLAN Mode</b>	Select this option to enable edge VLAN mode. When selected, the IP address in the VLAN is not used for normal operations, as its now designated to isolate devices and prevent connectivity. This feature is enabled by default.
-----------------------	--

15. Click the **IGMP Snooping** tab to set or override the IGMP snooping configuration.



**Figure 5-169** Device Overrides - Network Bridge VLAN - IGMP Snooping screen

16. Set the following parameters to configure **IGMP Snooping** values:

<b>Enable IGMP Snooping</b>	Select this option to enable IGMP snooping. If disabled, snooping on this bridge VLAN is disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden.
<b>Forward Unknown Multicast Packets</b>	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the <i>Unknown Multicast Forward</i> feature is also disabled for the selected VLANs. This settings is enabled by default.

17. Set the following parameters for **Multicast Router** configuration:

<b>Interface Name</b>	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
<b>Multicast Router Learn Mode</b>	Set the learning mode to either <i>pim-dvmrp</i> or <i>static</i> .

18. Set the following parameters for **IGMP Querier** configuration:

<b>Enable IGMP Querier</b>	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then forwarded on that port.
<b>Source IP Address</b>	Define an IP address applied as the source address in the IGMP query packet. This address is used as the default VLAN querier IP address.
<b>IGMP Version</b>	Use the spinner control to set the IGMP version compatibility to IGMP version 1, 2 or 3. The default IGMP version is 3.
<b>Maximum Response Time</b>	Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
<b>Other Querier Time Expiry</b>	Specify an interval in either <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

19. Select the **OK** button to save the changes and overrides to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

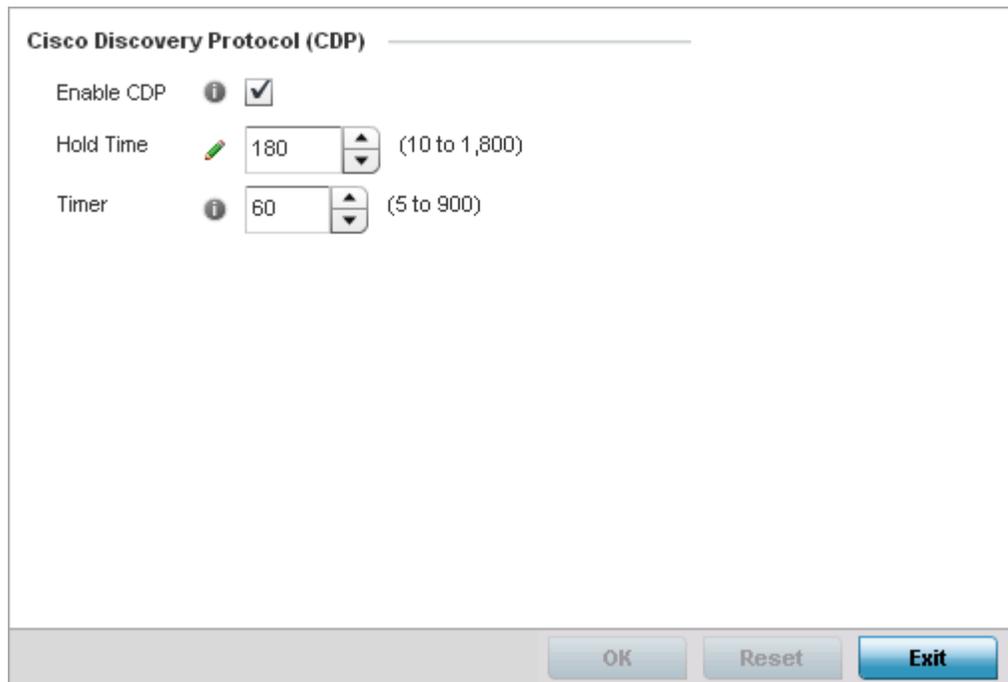
#### 5.4.5.4.11 Overriding a Cisco Discovery Protocol Configuration

##### ► *Overriding the Network Configuration*

The *Cisco Discovery Protocol* (CDP) is a proprietary data link layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To override a profile's CDP configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Cisco Discovery Protocol**.



**Figure 5-170** Cisco Discovery Protocol (CDP) screen

6. Enable/disable CDP and set the following timer settings:

<b>Enable CDP</b>	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default.
<b>Hold Time</b>	Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 180.
<b>Timer</b>	Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds.

7. Select the **OK** button located at the bottom right of the screen to save the changes and overrides to the CDP configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.120 Overriding a Link Layer Discovery Protocol Configuration

##### ► *Overriding the Network Configuration*

The *Link Layer Discovery Protocol* (LLDP) provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one *Link Layer Discovery Protocol Data Unit* (LLDP PDU). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To override a profile's LLDP configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.

3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Link Layer Discovery Protocol**.

**Link Layer Discovery Protocol (LLDP)**

Enable LLDP

Hold Time  (10 to 1,800)

Timer  (5 to 900)

Inventory Management Discovery

Extended Power via MDI Discovery

OK Reset Exit

**Figure 5-171** Link Layer Discovery Protocol (LLDP) screen

6. Set the following LLDP parameters for the profile configuration:

<b>Enable LLDP</b>	Select this option to enable LLDP on the access point. LLDP is enabled by default. When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them.
<b>Hold Time</b>	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds.
<b>Timer</b>	Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds.
<b>Inventory Management Discovery</b>	Select this option to include LLDP-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.
<b>Extended Power via MDI Discovery</b>	Select this option to include LLDP-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default.

7. Select the **OK** button to save the changes and overrides to the LLDP configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.130 Overriding a Miscellaneous Network Configuration

##### ► *Overriding the Network Configuration*

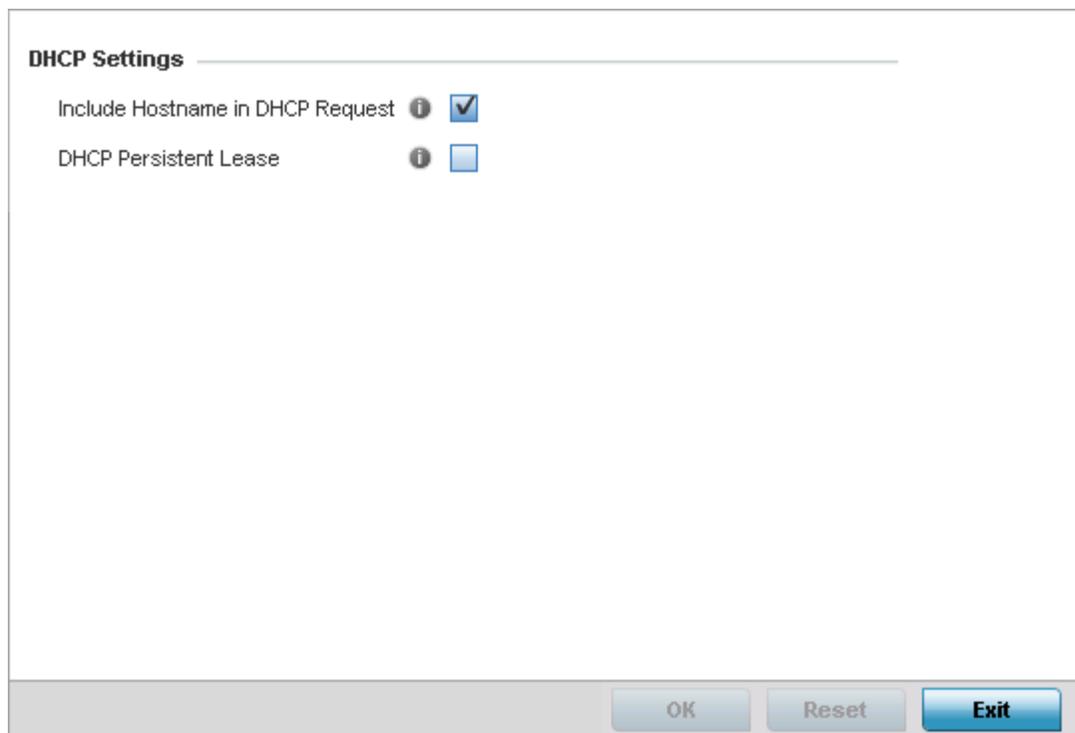
An access point profile can be configured to include a hostname in a DHCP lease for a requesting device and its profile. This helps an administrator track the leased DHCP IP address by hostname for a device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include a hostnames in DHCP request:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand side of the UI.
4. Select **Network** to expand its sub menu options.
5. Select **Miscellaneous**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.



**Figure 5-172** Device Overrides - Network Miscellaneous screen

6. Select the **Include Hostname in DHCP Request** option to include a hostname in a DHCP lease for a requesting device. This feature is enabled by default.
7. Select the **DHCP Persistent Lease** option to retain the last DHCP lease used across a reboot if the access point's designated DHCP server is unavailable. This feature is enabled by default.
8. Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.4.14 Overriding Alias Configuration

##### ► *Overriding the Network Configuration*

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An *alias* enables an administrator to define a configuration item, such as a hostname, as an *alias* once and use the defined *alias* across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the *alias* used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration > Network > Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from **Configuration > Devices > System Profile > Network > Alias** screen. These aliases are available for use to a specific group of wireless controllers or access points. Alias values defined in this profile override alias values defined within global aliases.
- *RF Domain aliases* are defined from **Configuration > Devices > RF Domain > Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an *Network Alias* defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the Network Alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the Network Alias works with the 172.16.10.0/24 network. Existing ACLs using this Network Alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias can be classified as:

- *Network Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

#### 5.4.5.4.15 Network Basic Alias

##### ► *Overriding Alias Configuration*

A *basic alias* is a set of configurations that consist of VLAN, host, network and address range alias configurations. VLAN configuration is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

A basic alias configuration can contain multiple instances for each of the five (5) alias types.

To override a basic alias configuration:

1. Select **Devices** from the **Configuration** tab.

2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand side of the UI.
4. Select **Network** to expand it and display its sub menus.
5. Select the **Alias** item, the **Basic Alias** screen displays.

**Figure 5-173** Network - Basic Alias screen

6. Select **+ Add Row** to define **VLAN Alias** settings.

Use the **VLAN Alias** field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

<b>Name</b>	If adding a new <i>VLAN Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>VLAN</b>	Use the spinner control to set a numeric VLAN from 1 - 4094.

A *VLAN alias* can be used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3

- Switchport
  - Wireless LANs
7. Select **+ Add Row** to define **Host Alias** settings.

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	Set the IP address of the host machine.

A *host alias* can be used to replace hostnames in the following locations:

- IP Firewall Rules
  - DHCP
8. Select **+ Add Row** to define **Address Range Alias** settings.

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

<b>Name</b>	If adding a new <i>Address Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Start IP</b>	Set a starting IP address used with a range of addresses utilized with the address range alias.
<b>End IP</b>	Set a ending IP address used with a range of addresses utilized with the address range alias.

An *address range alias* can be used to replace an IP address range in IP firewall rules.

9. Select **+ Add Row** to define **Network Alias** settings.

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	Provide a network address in the form of <i>host/mask</i> .

A *network alias* can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

10. Select **+ Add Row** to define **String Alias** settings.

Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.

<b>Name</b>	If adding a new <i>String Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	Provide a string value to use in the alias.

A *string alias* can be used to replace domain name strings in DHCP.

11. Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

#### 5.4.5.4.16 Network Group Alias

##### ► *Overriding Alias Configuration*

A *network group alias* is a set of configurations that consist of host and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20. Host configuration is in the form of single IP address, 192.168.10.23.

A *network group alias* can contain multiple definitions for host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) Network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

A *network group alias* is used in IP firewall rules to substitute hosts, subnets and IP address ranges:

To edit or delete a network alias configuration:

1. Select **Devices** from the **Configuration** tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand side of the UI.
4. Select **Network** to expand it and display its sub menus.
5. Select the **Alias** item, the **Basic Alias** screen displays.
6. Select the **Network Group Alias** tab.



Name \$NGA\_01 ?

Host

1.2.3.4  
2.3.4.5  
3.4.5.6

Network    /

192.168.13.0/24

Range

Start IP	End IP	
1.2.3.4	4.3.2.1	<input type="button" value="🗑"/>
		<input type="button" value="🗑"/>

**Figure 5-175** Network - Alias - Network Group Alias Add screen

8. If adding a new **Network Group Alias**, provide it a name of up to 32 characters.



**NOTE:** The **Network Group Alias Name** always starts with a dollar sign (\$).

9. Define the following network group alias parameters:

<b>Host</b>	Specify the host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
<b>Network</b>	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

10. Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.
11. Select **OK** when completed to update the network group alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.4.5.4.17 Network Service Alias

#### ► *Overriding Alias Configuration*

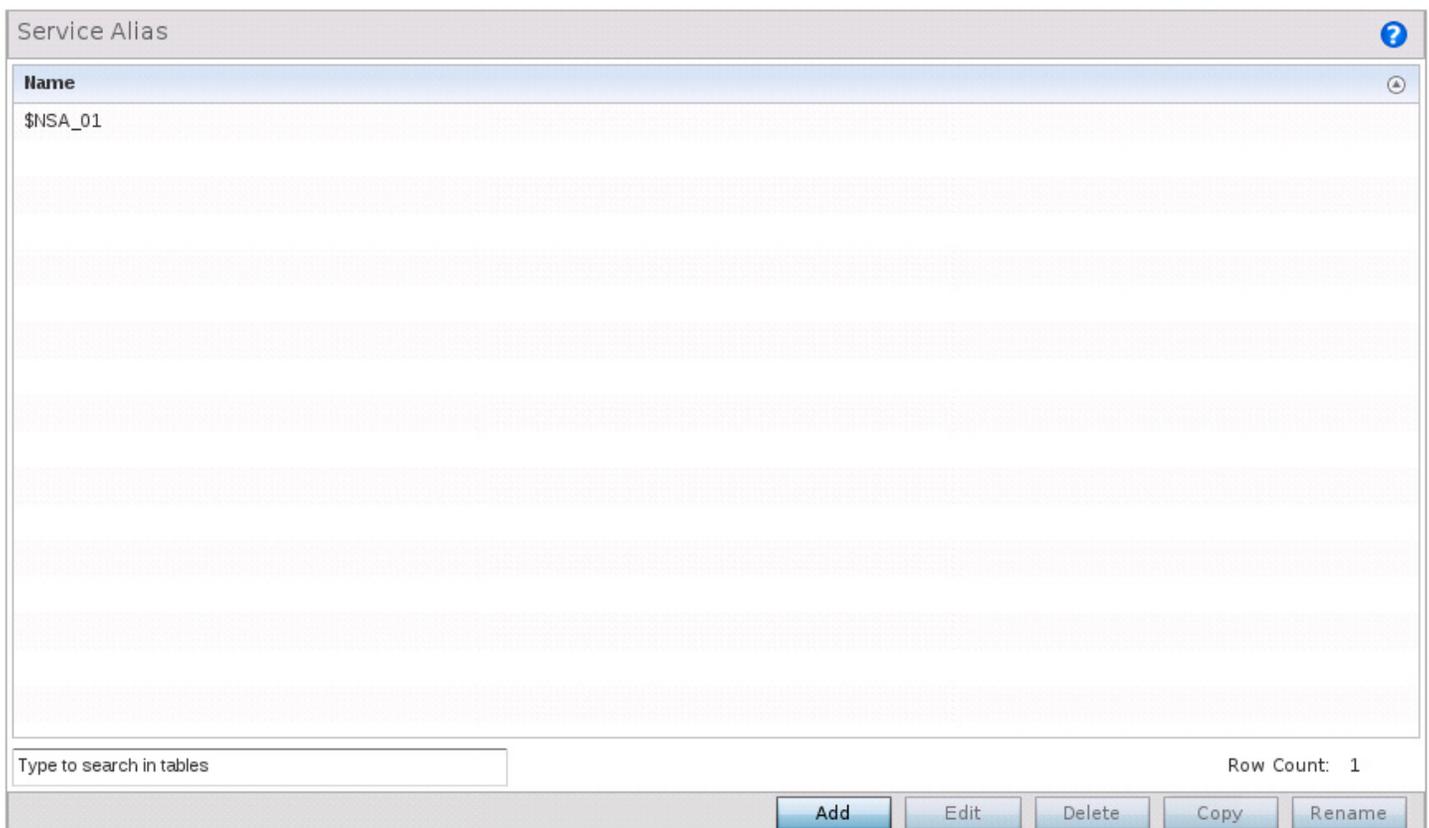
*Network Service Alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per *Network Service Alias*.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

A *network service alias* can be used in IP firewall rules to substitute protocols and ports:

To edit or delete a service alias configuration:

1. Select **Devices** from the **Configuration** tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand side of the UI.
4. Select **Network** to expand it and display its sub menus.
5. Select the **Alias** item, the **Basic Alias** screen displays.
6. Select the **Network Service Alias** tab.



**Figure 5-176** Network - Alias - Network Service Alias screen

7. Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Service Alias**.

Name \$NSA\_01 ?

Entry

Protocol	Source Port(Low and High)	Destination Port(Low and High)	
* igmp	2	Enter R	
6	80-92	80	

+ Add Row

▶ OK
Reset
Exit

**Figure 5-177** Network - Alias - Network Service Alias Add screen

8. If adding a new **Network Service Alias**, provide it a name up to 32 characters.



**NOTE:** The **Network Service Alias Name** always starts with a dollar sign (\$).

9. Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

<b>Protocol</b>	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from <i>eigrp</i> , <i>gre</i> , <i>icmp</i> , <i>igmp</i> , <i>ip</i> , <i>rrp</i> , <i>igp</i> , <i>ospf</i> , <i>tcp</i> and <i>udp</i> . Select <i>other</i> if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
<b>Source Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
<b>Destination Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

10. Select **OK** when completed to update the network service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 5.4.5.5 Overriding a Security Configuration

#### ▶ Device Overrides

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy applied. If an existing firewall, client role or NAT policy is unavailable create the required security policy configuration. Once created, a configuration can have an override applied as needed to meet the changing data protection requirements of a

device's deployed environment. However, in doing so this device must now be managed separately from the profile configuration shared by other identical models within the network.

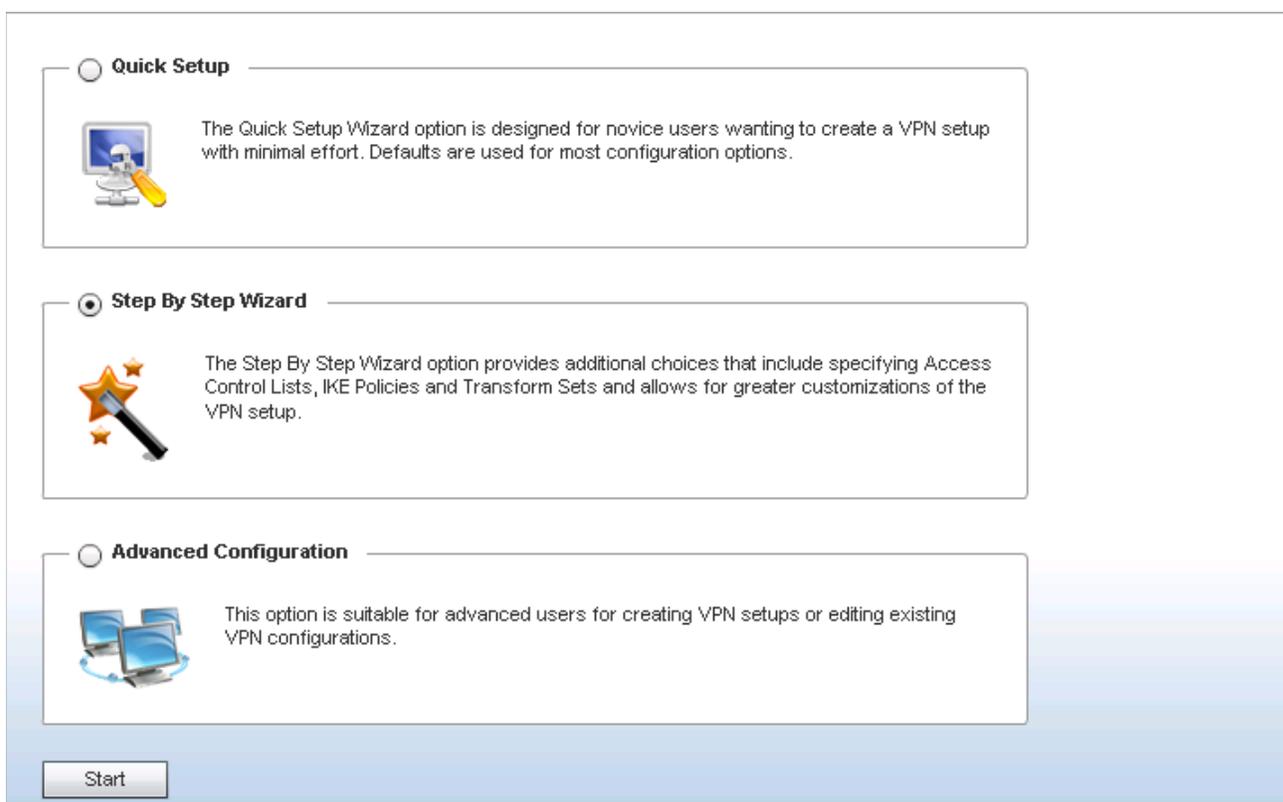
For more information on applying an override to an existing device profile, refer to the following sections:

- [Overriding General Security Settings](#)
- [Overriding a Certificate Revocation List \(CRL\) Configuration](#)
- [Overriding a Profile's NAT Configuration](#)

### 5.4.5.1 Overriding VPN Configuration using Wizards

#### ► [Overriding a Security Configuration](#)

VPN can be overridden by using either the inbuilt wizards or by manually configuring the required parameters. This section describes how to use the inbuilt wizards to override the VPN parameters. The user interface provides two (2) wizards that provide different levels of configuration. The following screen displays:



**Figure 5-178** Security Configuration Wizard screen

The following options are available:

- **Quick Setup Wizard** – Use this wizard to setup basic VPN Tunnel on the device. This wizard is aimed at novice users and enables them to setup a basic VPN with minimum effort. This wizard uses default values for most of the parameters.
- **Step By Step Wizard** – Use this wizard to setup a VPN Tunnel step by step. This wizard is aimed at intermediate users who require the ability to customize some of the parameters.
- **Advanced Configuration** – Use this option to configure the VPN parameters manually.

Click the **Start** button to display the next screen for the wizards or when **Advanced Configuration** is selected, to display the VPN screen.

### 5.4.5.2 Quick Setup Wizard

#### ► *Overriding General Security Settings*

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

**Figure 5-179** VPN Quick Setup Wizard

1. Provide the following information to configure a VPN tunnel:

<b>Tunnel Name</b>	Provide a name for the tunnel. Tunnel name must be such that it easily identifies the tunnel uniquely.
<b>Tunnel Type</b>	Configure the tunnel type as one of the following: <ul style="list-style-type: none"> <li>• <i>Site-to-Site</i> – Provides a secured connection between two sites</li> <li>• <i>Remote Access</i> – Provides access to a network to remote devices.</li> </ul>

<b>Select Interface</b>	Configure the interface for creating the tunnel. The following options are available: <ul style="list-style-type: none"> <li>• <i>VLAN</i> – Configures the tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number.</li> <li>• <i>WWLAN</i> – Configures the tunnel over the WWLAN interface.</li> <li>• <i>PPPoE</i> – Configures the tunnel over the PPPoE interface.</li> </ul>
<b>Traffic Selector (ACL)</b>	Configure ACLs that manage the traffic passing through the VPN Tunnel. <ul style="list-style-type: none"> <li>• <i>Source</i> – Provide the source network along with its mask</li> <li>• <i>Destination</i> – Provide the destination network along with its mask.</li> </ul>
<b>Peer</b>	Configures the peer for this tunnel. The peer device can be specified either by its hostname or by its IP address.
<b>Authentication</b>	Configure the authentication used to identify peers. The following can be configured: <ul style="list-style-type: none"> <li>• <i>Certificate</i> – Use a certificate to authenticate</li> <li>• <i>Pre-Shared Key</i> – Use a pre-shared key to authenticate.</li> </ul>
<b>Local Identity</b>	Configure the local identity used with peer configuration for an IKE exchange with the target VPN IPSec peer. Options include <i>IP Address</i> , <i>Distinguished Name</i> , <i>FQDN</i> , <i>email</i> and <i>string</i> . The default setting is string.
<b>Remote Identity</b>	Configure the access point remote identifier for an IKE exchange with the target VPN IPSec peer. Options include <i>IP Address</i> , <i>Distinguished Name</i> , <i>FQDN</i> , <i>email</i> and <i>string</i> . The default setting is string.
<b>IKE Policy</b>	Configure the IKE policy to use. IKE is used to exchange authentication keys. Select from one of the following: <ul style="list-style-type: none"> <li>• <i>All</i> – Uses any IKE policy.</li> <li>• <i>IKE1</i> – Uses IKE 1 only</li> <li>• <i>IKE2</i> – Uses IKE 2 only</li> </ul>
<b>Transform Set</b>	Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down menu.

2. Click the **Save** button to save the VPN Tunnel configuration. To exit without saving, click **Cancel**.

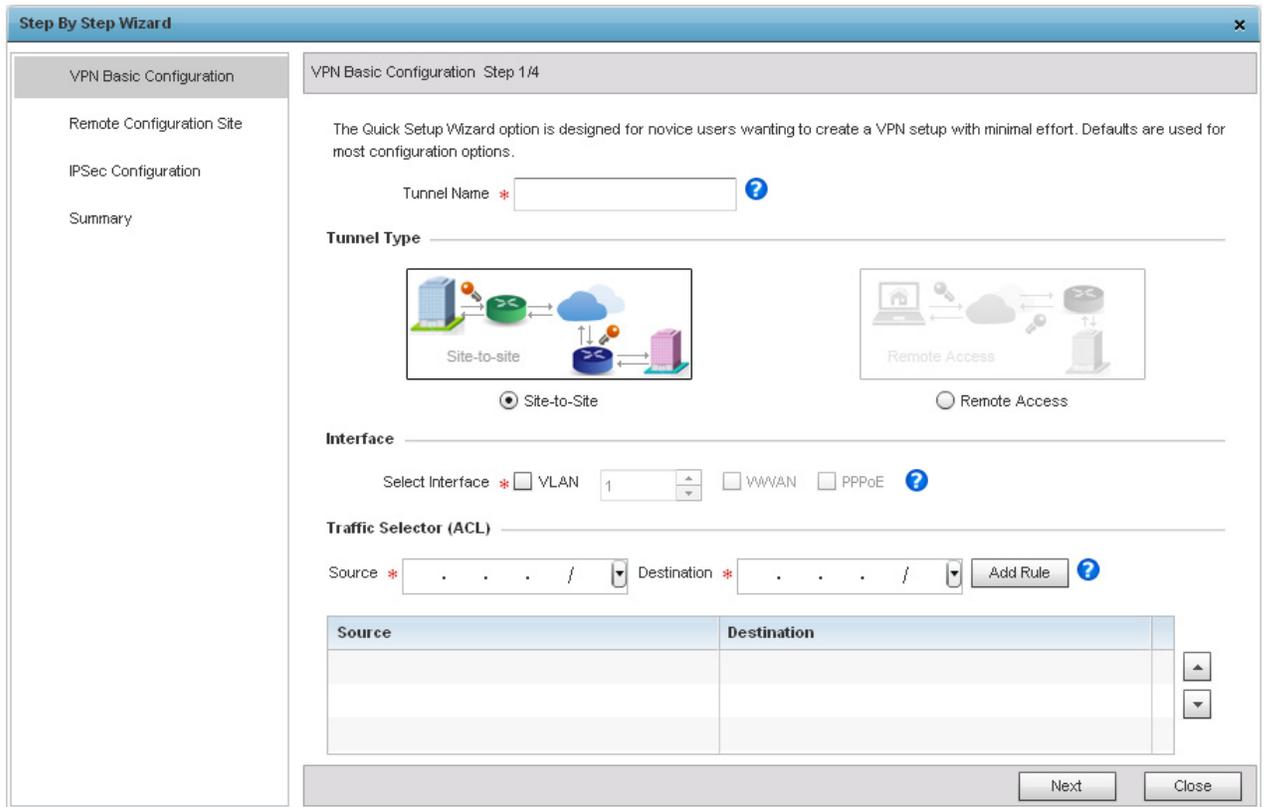
### 5.4.5.5.3 Step By Step Wizard

#### ► *Overriding General Security Settings*

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

The Step-By-Step wizard creates a VPN connection with more manual configuration than the Quick Setup Wizard. Use this wizard to manually configure *Access Control Lists*, *IKE Policy*, and *Transform Sets* to customize the VPN Tunnel.

1. Select the **Step-By-Step Wizard** option from the VPN screen.
2. Click the **Start** button. The following screen displays:



**Figure 5-180** VPN Step-By-Step Wizard - Step 1

3. Define the following:

<b>Tunnel Name</b>	Provide a name for the tunnel in the <i>Tunnel Name</i> field.
<b>Tunnel Type</b>	Select the tunnel type being created. Two types of tunnels can be created. <i>Site to Site</i> is used to create a tunnel between two remote sites as indicated in the image. <i>Remote Access</i> is used to create a tunnel between an user device and a network as indicated in the image.
<b>Interface</b>	Select the interface to use. Interface can be a <i>Virtual LAN (VLAN)</i> or <i>WWAN</i> or <i>PPPoE</i> depending on the interfaces available on the device.
<b>Traffic Selector (ACL)</b>	This field creates the <i>Access Control List (ACL)</i> that is used to control who uses the network. Provide the <i>Source</i> and <i>Destination</i> IP address ranges with their net mask. Click the <i>Add Rule</i> button to add the rule into the ACL.

4. Click the **Next** button to go to Step 2.

**Figure 5-181** VPN Step-By-Step Wizard - Step 2

5. In *Step 2* screen, configure the following parameters:

<b>Peer</b>	Select the type of peer for this device when forming a tunnel. Peer information can be either <i>IP Address</i> or <i>Host Name</i> . Provide the IP address or the hostname of the peer device.
<b>Authentication</b>	Configure how the devices authenticate with each other. <ul style="list-style-type: none"> <li>• <i>Certificate</i> – The devices use certificates to validate credentials.</li> <li>• <i>Pre-Shared Key</i> – The devices use pre-shared key to authenticate.</li> </ul>
<b>Local Identity</b>	Configure the local identity for the VPN Tunnel. <ul style="list-style-type: none"> <li>• <i>IP Address</i> – The local identity is an IP address.</li> <li>• <i>FQDN</i> – The local identity is a <i>Fully Qualified Domain Name (FQDN)</i>.</li> <li>• <i>Email</i> – The local identity is an E-mail address.</li> </ul>
<b>Remote Identity</b>	Configure the remote identity for the VPN Tunnel. <ul style="list-style-type: none"> <li>• <i>IP Address</i> – The remote identity is an IP address.</li> <li>• <i>FQDN</i> – The remote identity is a <i>Fully Qualified Domain Name (FQDN)</i>.</li> <li>• <i>Email</i> – The remote identity is an E-mail address.</li> </ul>
<b>IKE Policy</b>	Configure the IKE policy to use when creating this VPN Tunnel. The following options are available: <ul style="list-style-type: none"> <li>• <i>Use Default</i> – Click this option to use the default IKE profiles. Select one of <i>ike1-default</i> or <i>ike2-default</i>.</li> <li>• <i>Create new Policy</i> – Click this option to create a new IKE policy.</li> </ul>

6. Click the **Add Peer** button to add the Tunnel peer information into the *Peer(s)* table. This table lists all the peers configured for the VPN Tunnel.
7. Click the **Next** button to go to the next configuration screen. Use the **Back** button to go to the previous step.

The screenshot shows a 'Step By Step Wizard' window titled 'IPSec Configuration Step 3/4'. On the left, a navigation pane shows 'VPN Basic Configuration' and 'Remote Configuration Site' as completed steps, and 'IPSec Configuration' as the current step. The main area contains the following configuration options:

- Transform Set:** default (dropdown menu)
- Encryption:** esp-null (dropdown menu)
- Authentication:** md5-hmac (dropdown menu)
- Mode:** Tunnel (selected radio button), Transport (unselected radio button)
- Security Association:**
  - Lifetime: 3600 (spinner box) (Seconds 500 to 2147483646)
  - Data: 4608000 (spinner box) (Data-based IPsec security association lifetime. 500 to 2147483646)

At the bottom right, there are 'Next' and 'Close' buttons.

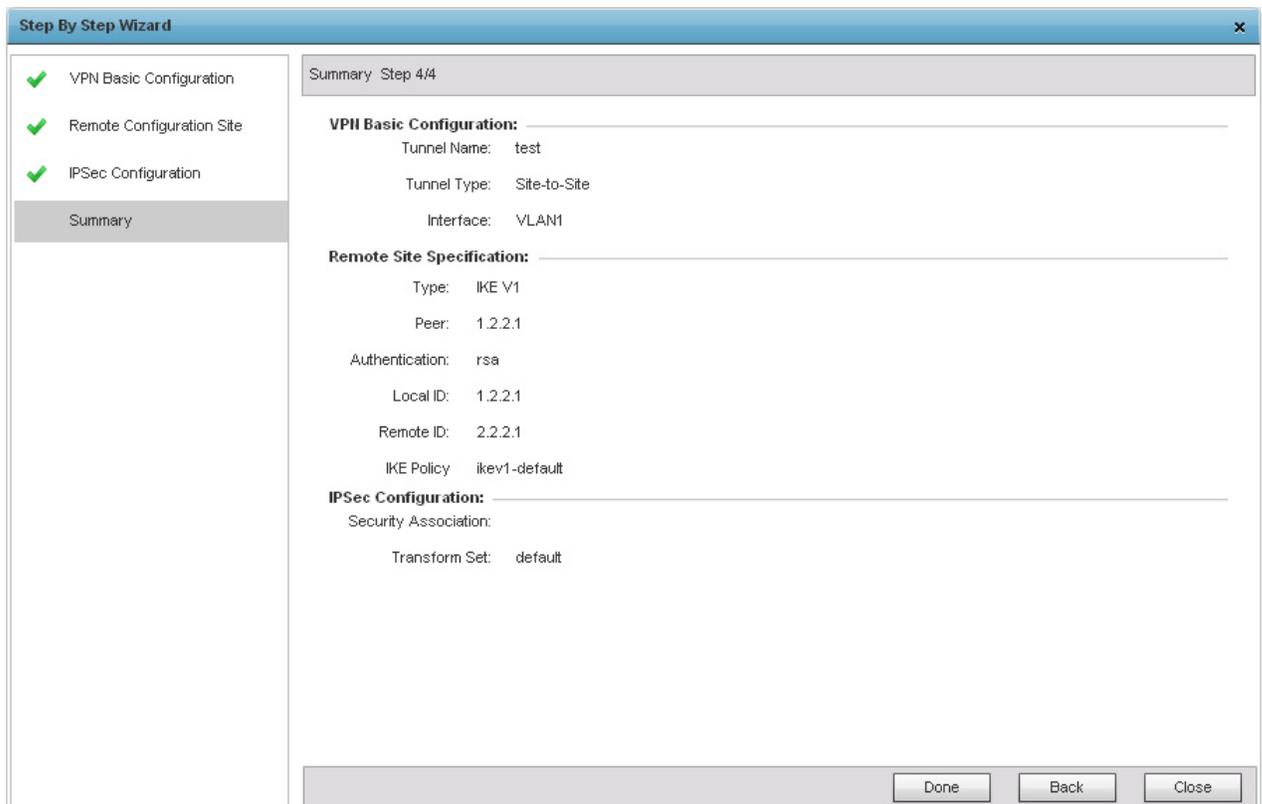
**Figure 5-182** VPN Step-By-Step Wizard - Step 3

8. Configure the following IPsec parameters:

<b>Transform Set</b>	<p>Transform set is a set of configurations exchanged for creating the VPN tunnel and impose a security policy. The transform set is comprised of the following:</p> <ul style="list-style-type: none"> <li>• <i>Encryption</i> – The encryption to use for creating the tunnel.</li> <li>• <i>Authentication</i> – The authentication used to identify tunnel peers</li> <li>• <i>Mode</i> – The mode of the tunnel. This is how the tunnel will operate.</li> </ul> <p>From the drop-down, select any pre-configured Transform Set or click the <i>Create New Policy</i> to create a new transform set.</p>
<b>Encryption</b>	<p>This field is enabled when <i>Create New Policy</i> is selected in <i>Transform Set</i> field. This is the encryption that is used on data traversing through the tunnel. Select from <i>esp-null</i>, <i>des</i>, <i>3des</i>, <i>aes</i>, <i>aes-192</i> and <i>aes-256</i> algorithms.</p>
<b>Authentication</b>	<p>This field is enabled when <i>Create New Policy</i> is selected in <i>Transform Set</i> field. This is the method peers authenticate as the source of the packet to other peers after a VPN Tunnel has been created. Select from <i>MD5</i> or <i>SHA</i>.</p>

<b>Mode</b>	<p>This field is enabled when <i>Create New Policy</i> is selected in <i>Transform Set</i> field. The mode indicates how packets are transported through the tunnel.</p> <ul style="list-style-type: none"> <li>• <i>Tunnel</i> – Use this mode when the tunnel is between two routers or servers.</li> <li>• <i>Transport</i> – Use this mode when the tunnel is created between a client and a server.</li> </ul>
<b>Security Association</b>	<p>Configures the lifetime of a <i>security association</i> (SA). Keys and SAs should be periodically renewed to maintain security of the tunnel.</p> <ul style="list-style-type: none"> <li>• <i>Lifetime</i> – Duration in seconds after which the keys should be changed. Set a value in from 500 - 2,147,413,646 seconds.</li> <li>• <i>Data</i> – The key is changed after this quantity of data has be encrypted/decrypted. Set a value from 500 - 2,147,413,646 KBs.</li> </ul>

9. Click the **Next** button to go to the next configuration screen. Use the **Back** button to go to the previous step.



**Figure 5-183** VPN Step-By-Step Wizard - Step 4

10. Review the configuration and click the **Done** button to create the VPN tunnel. Use the **Back** button to go back to previous screen for making modifications to the configuration. Click **Close** to close the wizard without creating a VPN Tunnel.

#### 5.4.5.5.4 Overriding Auto IPsec Tunnel Settings

##### ► *Overriding a Security Configuration*

IPsec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.

3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Security** to expand its sub menu options.
5. Select **Auto IPSec Tunnel** to configure its parameters.

The screenshot shows a configuration window titled "Settings" with the following fields and controls:

- Group ID:** A text input field.
- Authentication Type:** A dropdown menu.
- Authentication Key:** A text input field.
- IKE Version:** A dropdown menu with "ikev2" selected.
- Enable NAT after IPSec:** A checkbox that is currently unchecked.
- Use Unique ID:** A checkbox that is currently unchecked.

At the bottom right of the window are two buttons: "OK" and "Reset".

**Figure 5-184** Device Overrides - Security – Auto IPSec Tunnel screen

6. Refer to the following table to override the Auto IPSec tunnel settings:

<b>Group ID</b>	Configure the ID string used for IKE authentication. String length can be between 1-64 characters
<b>Authentication Type</b>	Set the IPSec Authentication Type. Options include <i>PSK</i> (Pre Shared Key) or <i>rsa</i> .
<b>Authentication Key</b>	Set the common key for authentication between the remote tunnel peer. Key length is between 8-21 characters
<b>IKE Version</b>	Configure the IKE version to use. The available options are <i>ikev1-main</i> , <i>ikev1-aggr</i> and <i>ikev2</i> .
<b>Enable NAT after IPSec</b>	Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels.
<b>Use Unique ID</b>	In scenarios where different access points behind different NAT boxes/routers have the same IP address, it is not possible to create a tunnel between the wireless controller and access point, as the wireless controller fails to identify the access point uniquely. When selected, each access point behind a same NAT box/router will have an unique ID which is used to create the VPN tunnel.

7. Select **OK** to save the updates made to the **Auto IPSec Tunnel** screen. Selecting **Reset** reverts the screen to its last saved configuration.

### 5.4.5.5 Overriding General Security Settings

#### ► *Overriding a Security Configuration*

A profile can leverage existing firewall, wireless client role and WIPS policies and configurations and apply them to the configuration. This affords a profile a truly unique combination of data protection policies. However, as deployment requirements arise, an individual access point may need some or all of its general security configuration overridden from that applied in the profile.

To define a profile's security settings and overrides:

1. Select **Devices** from the Configuration tab.

2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Security** to expand its sub menu options.
5. Select **Settings**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

The screenshot shows the 'General' section of the Security Settings screen. It contains three configuration items:

- Firewall Policy:** A dropdown menu currently set to 'default'. To its right are two icons: a green plus sign in a square and a gear icon.
- Wireless Client Role Policy:** A dropdown menu that is currently empty. To its right are the same two icons: a green plus sign in a square and a gear icon.
- WEP Shared Key Authentication:** A checkbox that is currently unchecked.

At the bottom of the screen, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 5-185** Device Overrides - Security Settings screen

6. Refer to the General field to assign or override the following:

<b>Firewall Policy</b>	Select the firewall policy used by devices with this profile. Use the icons next to this field to create or add new firewall policies.
<b>Wireless Client Role Policy</b>	Select the Wireless Client Role Policy used by devices with this profile. Use the icons next to this field to create or add new role policies.
<b>WEP Shared Key Authentication</b>	Select this option to require devices using this profile to use a WEP key to access the network using this profile. Clients without Motorola Solutions adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

7. Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

### 5.4.5.5.6 Overriding a Certificate Revocation List (CRL) Configuration

#### ► *Overriding a Security Configuration*

A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the *certificate authority* (CA) had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

To define a Certificate Revocation configuration or override:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Security** to expand its sub menu options.
5. Select **Certificate Revocation**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

**Certificate Revocation List (CRL) Update Interval**

Trustpoint Name	URL	Hours	
 trustpoint1	 www.trustpoint.com	 1	 



**Figure 5-186** Device Overrides - Certificate Revocation screen

6. Select the **+ Add Row** button to add a column within the *Certificate Revocation List* (CRL) Update Interval table to quarantine certificates from use in the network.

Additionally, a certificate can be placed on hold for a user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

7. Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.
8. Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.

9. Use the spinner control within the **Hours** field to specify an interval (in hours) after which the access point copies a CRL file from an external server and associates it with a trustpoint.
10. Select **OK** to save the changes and overrides made within the **Certificate Revocation** screen. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.7 Overriding a Profile's NAT Configuration

##### ▶ *Overriding a Security Configuration*

*Network Address Translation* (NAT) is a technique to modify network address information within IP packet headers in transit across a traffic routing device. This enables mapping one IP address to another to protect network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments, NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT provides outbound Internet access to wired and wireless hosts. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows the access point to translate one or more private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To define a NAT configuration or override that can be applied to a profile:

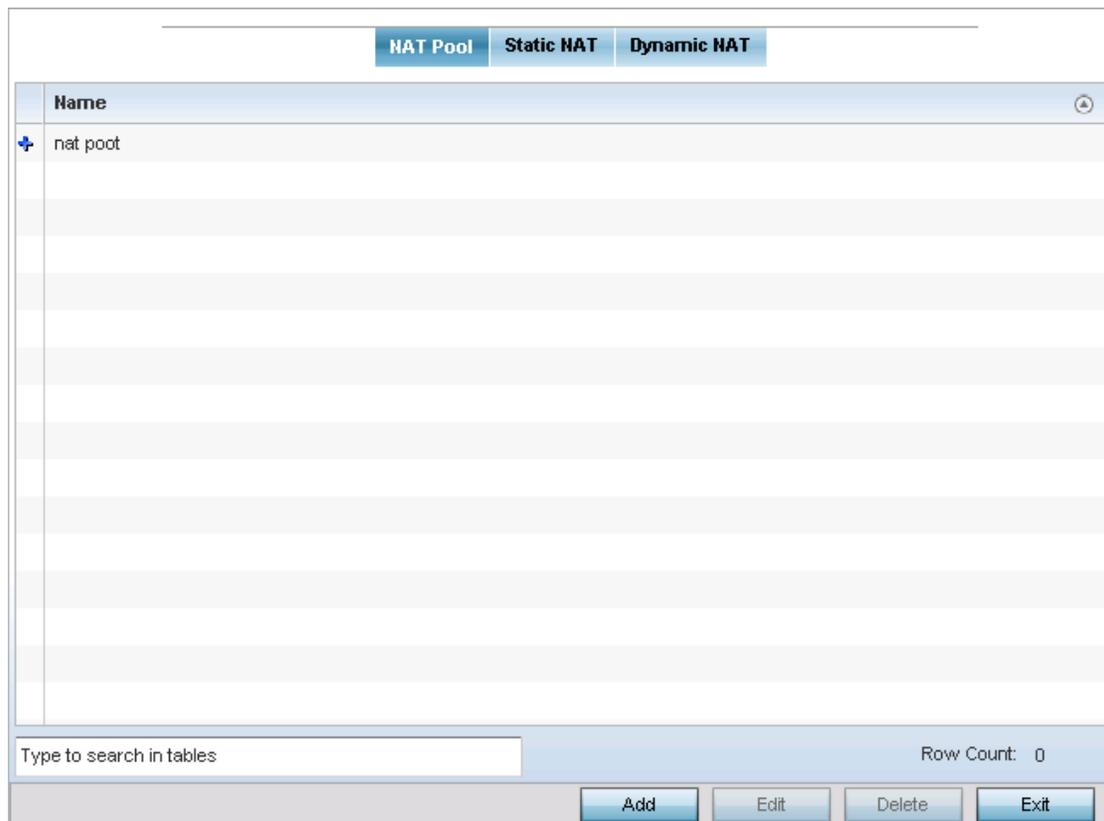
1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Security** to expand its sub menu options.
5. Select **NAT**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

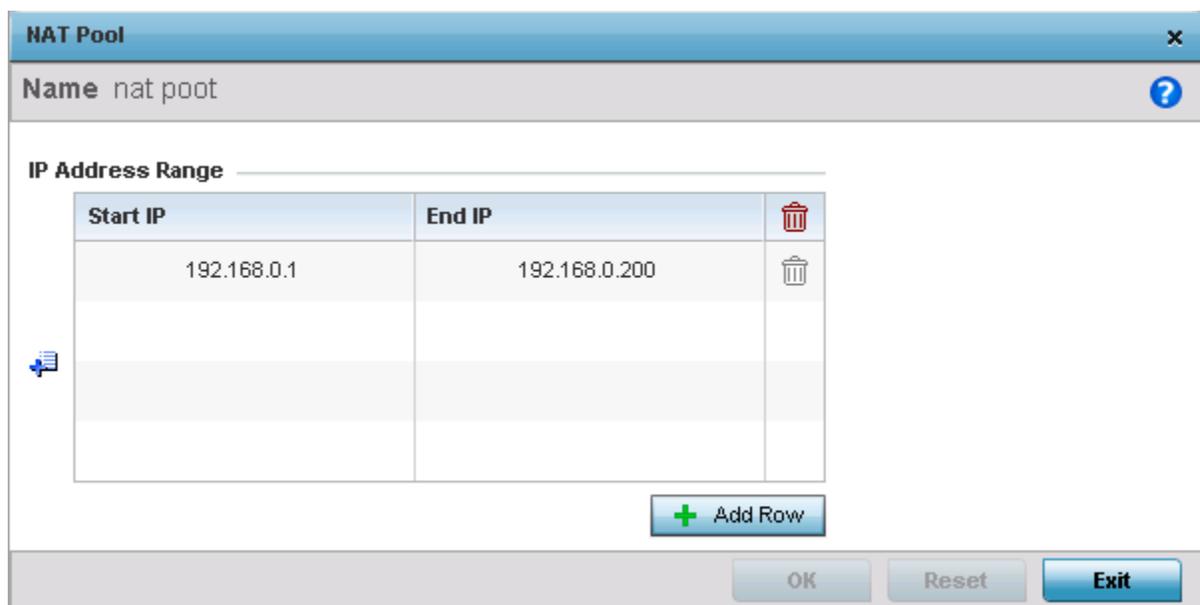
---

---



**Figure 5-187** Device Overrides - NAT Pool screen

6. The **NAT Pool** tab displays by default. The NAT Pool screen lists those NAT policies created thus far. Any of these policies can be selected and applied to a profile.
7. Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify or override the attributes of an existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.



**Figure 5-188** Device Overrides - Security - NAT Pool screen



**Figure 5-190** Device Overrides - Add NAT Source screen

12. Define the following **Source NAT** parameters:

<b>Protocol</b>	Select the protocol for use with static translation. <i>TCP</i> , <i>UDP</i> and <i>Any</i> are the available options. <i>Transmission Control Protocol</i> (TCP) is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The <i>User Datagram Protocol</i> (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is <i>Any</i> .
<b>Source IP</b>	Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Source Port</b>	Use the spinner control to set the local port number used at the (internal) end of the static NAT configuration. The default value is port 1.
<b>NAT IP</b>	Enter the IP address of the matching packet to the specified value. The IP address modified can be either <i>source</i> or <i>destination</i> based on the direction specified.



**Figure 5-192** Device Overrides - Add Destination NAT screen

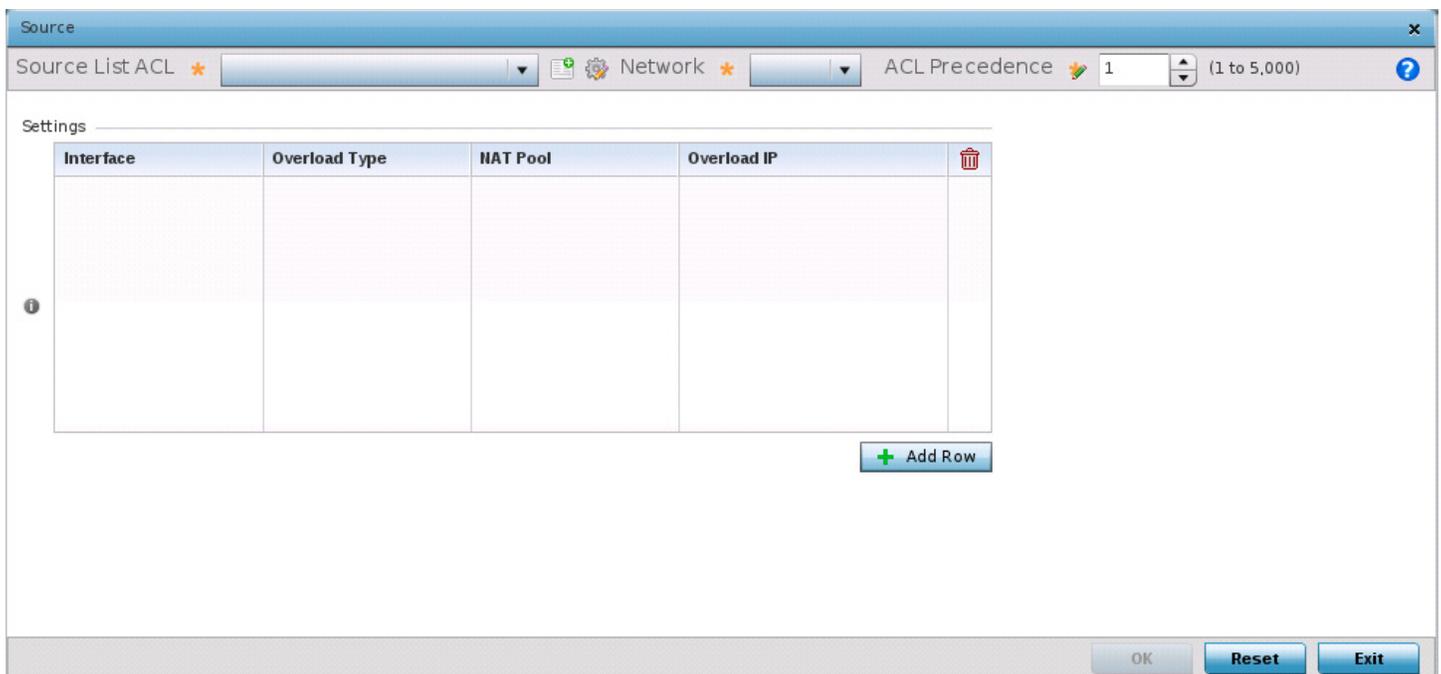
15. Set or override the following **Destination** configuration parameters:
16. Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

<b>Protocol</b>	Select the protocol for use with static translation. <i>TCP</i> , <i>UDP</i> and <i>Any</i> are available options. TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The <i>User Datagram Protocol</i> (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is <i>Any</i> .
<b>Destination IP</b>	Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Destination Port</b>	Use the spinner control to set the local port number used at the (source) end of the static NAT configuration. The default value is port 1.
<b>NAT IP</b>	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
<b>NAT Port</b>	Select this option and enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.



<b>Network</b>	Displays <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration.
<b>Interface</b>	Lists the VLAN (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.
<b>Overload Type</b>	Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . Interface IP Address is the default setting.
<b>NAT Pool</b>	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
<b>Overload IP</b>	If One Global IP Address is selected as the Overload Type, define an IP address used as a filter address for the IP ACL rule.
<b>ACL Precedence</b>	Lists the administrator assigned priority set for the listed source list ACL. The lower the value listed, the higher the priority assigned to this ACL rule.

20. Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify or override an existing configuration or **Delete** to permanently remove a configuration.



**Figure 5-194** Device Overrides - Security - NAT - Source ACL List screen

21. Set or override the following to define the **Dynamic NAT** configuration:

<b>Source List ACL</b>	Use the drop-down menu to select an ACL name to define the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access-list. These addresses (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.
<b>ACL Precedence</b>	Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to the ACL rule.

<b>Interface</b>	Select the VLAN (from 1 - 4094) or WWAN used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected adequately supports the intended network traffic within the NAT supported configuration.
<b>Overload Type</b>	Define the overload type utilized when Several internal addresses are NATed to only one or a few external addresses. Options include <i>NAT Pool</i> , <i>One Global Address and Interface IP Address</i> . Interface IP Address is the default setting.
<b>NAT Pool</b>	Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
<b>Overload IP</b>	If <i>One Global IP Address</i> is selected as the <i>Overload Type</i> , define an IP address used a filter address for the IP ACL rule.

22. Select **OK** to save the changes or overrides made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

### 5.4.5.8 Overriding the Profile's Bridge NAT Configuration

#### ► Profile Security Configuration

Use *Bridge NAT* to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.



**NOTE:** Bridge NAT supports single AP deployments only. This feature cannot be used in a branch deployment with multiple access points.

To define a Bridge NAT configuration that can be applied to a profile:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **Device Overrides** from the options on left-hand side of the UI.
4. Expand the **Security** menu and select **Bridge NAT**.



**Figure 5-196** Profile Security - Dynamic NAT screen

7. Select the **ACL** whose IP rules are applied to this policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.
8. Use the spinner to select the **ACL Precedence**. The lower the precedence value, the higher the priority assigned to this Dynamic NAT policy rule.
9. Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the Internet.

<b>Interface</b>	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN.
<b>NAT Pool</b>	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool.
<b>Overload IP</b>	Lists whether the single global address supporting numerous local addresses.
<b>Overload Type</b>	Displays the override type for this policy based forwarding rule.

10. Select **+ Add Row** to set the IP address range settings for the Bridge NAT configuration.

The screenshot shows a dialog box titled "Add Row" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Interface:** A radio button followed by a dropdown menu.
- VLAN ID:** A radio button followed by a text box containing "1" and up/down arrow buttons.
- Overload Type:** Three radio buttons: "NAT Pool", "One Global Address", and "Interface IP Address". The "Interface IP Address" option is selected.
- NAT pool:** A radio button followed by a dropdown menu showing "<none>".
- Overload IP:** A radio button followed by a text box with three dots (". . .").

At the bottom of the dialog are two buttons: "OK" and "Exit".

**Figure 5-197** Profile Security - Source Dynamic NAT screen - Add Row field

11. Select **OK** to save the changes made within the **Add Row** and **Dynamic NAT** screens. Select **Reset** to revert to the last saved configuration.

### 5.4.5.6 Overriding the Virtual Router Redundancy Protocol (VRRP) Configuration

#### ▶ *System Profile Configuration*

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available on an AP7131, and a router failure occurs, then the access point should act as a router and forward traffic on to its WAN link.

Define an external *Virtual Router Redundancy Protocol (VRRP)* configuration when router redundancy is required in a wireless network requiring high availability.

Central to the configuration of VRRP is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- *Responds to ARP requests*
- *Forwards packets with a destination link layer MAC address equal to the virtual router MAC address*
- *Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner*
- *Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true*

Those nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.



**NOTE:** VRRP support is available only on AP7131 model access point, and is not available on other models.

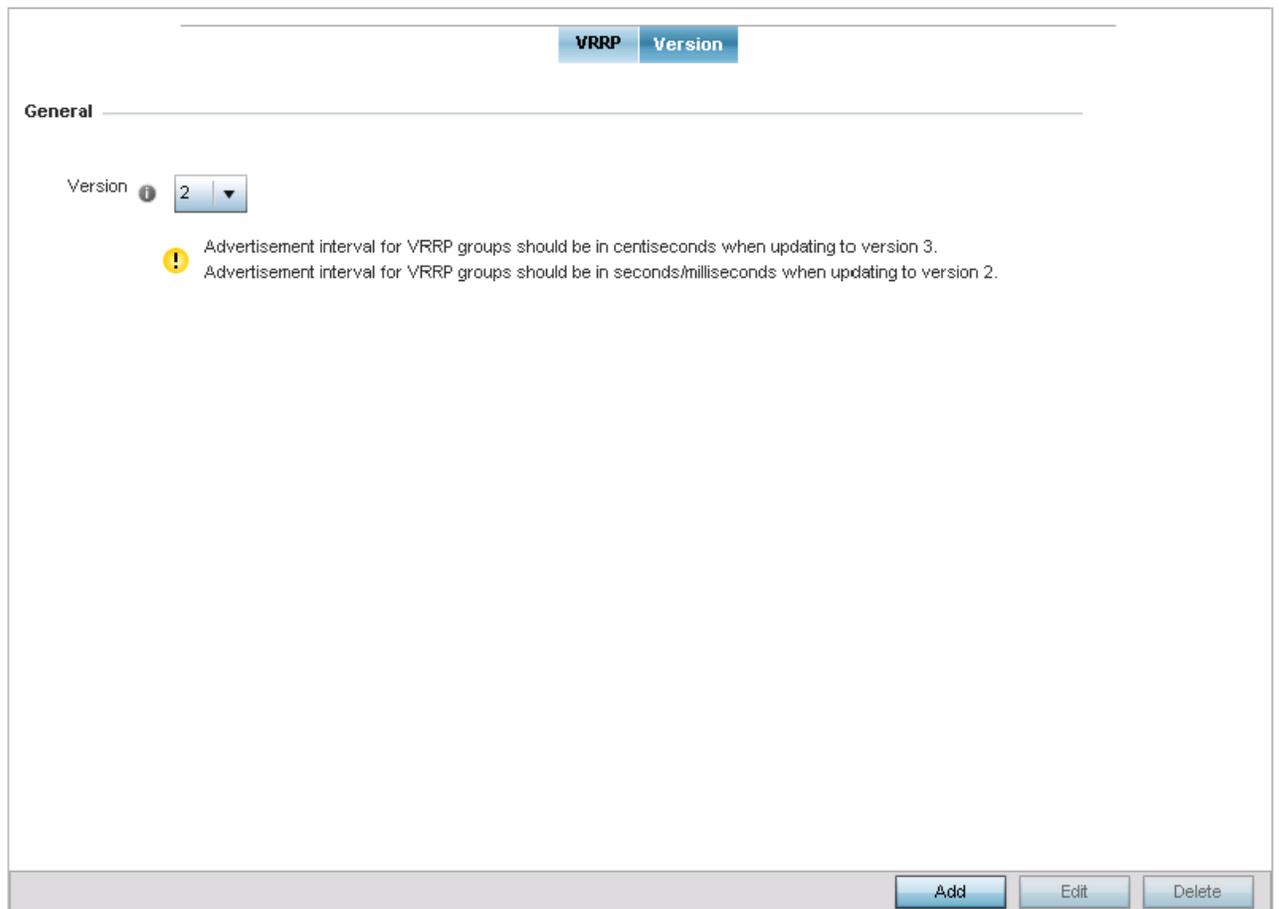
---

---

To define the configuration of a VRRP group:

1. Select the **Configuration** tab from the Web UI.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **VRRP**.





**Figure 5-199** Device Overrides - VRRP screen - Version tab

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are selectable to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications (available publicly) refer to <http://www.ietf.org/rfc/rfc3768.txt> (version 2) and <http://www.ietf.org/rfc/rfc5798.txt> (version 3).

7. From within the **VRRP** tab, select **Add** to create a new VRRP configuration or **Edit** to modify the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by selecting **Delete**.

The screenshot shows the VRRP configuration window with the following settings:

- Virtual Router ID:** 1 (range 1 to 255)
- General:**
  - Description: (empty field)
  - Priority: 100 (range 1 to 254)
  - Virtual IP Addresses: A table with 4 rows, each containing '0 . 0 . 0 . 0' and a 'Clear' button.
  - Advertisement Interval Unit: seconds
  - Advertisement Interval: 1 (range 1 to 255) with a checkbox for 250 (range 250 to 999)
  - Preempt:
  - Preempt Delay: 1 (range 1 to 65,535 seconds)
  - Interface:  VLAN ID: 1 (range 1 to 4,094)
- Protocol Extension:**
  - Sync Group:
  - Network Monitoring:
    - Local Interface:  wwan1,  pppoe1,  VLAN ID: 1 (range 1 to 4094)
    - Critical Resources: None
    - Delta Priority:  1 (range 1 to 253)

Buttons at the bottom: OK, Reset, Exit.

**Figure 5-200** Device Overrides - VRRP screen

- If creating a new VRRP configuration, assign a **Virtual Router ID** from 1 - 255. In addition to functioning as numerical identifier, the ID identifies the access point's virtual router a packet is reporting status for.
- Define the following VRRP **General** parameters:

<b>Description</b>	In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration.
<b>Priority</b>	Use the spinner control to set a VRRP priority setting from 1 - 254. The access point uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master.

<b>Virtual IP Addresses</b>	Provide up to 8 IP addresses representing the Ethernet switches, routers or security appliances defined as virtual router resources to the AP7131 access point.
<b>Advertisement Interval Unit</b>	Select either <i>seconds</i> , <i>milliseconds</i> or <i>centiseconds</i> as the unit used to define VRRP advertisements. Once an option is selected, the spinner control becomes enabled for that <i>Advertisement Interval</i> option. The default interval unit is seconds. If changing the VRRP group version from 2 to 3, ensure the advertisement interval is in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.
<b>Advertisement Interval</b>	Once the <i>Advertisement Interval Unit</i> has been selected, use the spinner control to set the interval at which the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second.
<b>Preempt</b>	Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the <i>Preempt Delay</i> option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can takeover all the Virtual IPs from the nodes with a lower priority.
<b>Preempt Delay</b>	If the <i>Preempt</i> option is selected, use the spinner control to set the delay interval (in seconds) for preemption.
<b>Interface</b>	Select this value to enable/disable VRRP operation and define the AP7131 VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure.

10. Refer to the **Protocol Extension** field to define the following:

<b>Sync Group</b>	Select this option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled by default.
<b>Network Monitoring: Local Interface</b>	Select <i>wwan1</i> , <i>pppoe1</i> and <i>VLAN ID(s)</i> as needed to extend VRRP monitoring to these local access point interfaces. Once selected, these interfaces can be assigned an increasing or decreasing level or priority for virtual routing within the VRRP group.
<b>Network Monitoring: Critical Resources</b>	Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include <i>None</i> , <i>increment-priority</i> , and <i>decrement priority</i> .
<b>Network Monitoring: Delta Priority</b>	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.

11. Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

### 5.4.5.7 Profile Critical Resources

#### ▶ System Profile Configuration

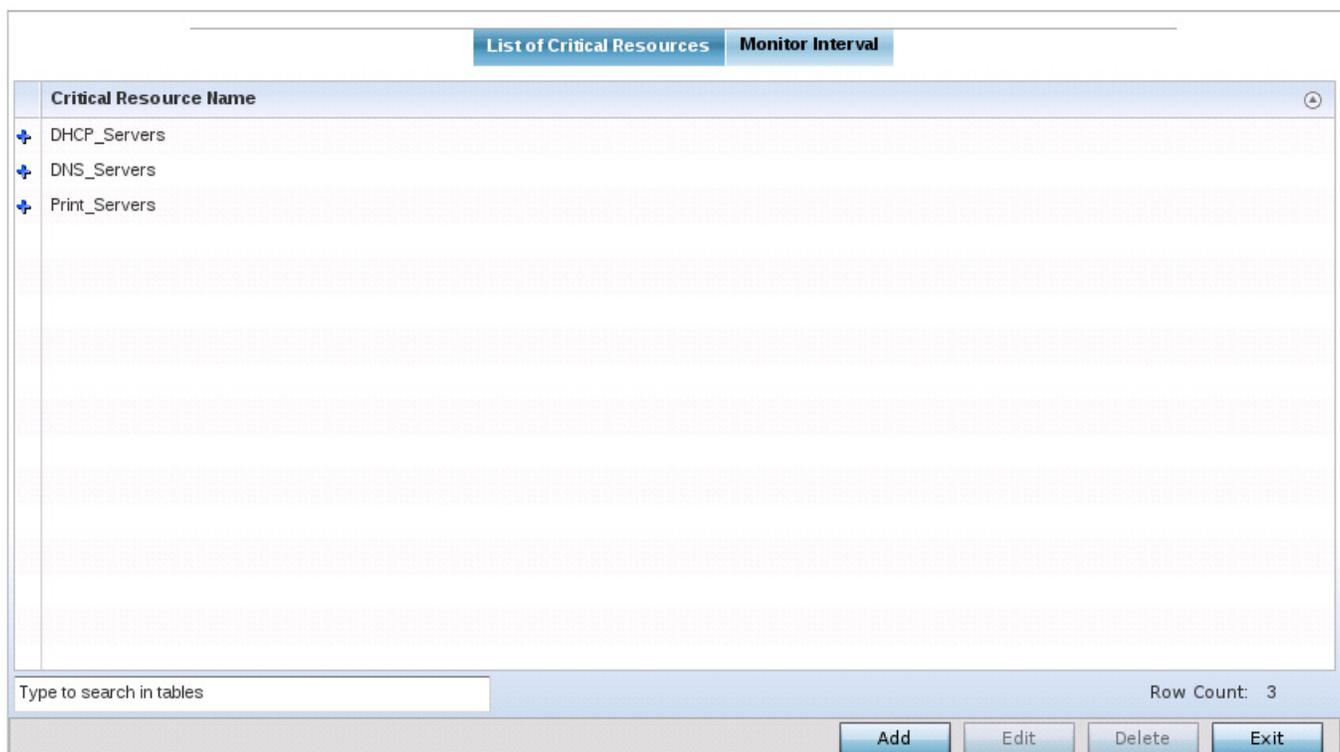
Critical resources are device IP addresses or interface destinations on the network interoperated as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, a AAA server, a WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy, and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they're discovered. For example, a critical resource on the same subnet as the access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

Critical resources can be configured for access points and wireless controllers using their respective profiles.

To define critical resources:

1. Select the **Configuration** tab from the Web UI.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Critical Resources**.



**Figure 5-201** Device Overrides - Critical Resources screen - List of Critical Resources tab

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the access point or controller, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5. Select the **Add** button at the bottom of the screen to add a new critical resource and connection method, or select and existing resource and select **Edit** to update the resource's configuration.

**Figure 5-202** Device Overrides - Critical Resources screen - Adding a Critical Resource

6. Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated. Options include *Any* and *All*. If selecting **Any**, an event is generated when the state of any single critical resource changes. If selecting **All**, an event is generated when the state of all monitored critical resources change.
7. Select the **IP** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided critical resource IP address as a network identifier.
8. Select the **Interface** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource using either the critical resource's VLAN, WWAN1 or PPPoE1 interface. If VLAN is selected, a spinner control is enabled to define the destination VLAN ID used as the interface for the critical resource.
9. Select **+ Add Row** to define the following for critical resource configurations:

<b>IP Address</b>	Provide the IP address of the critical resource. This is the address used by the access point to ensure the critical resource is available. Up to four addresses can be defined.
<b>Mode</b>	Set the ping mode used when the availability of a critical resource is validated. Select from: <ul style="list-style-type: none"> <li>• <i>arp-only</i> – Use the <i>Address Resolution Protocol</i> (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.</li> <li>• <i>arp-and-ping</i> – Use both ARP and <i>Internet Control Message Protocol</i> (ICMP) for pinging the critical resource and sending control messages (device not reachable, requested service not available, etc.).</li> </ul>
<b>Port</b>	Provide the port on which the critical resource is available. Use the spinner control to set the port number.
<b>VLAN</b>	Define the VLAN on which the critical resource is available using the spinner control.

10. Select the **Monitor Interval** tab.

The screenshot shows a configuration window titled "List of Critical Resources" with a sub-tab "Monitor Interval". Under the "General" section, there are two fields:

- Monitor Interval:** A numeric input field containing "30" with a range "(5 to 86,400 seconds)" to its right.
- Source IP For Port-Limited Monitoring:** A dotted IP address input field containing "0 . 0 . 0 . 0".

At the bottom right of the window, there are two buttons: "OK" and "Reset".

**Figure 5-203** Device Overrides - Critical Resources screen - Monitor Interval tab

11. Set the duration between two successive pings from the access point to critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.
12. Configure the IP address for Port-Limited Monitoring in the **Source IP for Port-Limited Monitoring** field. Sets the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. Generally, the source address 0.0.0.0 is used in the APR packets used to detect critical resources. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.
13. Select **OK** to save the changes to the critical resource configuration and monitor interval. Select **Reset** to revert to the last saved configuration.

### 5.4.5.8 Overriding a Services Configuration

#### ▶ *Device Overrides*

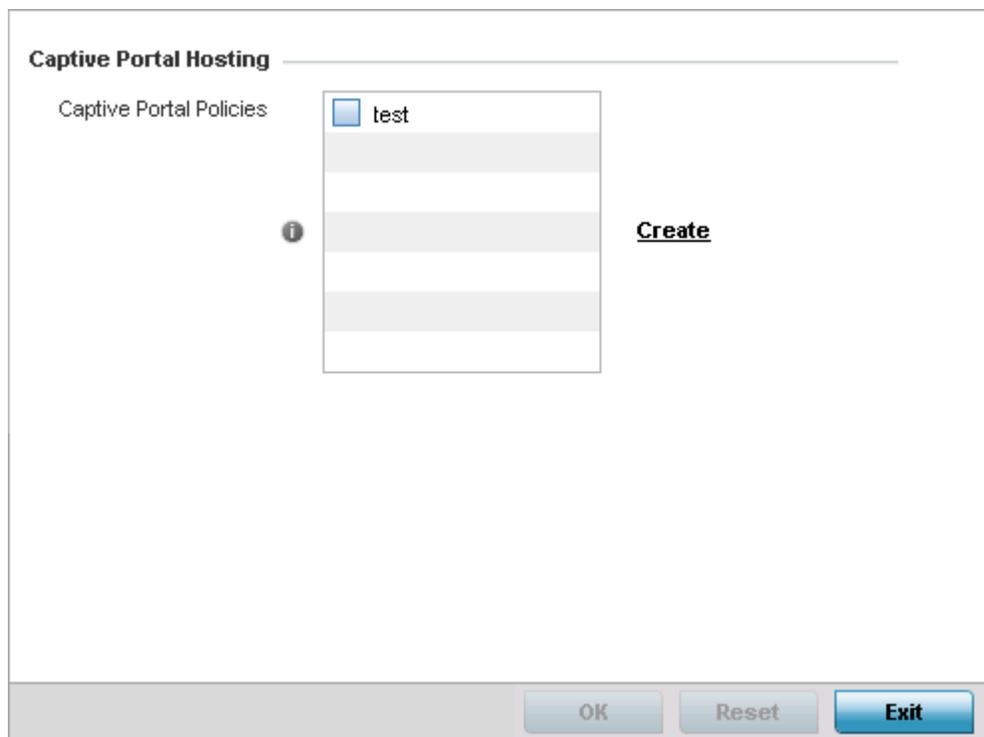
A profile can contain specific guest access (captive portal), DHCP server and RADIUS server configurations. These access, IP assignment and user authorization resources can be defined uniquely as profile requirements dictate.

To define or override a profile's services configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Services**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the Basic Configuration screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.



**Figure 5-204** Device Overrides - Services screen

5. Refer to the **Captive Portal Hosting** field to set or override a guest access configuration (captive portal) for use with this profile.

A captive portal is guest access policy for providing temporary and restrictive access to the network. The primary means of securing such guest access is a captive portal.

A captive portal configuration provides secure authenticated access using a standard Web browser. A captive portal provides authenticated access by capturing and re-directing a user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on the captive portal's screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal configuration that can be applied to a profile. For more information, see [Configuring Captive Portal Policies on page 9-2](#).

6. Select **OK** to save the changes or overrides made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

### 5.4.5.9 Overriding a Management Configuration

#### ▶ [Device Overrides](#)

There are mechanisms to allow/deny management access to the network for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). These management access configurations can be applied strategically to profiles as resource permissions dictate for the profile. Additionally, overrides can be applied to customize a device's management configuration, if deployment requirements change and a device's configuration must be modified from its original device profile configuration.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support.

To define or override a profile's management configuration:

1. Select **Devices** from the Configuration tab.
2. Select **Device Overrides** from the Device menu to expand it into sub menu options.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Management**.



**NOTE:** A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

---

---

**Message Logging**

Enable Message Logging

Remote Logging Host

IP Address	
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>
0 . 0 . 0 . 0	<a href="#">Clear</a>

Facility to Send Log Messages

Syslog Logging Level  Warning

Console Logging Level  Warning

Buffered Logging Level  Warning

Time to Aggregate Repeated Messages  Seconds ( 0 to 60 )

Forward Logs to Controller  Error

**System Event Messages**

Enable System Events

Enable System Event Forwarding

OK Reset Exit

**Figure 5-205** Device Overrides - Management Settings screen

- Refer to the Message Logging field to define how the profile logs system events. It's important to log individual events to discern an overall pattern that may be negatively impacting performance.

<b>Enable Message Logging</b>	Select this option to enable the profile to log system events to a user defined log file or a syslog server. Selecting this radio button enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.
<b>Remote Logging Host</b>	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select Clear as needed to remove an IP address.
<b>Facility to Send Log Messages</b>	Use the drop-down menu to specify the local server facility (if used) for the profile event log transfer.
<b>Syslog Logging Level</b>	Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info and 7 - Debug. The default logging level is 4.

<b>Console Logging Level</b>	Event severity coincides with the console logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Buffered Logging Level</b>	Event severity coincides with the buffered logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Time to Aggregate Repeated Messages</b>	Define the increment (or interval) system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged. Either define an interval in <i>Seconds</i> (0 - 60) or <i>Minutes</i> (0 - 1). The default value is 0 seconds.
<b>Forward Logs to Controller</b>	Select this option to define a log level for forwarding event logs to the control. Log levels include <i>Emergency, Alert, Critical, Error, Warning, Notice, Info</i> and <i>Debug</i> . The default logging level is <i>Error</i> .

- Refer to the **System Event Messages** field to define or override how system messages are logged and forwarded on behalf of the profile.
- Select the **Enable System Events** radio button to allow the profile to capture system events and append them to a log file. It's important to log individual events to discern an overall pattern that may be negatively impacting performance. This settings is enabled by default.
- Select the **Enable System Event Forwarding** radio button to enable the forwarding of system events. This setting is enabled by default.
- Refer to the **Events E-mail Notification** field to define or override how system event notification E-mails are sent.

<b>SMTP Server</b>	Specify either the <i>Hostname</i> or <i>IP Address</i> of the outgoing SMTP server where notification E-mails are originated.
<b>Port of SMTP</b>	If a non-standard SMTP port is used on the outgoing SMTP server select this option and specify a port from 1 - 65,535 for the outgoing SMTP server to use.
<b>Sender E-mail Address</b>	Specify the E-mail address that notification E-mails will be sent from. This will be the from address on notification E-mails.
<b>Recipient's E-mail Address</b>	Specify the E-mail address(es) of recipients for E-mail notifications.
<b>Username for SMTP Server</b>	Specify the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending E-mail through the server.
<b>Password for SMTP Server</b>	Specify the password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending E-mail through the server.

- Use the **Configure** drop-down menu within the **Persist Configuration Across Reloads** field to define whether the access point saves a configuration received from a Virtual Controller AP to flash memory. The configuration would then be made available if the this access point reboots and the Virtual Controller AP is not reachable. Options include *Enabled, Disabled* and *secure*.
- Use the **HTTP Analytics** section to define how data for analysis by an external engine is sent. Select **Compress** to compress the data before sending. Use the **Update Interval** field to set the duration and set the time interval in *minutes, seconds* or *hours* when the collected data is sent to the external analytics engine.

12. Select **OK** to save the changes and overrides made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.
13. Select the **Firmware** tab from the Management menu.

The screenshot shows the 'Management Firmware' configuration screen. It is divided into two main sections: 'Auto Install via DHCP Option' and 'Automatic Adopted AP Firmware Upgrade'. In the first section, 'Enable Configuration Update' and 'Enable Firmware Update' are both checked. In the second section, 'Enable Controller Upgrade of AP Firmware' is checked and set to 'AP71xx'. Below this, 'Number of Concurrent Upgrades' is set to 10 using a spinner control, with a range of 1 to 20 APs. At the bottom of the screen are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 5-206** Device Overrides - Management Firmware screen

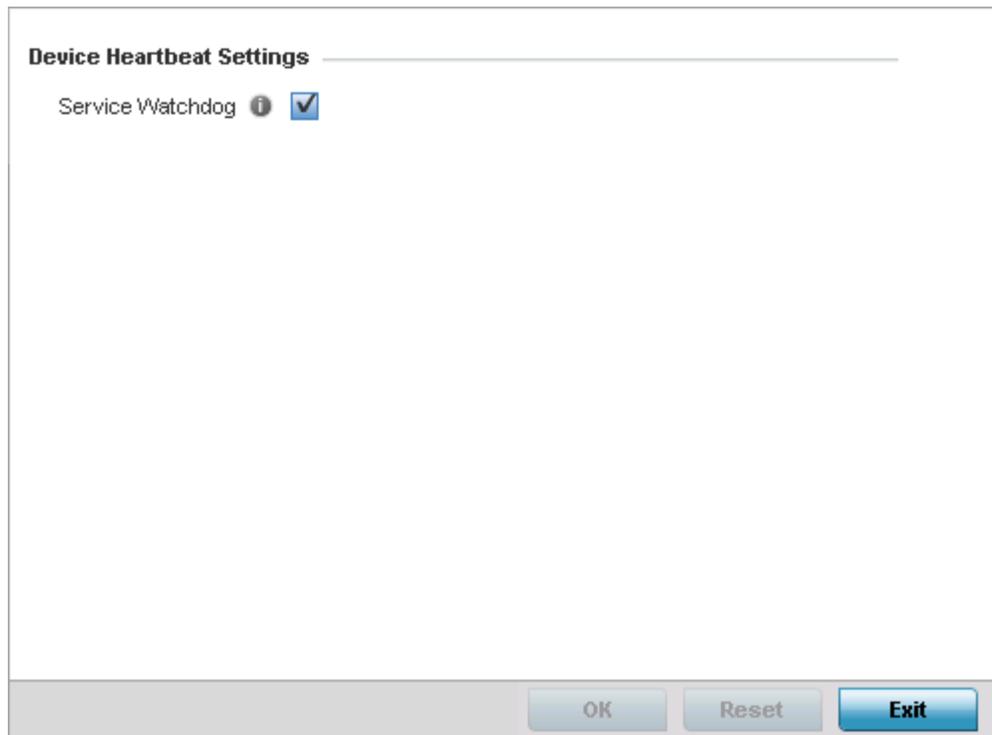
14. Refer to the **Auto Install via DHCP Option** field to define automatic configuration file and firmware updates.

<b>Enable Configuration Update</b>	Select this option to enable automatic configuration file updates for the controller profile from a location external to the access point. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update.
<b>Enable Firmware Update</b>	Select this option to enable automatic firmware updates from a user defined remote location. This value is disabled by default.

15. Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware upgrade from a controller based file.

<b>Enable Controller Upgrade of AP Firmware</b>	Select the access point model to upgrade using its associated Virtual Controller AP's most recent firmware file for that model. This parameter is enabled by default.
<b>Number of Concurrent Upgrades.</b>	Use the spinner control to define the maximum number (1 - 20) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind during a firmware upgrade, the access point is offline and unable to perform its normal wireless client support function until the upgrade process is complete.

16. Select **OK** to save the changes and overrides made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.
17. Select **Heartbeat** from the Management menu.



**Figure 5-207** Device Overrides - Management Heartbeat screen

18. Select the **Service Watchdog** option to implement heartbeat messages to ensure other associated devices are up and running and capable of effectively interoperating. The Service Watchdog is enabled by default.
19. Select **OK** to save the changes and overrides made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.10 Overriding Mesh Point Configuration

##### ▶ [Device Overrides](#)

The access point can be configured to be a part of a meshed network. A mesh network is one where each node in the network is able to communicate with other nodes in the network and where the node can maintain more than one path to its peers. Mesh network provides robust, reliable and redundant connectivity to all the members of the network. When one of the participant node in a mesh network becomes unavailable, the other nodes in the network are still able to communicate with each other either directly or through intermediate nodes.

Mesh Point is the name given to a device that is a part of a meshed network.

Use the Mesh Point screen to configure or override the parameters that set how this device behaves as a part of the mesh network.

To override Mesh Point configuration:

1. Select **Devices** from the Configuration menu.
2. Select **Device Overrides** to expand its menu items.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Mesh Point**.



**Mesh Connex Policy** \* [Dropdown] [Create] [Edit] [Help]

Settings | Auto Channel Selection

**General**

Is Root: [None] [v]

Root Selection Method: [None] [v]

Set as Cost Root:

Monitor Critical Resources:

Monitor Primary Port Link:

Wired Peer Excluded:

Path Method: [None] [v]

**Root Path Preference**

Preferred Neighbor: [00 - 00 - 00 - 00 - 00 - 00]

Preferred Root: [00 - 00 - 00 - 00 - 00 - 00]

Preferred Interface: [None] [v]

**Path Method Hysteresis**

Minimum Threshold: [0] [v] (-100 to 0 dB)

Signal Strength Delta: [1] [v] (1 to 100 dB)

Sustained Time Period: [1] [v] [Seconds] [v] (0 to 600)

SNR Delta Range: [1] [v] (1 to 100 dB)

[OK] [Reset] [Exit]

**Figure 5-209** Device Overrides - Add Mesh Point screen

6. Refer to the following to configure Mesh Point general parameters:

<b>Mesh Connex Policy</b>	Provide a name for the Mesh Connex Policy. Use the <i>Create</i> icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the drop-down and click the <i>Edit</i> icon. For more information on creating or editing a Mesh Connex Policy, see <a href="#">MeshConnex Policy on page 6-85</a> .
<b>Is Root</b>	From the drop-down menu, select the root behavior of this access point. Select <i>True</i> to indicate this access point is a root node for this mesh network. Select <i>False</i> to indicate this access point is not a root node for this mesh network. A Root Mesh Point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network.
<b>Root Selection Method</b>	Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either <i>None</i> (the default setting) or <i>auto-mint</i> .
<b>Set as Root</b>	Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default.

<b>Monitor Critical Resources</b>	Select this option to enable critical resource monitoring for this mesh point.
<b>Monitor Primary Port Link</b>	Select to enable monitoring of primary port link is enabled for this mesh connex policy. If the primary port link is not present and if the device is a mesh root, it is automatically changed to a non-root device. When the primary port link becomes available again, the non-root device is changed back to a root device.
<b>Wired Peer Exclude</b>	Select this option to exclude wired peers when creating mesh links.
<b>Path Method</b>	From the drop-down menu, select the method to use for path selection in a mesh network. The available options are: <ul style="list-style-type: none"> <li>• <i>None</i> – Select this to indicate no criteria used in root path selection.</li> <li>• <i>uniform</i> – Select this to indicate that the path selection method is uniform. When selected, two paths will be considered equivalent if the average value is the same for these paths.</li> <li>• <i>mobile-snr-leaf</i> – Select this if this access point is mounted on a vehicle or a mobile platform (AP7161 models only). When selected, the path to the route will be selected based on the <i>Signal To Noise Ratio</i> (SNR) to the neighbor device.</li> <li>• <i>snr-leaf</i> – Select this to indicate that the path with the best signal to noise ratio is always selected.</li> </ul>
<b>Minimum Threshold</b>	Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered. This field along with <i>Signal Strength Delta</i> and <i>Sustained Time Period</i> are used to dynamically select the next hop in a dynamic mesh network.
<b>Signal Strength Delta</b>	Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR higher than the value configured here. This field along with the <i>Minimum Threshold</i> and <i>Sustained Time Period</i> are used to dynamically select the next hop in a dynamic mesh network.
<b>Sustained Time Period</b>	Enter the time duration in <i>seconds</i> (0 - 600) or <i>minutes</i> (0 - 10). This indicates the duration that a signal must sustain the constraints specified in the <i>Minimum Threshold</i> and <i>Signal Strength Delta</i> path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network.
<b>SNR Delta Range</b>	Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB.

7. Refer to the following to configure Mesh Point **Root Path Preference** parameters:

<b>Preferred Neighbor</b>	Enter the MAC address of the preferred neighbor for this mesh point.
<b>Preferred Root</b>	Enter the MAC address of the preferred mesh root for this mesh point.
<b>Preferred Interface</b>	Select the preferred Interface for this mesh point. Select <i>None</i> to set no preferences. The other interface choices are <i>2.4 GHz</i> and <i>5 GHz</i> .



**NOTE:** With this release of Motorola Solutions WiNG software, an AP7161 model access point can be deployed as a *Vehicle Mounted Modem* (VMM) to provide wireless network access to a mobile vehicle (car, train, etc.). A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see [Vehicle Mounted Modem \(VMM\) Deployment Consideration](#).

8. Click the **Auto Channel Selection** tab to configure the parameters for the Mesh Connex Auto Channel Selection policy. The following screen displays:

**Figure 5-210** Mesh Point Auto Channel Selection screen

9. By default, the **Dynamic Root Selection** screen displays.

This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies. Refer to the following for more information on the Auto Channel Selection Dynamic Root Selection screen. These descriptions are common for configuring the 2.4 GHz and 5.0/4.9 GHz frequencies

<b>Channel Width</b>	<p>Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
----------------------	--

<b>Priority Meshpoint</b>	Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
<b>Off Channel Duration</b>	Configure the duration in the range of 20 - 250 milliseconds for the <i>Off Channel Duration</i> field. This is the duration that the scan dwells on each channel when performing an off channel scan.
<b>Off Channel Scan Frequency</b>	Configure the time duration in seconds between two consecutive Off Channel Scans. Set a duration between 1 - 60 seconds.
<b>Meshpoint Root - Sample Count</b>	Configure the number of scans to be performed for data collection before a mesh channel is selected. Set a value between 1 - 10 scans.
<b>Meshpoint Root - Channel Hold Time</b>	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

10. Select the **Path Method SNR** tab to configure the signal to noise ratio when selecting the path to the mesh point root.

**Mesh Point** MeshConnex Policy MeshConnexPolicy\_01

Settings Auto Channel Selection

Dynamic Root Selection **Path Method SNR** Path Method Root Path Metric

**For 2.4 GHz**

Channel Width

Priority Meshpoint

SNR Delta  (1 to 100 dB)

SNR Threshold  (-100 to 0 dB)

Off-channel Duration  (20 to 250 milliseconds)

**For 5.0/4.9 GHz**

Channel Width

Priority Meshpoint

SNR Delta  (1 to 100 dB)

SNR Threshold  (-100 to 0 dB)

Off-channel Duration  (20 to 250 milliseconds)

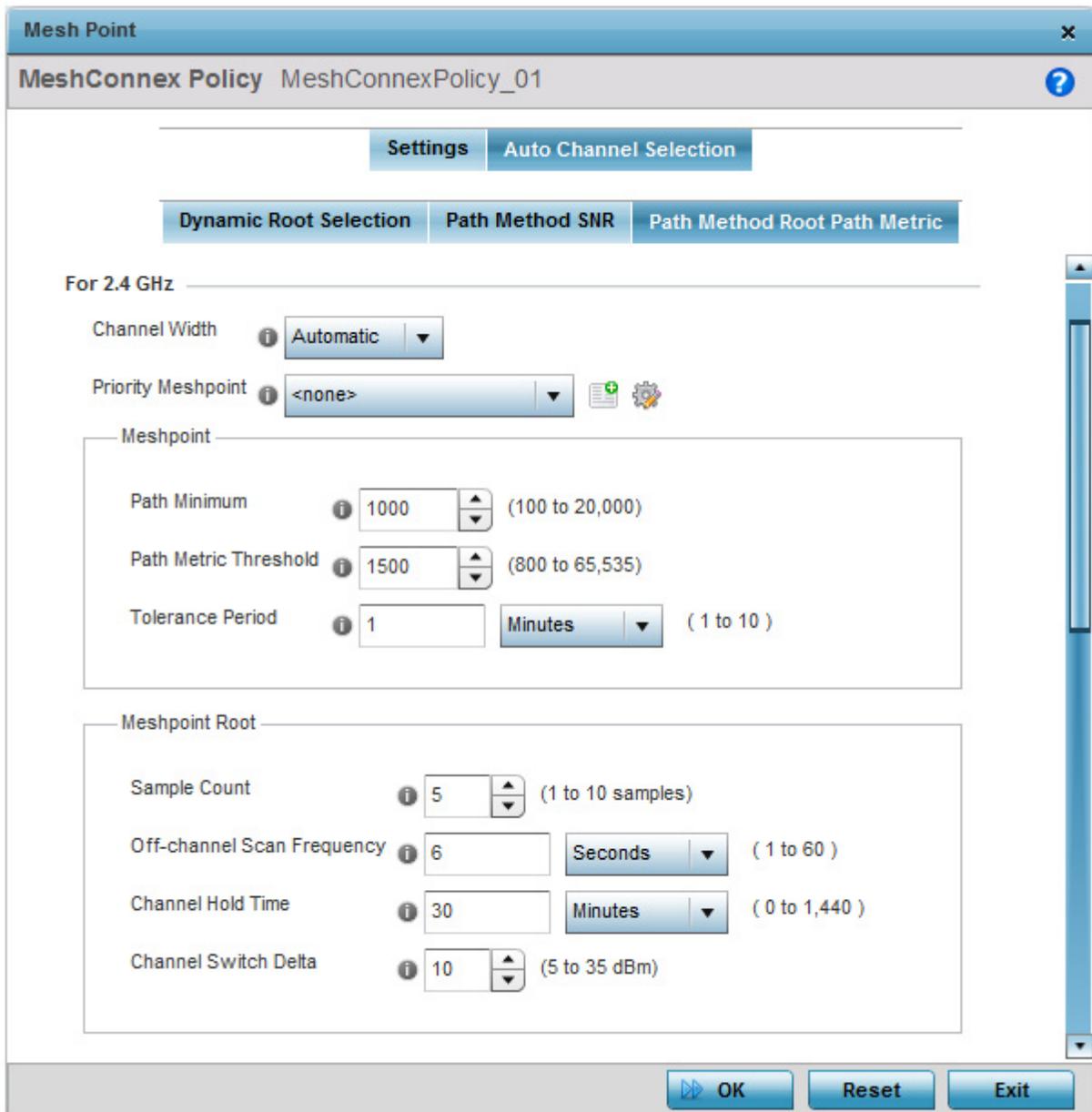
OK Reset Exit

**Figure 5-211** Mesh Point Auto Channel Selection Path Method SNR screen

Refer to the following for more information on the Path Method SNR screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

<b>Channel Width</b>	<p>Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
<b>Priority Meshpoint</b>	<p>Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.</p>
<b>SNR Delta</b>	<p>Configure the signal to noise ratio delta value for path selection.</p> <p>When path selection occurs, this set value is considered for selecting the optimal path. A better candidate on a different channel must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network.</p>
<b>SNR Threshold</b>	<p>Configure the signal to noise threshold value for path selection.</p> <p>When the signal strength of the next hop in the mesh network goes below this value, a scan is triggered to select a better next hop.</p>
<b>Off-channel Duration</b>	<p>Configure the duration in the range of 20 - 250 milliseconds for the <i>Off Channel Duration</i> field. This is the duration that the scan dwells on each channel when performing an off channel scan.</p>

11. Select the **Path Method Root Path Metric** tab to configure the parameters controlling the calculation of the root path metrics.



**Figure 5-212** Mesh Point Auto Channel Selection Path Method Root Path Metric screen

12. Refer to the following for more information on the Path Method Root Path Metric screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

<b>Channel Width</b>	<p>Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i> – Indicates the channel width is calculated automatically. This is the default value.</li> <li>• <i>20 MHz</i> – Indicates the width between two adjacent channels is 20 MHz.</li> <li>• <i>40 MHz</i> – Indicates the width between two adjacent channels is 40 MHz.</li> </ul>
----------------------	--

<b>Priority Meshpoint</b>	Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
<b>Meshpoint: Path Minimum</b>	Configure the minimum path metric value for a mesh connection. Set a value between 100 - 20,000.
<b>Meshpoint: Path Metric Threshold</b>	Configure a minimum threshold value for triggering an automatic channel selection for mesh point selection. Set a value in between 800 - 65535.
<b>Meshpoint: Tolerance Period</b>	Configure the time duration in seconds to wait before triggering a automatic channel selection for the next hop.
<b>Meshpoint: Root Sample Count</b>	Configure the number of scans to be performed for data collection before a mesh point root is selected. Set a value between 1 - 10 scans.
<b>Meshpoint: Root Off-channel Duration</b>	Configure the duration in the range of 20 - 250 milliseconds for the <i>Off Channel Duration</i> field when scanning for mesh point root. This is the duration that the scan dwells on each channel when performing an off channel scan.
<b>Meshpoint: Root Channel Switch Delta</b>	Configure the delta value in dBm in the range 5 - 35 dBm which when crossed triggers a mesh point root automatic channel selection.
<b>Meshpoint: Root Off-channel Scan Frequency</b>	Configure the duration in seconds between two consecutive Off Channel Scans for mesh point root. Set a duration between 1 - 60 seconds.
<b>Meshpoint: Root Channel Hold Time</b>	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change for mesh point root. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

13. Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to exit this screen.
14. Select **OK** to save the changes made to the profile's mesh point configuration. Select **Reset** to revert to the last saved configuration.

#### 5.4.5.10.1 Vehicle Mounted Modem (VMM) Deployment Consideration

##### ► *Mesh Point Configuration*

Before defining a VMM configuration (mounting an AP7161 mesh point on a moving vehicle), refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Disable layer 2 stateful packet inspection from the firewall policy.
- Set the RTS threshold value to 1 on all mesh devices. The default value is 2347. For more information on defining radio settings, see [Access Point Radio Configuration](#).
- Use *Opportunistic* as the rate selection settings for the AP7161 radio The default is *Standard*. For more information on defining this settings, see [Radio Override Configuration](#).
- Disable *Dynamic Chain Selection* (radio setting). The default value is enabled. This setting is disabled from the *Command Line Interface* (CLI) using the `dynamic-chain-selection` command, or, in the UI (refer [Radio Override Configuration](#)).
- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see [Radio Override Configuration](#).

### 5.4.5.11 Overriding an Advanced Configuration

#### ▶ *Device Overrides*

Advanced device settings sets or overrides a profile's MiNT and/or NAS configurations.

MINT secures controller profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. access point managed devices can communicate with each other exclusively over a MINT security domain. Keys can also be generated externally using any application (like openssl). These keys must be present on the managed device managing the domain for key signing to be integrated with the UI. A MAP device that needs to communicate with another first negotiates a security context with that device. The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for access points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

The profile database on the RADIUS server consists of user profiles for each connected *Network Access Server* (NAS) port. Each profile is matched to a username representing a physical port. When users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection.

To set or override an advanced configuration:

1. Select **Devices** from the Configuration menu.
2. Select **Device Overrides** to expand its menu items.
3. Select a target device from the device browser in the lower, left-hand, side of the UI.
4. Select **Advanced** to expand its sub menu items.
5. Select **Client Load Balancing**.

**Figure 5-213** Device Overrides - Client Load Balancing

- Use the drop-down to set a value for **SBC strategy**. Options include *Prefer 5GHz*, *Prefer 2.4 GHz*, and *distribute-by-ratio*. The default value is *Prefer 5GHz*.
- Refer to the following **Neighbor Selection Strategies** fields to configure or override it:

<b>Using probes from common clients</b>	Select this option to enable neighbor selection using probe requests from common clients between the neighbor device and this device.
<b>Using notifications from roamed clients</b>	Select this option to enable neighbor selection using notifications from clients roamed from other devices.
<b>Using smart-rf neighbor detection</b>	Select this option to enable neighbor selection using Smart RF neighbor detection algorithm.

- Select **Balance Band Loads by Ratio** to configure or override **Band Load Balancing** configuration.
- Refer to the following **Channel Load Balancing** fields to configure or override it:

<b>Balance 2.4 GHz Channel Loads</b>	Select this option to balance the access point's 2.4GHz radio load across the channels supported within the country of deployment. This can prevent congestion on the 2.4GHz radio if a channel is over utilized.
--------------------------------------	---

<b>Balance 5 GHz Channel Loads</b>	Select this option to balance the access point's 5 GHz radio load across the channels supported within the country of deployment. This can prevent congestion on the 5 GHz radio if a channel is over utilized.
------------------------------------	---

10. Select **Balance AP Loads** to configure or override **AP Load Balancing** configuration.

AP Loads are balance by balancing the radio load, by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5 GHz band.

11. Refer to the following **Advanced Parameters**:

<b>Max 2.4 GHz Load Difference Considered Equal</b>	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points.
<b>Min. Value to Trigger 2.4GHz Channel Balancing</b>	Use the spinner control to define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHz radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.
<b>Max 5 GHz Load Difference Considered Equal</b>	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 5 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points.
<b>Min. Value to Trigger 5 GHz Channel Balancing</b>	Use the spinner control to define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHz radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.

12. Refer to the following **AP Load Balancing** fields to configure or override them:

<b>Min Value to Trigger Load Balancing</b>	Use the spinner control to set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other access point radios. When this radio load exceeds the defined threshold, load balancing is initiated. The default is 70%.
<b>Max. AP Load Difference Considered Equal</b>	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing access point radio load balances.
<b>Weightage given to Client Count</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHz radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.
<b>Weightage given to Throughput</b>	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize throughput in the access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.

13. Refer to the following **Band Control** parameters to configure or override them:

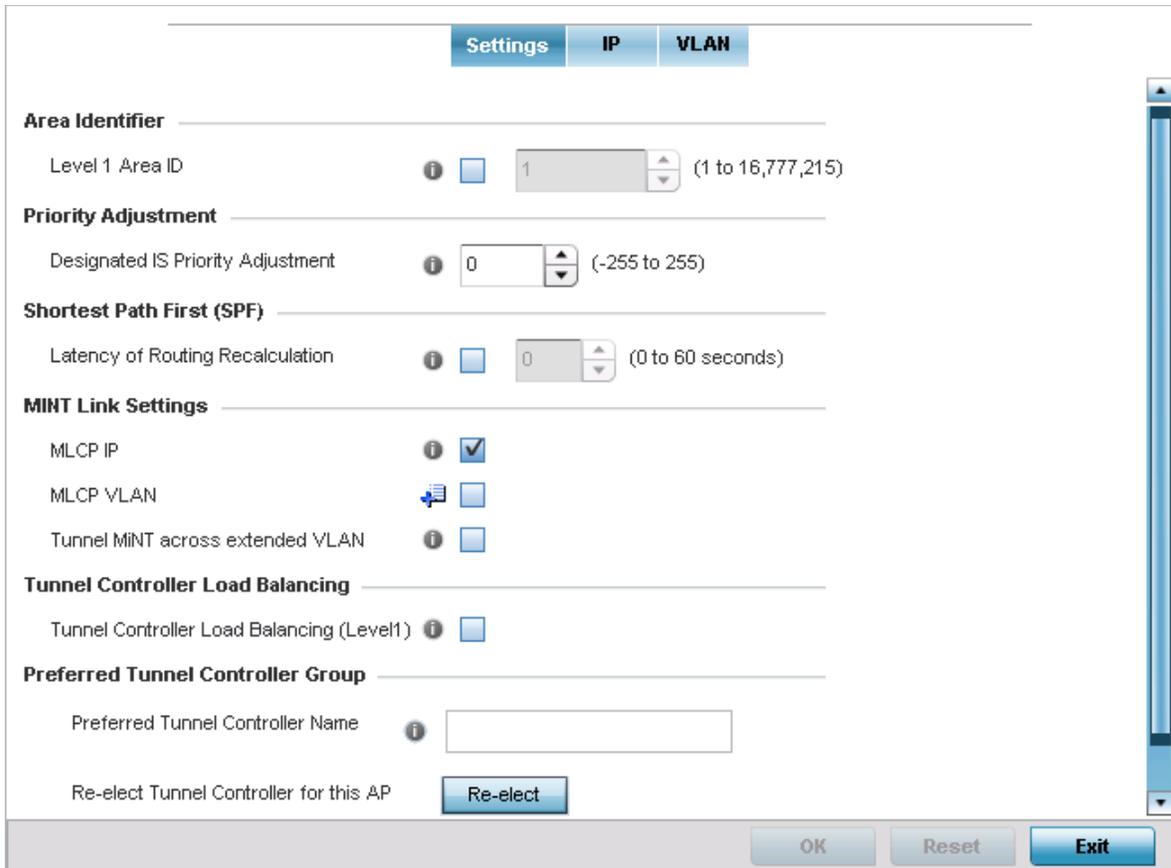
<b>Max. Band Load Difference Considered Equal</b>	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 and 5GHz radio band load balances on this access point. The default setting is 10%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing 2.4 and 5 GHz load balances on this access point.
<b>Band Ratio (2.4GHz)</b>	Use the spinner control to set a loading ratio (between 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1.
<b>Band Ratio (5 GHz)</b>	Use the spinner control to set a loading ratio (between 0 - 10) the access point 5 GHz radio uses in respect to radio traffic load on the 5 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 5 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 5 GHz radio band. The default setting is 1.
<b>5 GHz load which both bands enable</b>	Use the spinner control to set a load percentage (between 0 - 100) that enables the other band (2.4 GHz) to share load with the current band.
<b>2.4 GHz load which both bands enable</b>	Use the spinner control to set a load percentage (between 0 - 100) that enables the other band (5 GHz) to share load with the current band.

14. Refer to the following **Neighbor Selection** parameters to configure or override them:

<b>Minimum signal strength for common clients</b>	Use the spinner to set the minimum signal strength require to learn about neighbors from clients that are common with the neighbor access point.
<b>Minimum number of clients seen</b>	Use the spinner to set the minimum number of common clients seen before the neighbor is learnt.

<b>Max confirmed Neighbors</b>	Use the spinner to set the maximum number of learned neighbors stored at this device.
<b>Minimum signal strength for smart-rf neighbors</b>	Use the spinner to set the minimum signal strength of neighbor devices that are learnt through Smart RF before being recognized as neighbors.

15. Select **MINT Protocol**. The MINT Protocol screen displays the **Settings** tab by default.



**Figure 5-214** Device Overrides - Advanced Profile Overrides MINT screen - Settings tab

16. Refer to the **Area Identifier** field to define or override the Level 1 and Level 2 Area IDs used by the profile's MINT configuration.

<b>Level 1 Area ID</b>	Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 4,294,967,295. The default value is disabled.
------------------------	---

17. Define or override the following **Priority Adjustment** settings:

<b>Designated IS Priority Adjustment</b>	Use the spinner control to set a <i>Designated IS Priority Adjustment</i> setting from -255 - +255. This is the value added to the base level DIS priority to influence the <i>Designated IS (DIS)</i> election. A value of +1 or greater increases DISiness. The default setting is 0.
--	---

18. Select the **Latency of Routing Recalculation** option (within the *Shortest Path First (SPF)* field) to enable the spinner control used for defining or overriding a latency period from 0 - 60 seconds. The default setting has the option disabled.



**Figure 5-216** Device Overrides - Advanced Profile MINT screen - IP (Add)

25. Set the following **Link IP** parameters to complete the MINT network address configuration:

<b>IP</b>	Define or override the IP address used by peer access points for interoperation when supporting the MINT protocol.
<b>Routing Level</b>	Use the spinner control to define or override a routing level of either 1 or 2.
<b>Listening Link</b>	Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and doesn't scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted.
<b>Port</b>	To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number from 1 - 65,535.
<b>Forced Link</b>	Select this option to specify the MiNT link as a forced link. This setting is disabled by default.
<b>Link Cost</b>	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set or override an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.



The screenshot shows a 'VLAN' configuration window with the following parameters:

- VLAN:** 1 (range: 1 to 4,094)
- Routing Level:** 1 (range: 1 to 2)
- Link Cost:** 10 (range: 1 to 10,000)
- Hello Packet Interval:** 4 (range: 1 to 120) with a dropdown set to 'Seconds'
- Adjacency Hold Time:** 13 (range: 2 to 600) with a dropdown set to 'Seconds'

Buttons at the bottom include 'OK', 'Reset', and 'Exit'.

**Figure 5-218** Device Overrides - Advanced Profile MINT screen - Add VLAN screen

28. Set the following VLAN parameters to complete the MINT configuration:

<b>VLAN</b>	Define a VLAN ID from 1 - 4,094 used by peer controllers for interoperation when supporting the MINT protocol.
<b>Routing Level</b>	Use the spinner control to define or override a routing level of either 1 or 2.
<b>Link Cost</b>	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set or override an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 4 seconds.
<b>Adjacency Hold Time</b>	Set or override a hold time interval in either <i>Seconds</i> (2 - 600) or <i>Minutes</i> (1 - 10) for the transmission of hello packets. The default interval is 13 seconds.

29. Select **OK** to save the updates and overrides to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

30. Select the **Advanced Miscellaneous** menu item.

The screenshot shows a configuration window titled "Device Overrides - Miscellaneous". It is divided into several sections:

- Device RADIUS Authentication Parameters:** Contains two text input fields: "NAS-Identifier Attribute" and "NAS-Port-Id Attribute".
- LEDs (Light Emitting Diodes):** Contains a "Turn on LEDs" section with three radio button options: "Off (0)", "On (1)" (which is selected), and "Flash Pattern (2)".
- MeshConnex Parameters:** Contains a "Root Path Monitor Interval" section with a text input field set to "30", a dropdown menu set to "Seconds", and a range "( 1 to 65,535 )".
- RADIUS Dynamic Authorization:** Contains an "Additional Port" section with a spinner control set to "3799", a range "( 1 to 65,535 )", and a note "(Cisco ISE:1700)".
- Client Bridge:** Contains an "Aging Time" section with a text input field set to "10", a dropdown menu set to "Minutes", and a range "( 1 to 10,923 )".

At the bottom right of the window are two buttons: "OK" and "Reset".

**Figure 5-219** Device Overrides - Miscellaneous screen

31. Set a **NAS-Identifier Attribute** up to 253 characters in length. This is the RADIUS NAS-Identifier attribute that typically identifies where a RADIUS message originates
32. Set a **NAS-Port-Id Attribute** up to 253 characters in length. This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates
33. Refer to the **Turn on LEDs** option to enable an adopted access point's LEDs. This feature is enabled by default.
34. Select the **Flash Pattern** radio button to enable the access point to blink in a manner different from its operational LED behavior. Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate the initial configuration is complete.
35. Use the drop-down menu to configure the access point's **Meshpoint Behavior**. This field configures the access point's mobility behavior. The default is *External (fixed)* and indicates that the mesh point is fixed. The value *vehicle-mounted* indicates that the mesh point is mobile. This feature is only available on an AP7161 model access point.
36. Use the **Root Path Monitor Interval** to configure the interval to monitor path to the root node.
37. Set the **Additional Port** value for **RADIUS Dynamic Authorization** field. Set this value to 1700 to enable a CISCO *Identity Services Engine (ISE) Authentication, Authorization and Accounting (AAA)* server, when deployed in the network, to dynamically authenticate a client.

When a client requests access to the network, the CISCO ISE RADIUS server presents the client with a URL where the device's compliance to the networks security such as validity of anti-virus or anti-spyware software is checked for the validity for their definition files (this checking is called posture). If the client device complies, then it is allowed access to the network.

38. Set the **Aging Time** value for **Client Bridge**. Use the spinner control to set a value in *days, hours, minutes* and *seconds*.
39. Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

### 5.4.5.12 Overriding Environmental Sensor Configuration

► *Overriding a Device Configuration*



**NOTE:** This feature is available on the AP8132 model only.

An AP8132 sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using the *Environmental Sensor* screen.

To set an environmental sensor configuration for an AP8132 model access point:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices**.
3. Select **Device Overrides** from the options on left-hand side of the UI.
4. Select **Environmental Sensor**. The *Environmental Sensor* screen displays.

**Figure 5-220** Profile - Environmental Sensor screen

5. Override or set the following **Light Sensor** settings for the AP8132's sensor module:.

<b>Enable Light Sensor</b>	Select this option to enable the light sensor on the module. This setting is enabled by default.
<b>Polling Time to Determine if Light is On/ Off</b>	Define an interval in <i>Seconds</i> (2 - 201) or <i>Minutes</i> (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 11 seconds. Light intensity is used to determine whether the access point's deployment location is currently populated with clients.
<b>Shutdown WLAN Radio at Low Limit of Light Threshold</b>	Select this option to power off the AP8132's radio's if the light intensity falls below the set threshold. If enabled, select <i>All</i> (both AP8132 radios), <i>radio-1</i> or <i>radio-2</i> .

<b>Low Limit of Light Threshold</b>	Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the AP8132's deployment location. The default is 100.
<b>High Limit of Light Threshold</b>	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the AP8132's deployment location. The default is 500.

6. Enable or disable the following **Environmental Sensors**:

<b>Enable Temperature Sensor</b>	Select this option to enable the module's temperature sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
<b>Enable Motion Sensor</b>	Select this option to enable the module's motion sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
<b>Enable Humidity Sensor</b>	Select this option to enable the module's humidity sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.

7. Define or override the following **Shared Configuration** setting:

<b>Polling Interval for All Sensors</b>	Set an interval in either <i>Seconds</i> (1 - 100) or <i>Minutes</i> (1 - 2) for the time between all environmental polling (both light and environment). The default setting is 5 seconds.
---	---

8. Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

## 5.5 Managing an Event Policy

### ► Device Configuration

*Event Policies* enable an administrator to create specific notification mechanisms using one, some or all of the SNMP, syslog, controller forwarding or E-mail notification options available to the controller. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/encryption and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices. By default, there's no enabled event policy and one needs to be created and implemented.

When initially displayed, the **Event Policy** screen lists the access point interfaces. Existing policies can have their event notification configurations modified as device profile requirements warrant.

To define an access point event policy:

1. Select **Devices** from the Configuration menu.
2. Select **Event Policy**.

Event Name	SNMP <input type="checkbox"/>	Syslog <input type="checkbox"/>	Forward to Controller <input type="checkbox"/>	Email Notification <input type="checkbox"/>
radio-antenna-error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
resume-home-channel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
acs-scan-complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radar-scan-started	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
acs-scan-started	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radio-state-change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radar-detected	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radar-scan-completed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radio-antenna-setting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
channel-country-mismatch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Figure 5-221** Event Policy screen

3. Ensure the **Activate Event Policy** option is selected to enable the screen for configuration. This option needs to remain selected to apply the event policy configuration to the access point profile.
4. Refer to the **Select Event Module** drop-down menu on the top right-hand side of the screen and select an event module used to track the occurrence of each list event.
5. Review each event and select (or deselect) the *SNMP*, *Syslog*, *Forward to Switch* or *Email Notification* option as required for the event. Map an existing policy to a device profile as needed. Select Profile from the Map drop-down menu in the lower-left hand side of the screen. Expand the list of device profiles available, and apply the event policy as required.
6. Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. **Delete** obsolete rows as needed.

# CHAPTER 6

## WIRELESS CONFIGURATION

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

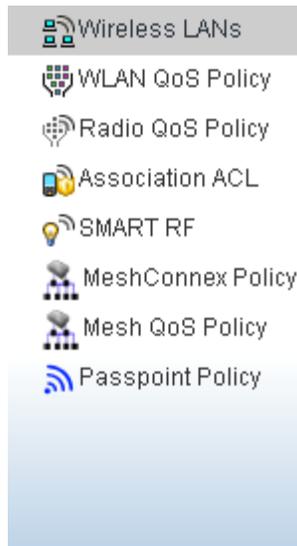
WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), E-mail, file and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

The wireless configuration is comprised of the following policies:

- *Wireless LANs*
  - *WLAN QoS Policy*
  - *Radio QoS Policy*
  - *Association ACL*
  - *SMART RF*
  - *MeshConnex Policy*
  - *Mesh QoS Policy*
  - *Passpoint Policy*
-



**Figure 6-1** Configuration > Wireless menu



<b>DHCP Option 82</b>	Displays if DHCP Option 82 is enabled or not. DHCP option 82 provides additional information on the physical attachment of a client
<b>Authentication Type</b>	Displays the name of the authentication scheme used by each listed WLAN to secure client transmissions. <i>None</i> is listed if authentication is not used within a WLAN. In case of no authentication, refer to the <i>Encryption Type</i> column to verify if there is some sort of data protection used with the WLAN, or risk using this WLAN with no protection at all.
<b>Encryption Type</b>	Displays the name of the encryption scheme used by each listed WLAN to secure client membership transmissions. <i>None</i> is listed if encryption is not used within this WLAN. In case of no encryption, refer to the <i>Authentication Type</i> column to verify if there is some sort of data protection used with the WLAN or risk using this WLAN with no protection at all.
<b>QoS Policy</b>	Lists the QoS policy applied to each listed WLAN. A QoS policy needs to be custom selected (or created) for each WLAN in respect to the WLAN's intended client traffic, and the voice, video or normal data traffic it supports.
<b>Association ACL</b>	Lists the Association ACL policy applied to each listed WLAN. An Association ACL is a policy-based <i>Access Control List</i> (ACL) that either prevents or allows wireless clients from connecting to a access point managed WLAN. The mapping of an Association ACL is strictly optional.

Use the sequential set of WLAN screens to define a unique configuration for each WLAN. Refer to the following to set WLAN configurations:

- [Basic WLAN Configuration](#)
- [Configuring WLAN Security](#)
- [Configuring WLAN Firewall Support](#)
- [Configuring Client Settings](#)
- [Configuring WLAN Accounting Settings](#)
- [Configuring Service Monitoring Settings](#)
- [Configuring Client Load Balancing](#)
- [Configuring Advanced WLAN Settings](#)
- [Configuring Auto Shutdown Settings](#)

## 6.1.1 Basic WLAN Configuration

### ► Wireless LANs

When creating or modifying a WLAN, the *Basic Configuration* screen is the first screen that displays as part of the WLAN configuration screen flow. Use this screen to enable a WLAN, and define its SSID, client behavior and VLAN assignments.

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select **Edit** to modify selected WLAN's properties. WLANs can also be removed as they become obsolete by selecting **Delete**.

**WLAN Configuration**

SSID ★ BranchSales

Description ⓘ Wlan for use of Sales Dept.

WLAN Status ⓘ  Disabled  Enabled

QoS Policy ★ default

Bridging Mode ⓘ Local

DHCP Option 82 ⓘ

**Other Settings**

Broadcast SSID ⓘ

Answer Broadcast Probes ⓘ

**VLAN Assignment**

Single VLAN

ⓘ VLAN 19

**RADIUS VLAN Assignment**

Allow RADIUS Override ⓘ

**Figure 6-3** WLAN Basic Configuration screen

5. Refer to the **WLAN Configuration** field to define the following:

<b>WLAN</b>	If adding a new WLAN, enter its name in the space provided. Spaces between words are not permitted. The name could be a logical representation of the WLAN coverage area (engineering, marketing etc.). If editing an existing WLAN, the WLAN's name appears at the top of the screen and cannot be modified. The name cannot exceed 32 characters.
<b>SSID</b>	Enter or modify the <i>Services Set Identification</i> (SSID) associated with the WLAN. The WLAN name is auto-generated using the SSID until changed by the user. The maximum number of characters for the SSID is 32.

<b>Description</b>	Provide a textual description for the WLAN to help differentiate it from others with similar configurations. A description can be up to 64 characters.
<b>WLAN Status</b>	Select the <i>Enabled</i> radio button to ensure this WLAN is active and available to clients on the radios where it has been mapped. Select the <i>Disabled</i> radio button to make this WLAN inactive, meaning even if the WLAN is mapped to radios, it is not available for clients to associate.
<b>QoS Policy</b>	Use the drop-down menu to assign an existing QoS policy to the WLAN. If needed, select the <i>Create</i> icon to define a new QoS policy or select the <i>Edit</i> icon to modify the configuration of a selected QoS Policy. QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or per the proportion configured. For information on creating a QoS policy that can be applied to a WLAN, see <a href="#">WLAN QoS Policy on page 6-46</a> .
<b>Bridging Mode</b>	Use the drop-down menu to specify the WLAN's bridging mode as either <i>Local</i> or <i>Tunnel</i> . Select <i>Local</i> to bridge VLAN traffic locally, or <i>Tunnel</i> to use a shared tunnel for bridging the WLAN's VLAN traffic. <i>Local</i> is the default setting.
<b>DHCP Option 82</b>	Select this option to enable DHCP Option 82. DHCP option 82 provides additional information on the physical attachment of a client. This setting is disabled by default.

6. Refer to the **Other Settings** field to define broadcast behavior within this specific WLAN.

<b>Broadcast SSID</b>	Select this radio button to broadcast SSIDs within beacons. If a hacker tries to isolate and hack a client SSID via a client, the ESSID displays since the ESSID is in the beacon. This feature is enabled by default.
<b>Answer Broadcast Probes</b>	Select this radio button to associate a client with a blank SSID (regardless of which SSID the wireless controller is currently using). This feature is enabled by default.

7. Refer to the **VLAN Assignment** field to add or remove VLANs for the selected WLAN, and define the number of clients permitted. Remember, users belonging to separate VLANs can share the same WLAN. It's not necessary to create a new WLAN for every VLAN in the network.

<b>Single VLAN</b>	Select this radio button to assign just one VLAN to this WLAN. Enter the VLAN ID that displays when the <i>Single VLAN</i> radio button is selected. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool.
--------------------	---

8. Select **Allow RADIUS Override** to allow the access point to override the client VLAN assignment and use the VLAN assigned by a RADIUS Server instead. If, as part of the authentication process, the RADIUS server returns a client's VLAN ID in a RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forwarded on that VLAN. If disabled, the RADIUS server returned VLAN ID is ignored and the VLAN configuration (defined in the preceding step) is used.

If RADIUS authentication fails, the VLAN defined is the VLAN assigned to the WLAN.

9. Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen back to the last saved configuration.

### 6.1.1.1 WLAN Basic Configuration Deployment Considerations

#### ▶ Basic WLAN Configuration

Before defining a WLAN's basic configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Deploy separate VLAN for providing secure WLAN access.
- Define separate VLAN for each WLAN providing guest access.

## 6.1.2 Configuring WLAN Security

#### ▶ Wireless LANs

Assign WLANs unique security configurations supporting authentication, captive portal (hotspot), self registration or encryption schemes as data protection requirements dictate.

**Select Authentication**

EAP
  EAP-PSK
  EAP-MAC
  MAC
  PSK / None

AAA Policy ▼

Reauthentication  30 (30 to 86,400)

---

**Captive Portal**

Enforcement  Captive Portal Enable  Captive Portal if Primary Authentication Fails

Captive Portal Policy ▼

---

**Passpoint Policy**

Passpoint Policy ▼

---

**MAC Registration**

Enable

Radius Group Name

Expiry Time 1500 (1 to 1,500 days)

Agreement Refresh 0 (0 to 100 days)

---

**External Controller**

Enable

Host  Hostname ▼

Proxy Mode  None ▼

---

**Select Encryption**

WPA/WPA2-TKIP
  WPA2-CCMP
  WEP 128
  KeyGuard
  WEP 64
  Open

No Encryption

OK Reset **Exit**

**Figure 6-4** WLAN Security screen

Authentication ensures only known and trusted users or devices access an access point managed WLAN. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as user name, password and secret-key information.

A client must authenticate to an access point to receive resources from the network. *802.1x EAP*, *802.1x EAP-PSK*, *MAC* and *PSK/None* authentication options are supported.

Refer to the following to configure a WLAN's authentication scheme:

- [802.1x EAP, EAP-PSK and EAP MAC](#)
- [MAC Authentication](#)
- [PSK / None](#)

Secure guest access to the network is referred to as captive portal. A captive portal is guest access policy for providing temporary and restrictive access to the access point managed wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

A captive portal policy provides secure authenticated access using a standard Web browser. A captive portal provides authenticated access by capturing and re-directing a wireless user's Web browser session to a login page, where a user must enter valid credentials to access the network. Once logged into the captive portal, additional *Agreement*, *Welcome* and *Fail* pages provide an administrator with a number of options for the screen flow and appearance.

Refer to [Captive Portal on page 6-11](#) for information on assigning a captive portal policy to a WLAN.

MAC Registration enables returning captive portal users faster authentication and access to the captive portal service. When the user connects to the captive portal for the first time, the MAC address of the user is recorded once the authentication is successful. The next time the device is used to access the captive portal, MAC Registration allows the device and the user to be authenticated faster.

Refer to [MAC Registration on page 6-12](#) for information on enabling and configuring MAC Registration.

Encryption is essential for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, *Wired Equivalent Privacy* (WEP) was the primary encryption mechanism. WEP has since been interpreted as flawed in many ways, and is not considered an effective standalone scheme for securing a WLAN. WEP is typically used with WLAN deployments supporting legacy clients. New deployments should use either WPA or WPA2 encryption.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized hacking. Decryption applies the algorithm in reverse, to restore the data to its original form. A sender and receiver must employ the same encryption/decryption method to interoperate. When both TKIP and CCMP are both enabled a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

Refer to the following to configure a WLAN's encryption scheme:

- [WPA/WPA2-TKIP](#)
- [WPA2-CCMP](#)
- [WEP 64](#)
- [WEP 128 and KeyGuard](#)

### 6.1.2.1 802.1x EAP, EAP-PSK and EAP MAC

#### ▶ [Configuring WLAN Security](#)

The *Extensible Authentication Protocol* (EAP) is the de-facto standard authentication method used to provide secure authenticated access to WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over wireless controller managed WLANs.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An access point passes EAP packets from the client to an authentication server on the wired side of the access point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.

802.1X EAP provides mutual authentication over the WLAN during authentication. The 802.1X EAP process uses credential verification to apply specific policies and restrictions to WLAN users to ensure access is only provided to specific wireless controller resources.

802.1X requires a 802.1X capable RADIUS server to authenticate users and a 802.1X client installed on each device accessing the EAP supported WLAN. An 802.1X client is included with most commercial operating systems, including Microsoft Windows, Linux and Apple OS X.

The RADIUS server authenticating 802.1X EAP users resides externally to the access point. User account creation and maintenance can be provided centrally using RFMS or individually maintained on each device. If an external RADIUS server is used, EAP authentication requests are forwarded.

When using PSK with EAP, packets are sent requesting a secure link using a pre-shared key. The access point and authenticating device must use the same authenticating algorithm and passcode. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP. The only encryption types supported with this are *TKIP*, *CCMP* and *TKIP-CCMP*.

To configure EAP on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its security properties.
5. Select **Security**.
6. Select **EAP**, **EAP-PSK** or **EAP MAC** as the Authentication Type.

Either authentication type enables the radio buttons for various encryption options as an additional measure of security with the WLAN that can be used with EAP.

Either select an existing **AAA Policy** from the drop-down menu, select the **Create** icon to the right of the AAA Policy parameter to create a new AAA policy, or select the **Edit** icon to modify the selected AAA policy's configuration.

*Authentication, authorization, and accounting (AAA)* is a framework for intelligently controlling access to the network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows. For information on defining a new AAA policy, see [AAA Policy on page 7-12](#).

7. Select the **Reauthentication** radio button to force EAP supported clients to reauthenticate. Use the spinner control set the number of seconds (from 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate to use the resources supported by the WLAN.
8. Select **OK** to update the WLAN's EAP configuration. Select **Reset** to revert back to the last saved configuration.

## EAP, EAP-PSK and EAP MAC Deployment Considerations

### ▶ [802.1x EAP, EAP-PSK and EAP MAC](#)

Before defining a *802.1x EAP*, *EAP-PSK* or *EAP MAC* supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends a valid certificate be issued and installed on devices providing 802.1X EAP. The certificate should be issued from an *Enterprise* or *public certificate authority* to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.

- If using an external RADIUS server for EAP authentication, Motorola Solutions recommends the round trip delay over the WAN does not exceed 150 ms. Excessive delay over a WAN can cause authentication and roaming issues and impact wireless client performance.

### 6.1.2.2 MAC Authentication

#### ► *Configuring WLAN Security*

MAC is a device-level authentication method used to augment other security schemes. MAC can be used open, with *WEP 64* or *WEP 128*, *KeyGuard*, *TKIP* or *CCMP*.

MAC authentication enables device-level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static *WEP*, *WPA-PSK* and *WPA2-PSK*). MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date access restrictions.

MAC authentication can only identify devices, not users. MAC authentication only references a client's wireless interface card MAC address when authenticating the device, it does not distinguish the device's user credentials. MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can mimic a trusted device within the network.

MAC authentication is enabled per WLAN, augmented with the use of a RADIUS server to authenticate each device. A device's MAC address can be authenticated against an access point's local RADIUS server (if supported) or centrally (from a datacenter). For RADIUS server compatibility, the format of the MAC address can be forwarded to the RADIUS server in non-delimited and or delimited formats:

To configure MAC authentication on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its security properties.
5. Select **Security**.
6. Select **MAC** as the Authentication Type.

Selecting MAC enables the radio buttons for the *Open*, *WEP 64*, *WEP 128*, *WPA/WPA2-TKIP*, *WPA2-CCMP* and *Keyguard* encryption options as additional measures for the WLAN.

7. Either select an existing AAA Policy from the drop-down menu or select the **Create** icon to the right of the AAA Policy parameter to display a screen where new AAA policies can be created. A default AAA policy is also available if configuring a WLAN for the first time and there's no existing policies. Select the **Edit** icon to modify the configuration of a selected AAA policy.

*Authentication, Authorization, and Accounting (AAA)* is a framework for intelligently controlling access to the wireless client managed network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows. For information on defining a new AAA policy, see [AAA Policy on page 7-12](#).

8. Select the **Reauthentication** radio button to force MAC supported clients to reauthenticate. Use the spinner control set the number of minutes (from 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate.
9. Select **OK** when completed to update the WLAN's MAC configuration. Select **Reset** to revert the screen back to the last saved configuration.

## MAC Authentication Deployment Considerations

### ▶ [MAC Authentication](#)

Before defining a MAC authentication configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- MAC authentication can only be used to identify end-user devices, not the users themselves.
- MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provision a MAC address on their device to mimic a trusted device.

### 6.1.2.3 PSK / None

#### ▶ [Configuring WLAN Security](#)

Open-system authentication can be referred to as no authentication, since no actual authentication and user credential validation takes place. When selecting PSK/None, a client requests (and is granted) authentication with no credential exchange.



**NOTE:** Although *None* implies no authentication, this option is also used when pre-shared keys are used for encryption (thus the /PSK in the description).

---



---

### 6.1.2.4 Captive Portal

#### ▶ [Configuring WLAN Security](#)

A *captive portal* is guest access policy that provides temporary and restrictive access to the wireless network. The primary means of securing such guest access is the use of a captive portal. For an overview of the captive portal process and information on how to define a captive portal policy that can be applied to a WLAN, see [Configuring Captive Portal Policies on page 9-2](#).

To assign a captive portal policy to a WLAN:

1. Select the **Configuration** tab from the Web UI.
  2. Select **Wireless**.
  3. Select **Wireless LANs** to display a high level display of existing WLANs.
  4. Select the **Add** button to create an additional WLAN or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.
  5. Select **Security**.
  6. Refer to the **Captive Portal** field within the WLAN security screen.
 

Select the **Captive Portal Enable** option if authenticated guess access is required with the selected WLAN. This feature is disabled by default.
  7. Select the **Captive Portal if Primary Authentication Fails** option to enable the captive portal policy if the primary authentication is unavailable
  8. Select the **Captive Portal Policy** to use with the WLAN from the drop-down menu. If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing captive portal policy. For more information, see [Configuring Captive Portal Policies on page 9-2](#).
  9. Select **OK** when completed to update the captive portal configuration. Select **Reset** to revert the screen back to the last saved configuration.
-

### 6.1.2.5 Passpoint Policy

#### ► *Configuring WLAN Security*

A Passpoint policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its properties.
5. Select **Security**.
6. Refer to the **Passpoint** field within the WLAN Policy security screen.
7. Select an existing Passpoint Policy from the drop down menu to apply it to the WLAN. If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing passpoint policy.
8. Select **OK** when completed to update the Captive Portal configuration. Select **Reset** to revert the *WLAN Policy Security* screen back to the last saved configuration.

### 6.1.2.6 MAC Registration

#### ► *Configuring WLAN Security*

The MAC Registration feature provides returning captive portal users quicker access to the captive portal.

When a user accesses the captive portal for the first time, user information is gathered and stored. This information is matched with the MAC address of the device accessing the captive portal. This information is stored on board the access point.

The next time the user accesses the captive portal service using the same device, he/she is authenticated immediately as the MAC address of the device is available in the access point's database along with the user's identification information. The user saves time as identification information is not collected again speeding the logon.

The MAC Registration feature must be enabled for each captive portal WLAN.

To enable MAC Registration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its properties.
5. Select **Security**.
6. Refer to the **MAC Registration** field within the WLAN security screen.  
Select the **MAC Registration Enable** option if quick access is required with the selected WLAN. This feature is disabled by default.
7. Select the RADIUS group name from the **Radius Group Name** drop-down list. A RADIUS group is a collection of user accounts that have same permissions.
8. Select **Expiry Time**. This is the duration for which MAC addresses are stored on the access point's database. Once this time expires, the user information is purged from the database. The user then has to provide login credentials as well as identification information again.
9. Set the **Agreement Refresh** as the amount of time before the agreement page is displayed if the user has not been logged during the specified period. The default setting is 0 days.

10. Select **OK** when completed to update the MAC Registration configuration. Select **Reset** to revert the screen back to the last saved configuration.

### 6.1.2.7 External Controller

#### ► *Configuring WLAN Security*

External controller configuration enables this WLAN to be managed by a remote wireless controller. This feature is disabled by default.

To configure the external server information:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its properties.
5. Select **Security**.
6. Refer to the **External Controller** field within the WLAN security screen.
7. Select the **Enable** option to enable this WLAN to be managed by an external controller.
8. Use the **Host** field to enter a hostname/IP address of the remote wireless controller. Use the spinner control to select the type of the remote controller.
9. Use the **Proxy Mode** drop-down to configure the proxy mode for accessing remote resources.
10. Select **OK** when completed to update the External Controller configuration. Select **Reset** to revert the screen back to the last saved configuration.

### 6.1.2.8 WPA/WPA2-TKIP

#### ► *Configuring WLAN Security*

*Wi-Fi Protected Access* (WPA) is an encryption scheme specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

The encryption method is *Temporal Key Integrity Protocol* (TKIP). TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector, however TKIP also has vulnerabilities.

*Wi-Fi Protected Access 2* (WPA2) is an enhanced version of WPA. WPA2 uses the *Advanced Encryption Standard* (AES) instead of TKIP. AES supports 128-bit, 192-bit and 256-bit keys. WPA/WPA2 also provide strong user authentication based on 802.1x EAP.

To configure WPA/WPA2 encryption on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify its properties.
5. Select **Security**.
6. Select the **WPA/WPA2-TKIP** radio button from within the **Select Encryption** field.

The screen populates with the parameters required to define a WPA/WPA2-TKIP configuration for the WLAN.

**Select Encryption**

WPA/WPA2-TKIP     WEP 128     WEP 64     Open  
 WPA2-CCMP     KeyGuard

**Key Settings**

Enter 64 HEX or 8-63 ASCII Characters

**Pre-Shared Key**  ASCII

**Key Rotation**

**Unicast Rotation Interval**  30 (30 to 86,400 seconds)

**Broadcast Rotation Interval**  30 (30 to 86,400 seconds)

**Advanced**

**TKIP Countermeasure Hold Time**  Minutes (0 to 1,093)

**Exclude WPA2 TKIP**

**Use SHA256**

OK    Reset    Exit

**Figure 6-5** WLAN Security - WPA/WPA2-TKIP screen

7. Define the **Key Settings**.

<b>Pre-Shared Key</b>	Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
-----------------------	---

8. Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for all clients in that subnet.

Motorola Solutions recommends rotating these keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

<b>Unicast Rotation Interval</b>	Define an interval for unicast key transmission interval from 30 - 86,400 seconds. Some clients have issues using unicast key rotation, so ensure you know which kind of clients are impacted before using unicast keys. This feature is disabled by default.
<b>Broadcast Rotation Interval</b>	When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default.

9. Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.



**NOTE:** Fast Roaming is available only when the authentication is *EAP* or *EAP-PSK* and the selected encryption is either *WPA/WPA2-TKIP* or *WPA-CCMP*.

Using 802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, **Opportunistic Key Caching** allows multiple access points to share PMKs amongst themselves. This allows a client to roam to an access point it has not previously visited and reuse a PMK from another access point to skip 802.1x authentication.

<b>Pre-Authentication</b>	Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1x authentication with other detected access points while still connected to its current access point. When a device roams to a neighboring access point, the device is already authenticated on the access point, thus providing faster re-association.
<b>Pairwise Master Key (PMK) Caching</b>	<i>Pairwise Master Key (PMK) Caching</i> is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1x authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated.
<b>Opportunistic Key Caching</b>	This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner.

10. Set the following **Advanced** settings for the WPA/WPA2-TKIP encryption scheme:

<b>TKIP Countermeasure Hold Time</b>	The <i>TKIP Countermeasure Hold Time</i> is the time a WLAN is disabled, if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either <i>Hours</i> (0-18), <i>Minutes</i> (0-1,092) or <i>Seconds</i> (0-65,535). The default setting is 60 seconds.
<b>Exclude WPA2-TKIP</b>	Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP, but do not support WPA2-CCMP. Motorola Solutions recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.
<b>Use SHA256</b>	Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits.

11. Select **OK** when completed to update the WLAN's WPA/WPA2-TKIP encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.



**NOTE:** WPA-TKIP is not supported on radios configured to exclusively use 802.11n.

---

---

### WPA-TKIP Deployment Considerations

Before defining a WPA-TKIP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Though TKIP offers better security than WEP, it can be vulnerable to certain attacks.
- When both TKIP and CCMP are enabled, a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

#### 6.1.2.9 WPA2-CCMP

##### ► *Configuring WLAN Security*

WPA2 is a newer 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the provided keys are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any for associated clients.

To configure WPA2-CCMP encryption on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.
5. Select **Security**.
6. Select the **WPA2-CCMP** radio button from within the select **Select Encryption** field.

The screen populates with the parameters required to define a WPA2-CCMP configuration for the WLAN.

---

**Select Encryption**

WPA/WPA2-TKIP
  WEP 128
  WEP 64
  Open

WPA2-CCMP
  KeyGuard

**Key Settings**

Enter 64 HEX or 8-63 ASCII Characters

**Pre-Shared Key**  ASCII

**Key Rotation**

**Unicast Rotation Interval**  30 (30 to 86,400 seconds)

**Broadcast Rotation Interval**  30 (30 to 86,400 seconds)

**Advanced**

**TKIP Countermeasure Hold Time**  Minutes (0 to 1,093)

**Exclude WPA2 TKIP**

**Use SHA256**

OK Reset Exit

**Figure 6-6** WLAN Security - WPA2-CCMP screen

7. Define **Key Settings**.

<b>Pre-Shared Key</b>	Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
-----------------------	---

8. Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2-CCMP, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for clients in that subnet.

Motorola Solutions recommends rotating these keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

<b>Unicast Rotation Interval</b>	Define a unicast key transmission interval from 30 - 86,400 seconds. Some clients have issues using unicast key rotation, so ensure you know which clients are impacted before using unicast keys. This value is disabled by default.
----------------------------------	---

<b>Broadcast Rotation Interval</b>	When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.
------------------------------------	---

9. Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.



**NOTE:** Fast Roaming is available only when the authentication is *EAP* or *EAP-PSK* and the selected encryption is either *WPA/WPA2-TKIP* or *WPA-CCMP*.

802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, Opportunistic Key Caching allows multiple access points to share PMKs amongst themselves. This allows a client to roam to an access point it has not previously visited and reuse a PMK to skip 802.1x authentication.

<b>Pre-Authentication</b>	Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1X authentication with other detected access points while still connected to its current access points. When a device roams to a neighboring access points, the device is already authenticated, thus providing faster re-association.
<b>Pairwise Master Key (PMK) Caching</b>	<i>Pairwise Master Key (PMK) Caching</i> is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1X authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated.
<b>Opportunistic Key Caching</b>	This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner.

10. Set the following **Advanced** for the WPA2-CCMP encryption scheme:

<b>TKIP Countermeasure Hold Time</b>	The <i>TKIP Countermeasure Hold Time</i> is the time a WLAN is disabled, if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either <i>Hours</i> (0-18), <i>Minutes</i> (0-1,092) or <i>Seconds</i> (0-65,535). The default setting is 60 seconds.
<b>Exclude WPA2-TKIP</b>	Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP, but do not support WPA2-CCMP. Motorola Solutions recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.

**Use SHA256**

Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits.

11. Select **OK** when completed to update the WLAN's WPA2-CCMP encryption configuration. Select **Reset** to revert back to its last saved configuration.

## WPA2-CCMP Deployment Considerations

### ▶ WPA2-CCMP

Before defining a WPA2-CCMP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends WPA2-CCMP be configured for all new (non visitor) WLANs requiring encryption, as it's supported by the majority of the hardware and client vendors using Motorola Solutions wireless networking equipment.
- WPA2-CCMP supersedes WPA-TKIP and implements all the mandatory elements of the 802.11i standard. WPA2-CCMP introduces a new AES-based algorithm called CCMP, which replaces TKIP and WEP and is considered significantly more secure.

### 6.1.2.10 WEP 64

#### ▶ Configuring WLAN Security

*Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP can be used with *open*, *shared*, *MAC* and *802.1X EAP* authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered.

WEP 64 uses a 40 bit key concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP 64 encryption on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select **Edit** to modify the properties of an existing wireless controller WLAN.
5. Select **Security**.
6. Select the **WEP 64** radio button from within the **Select Encryption** field.

The screen populates with the parameters required to define a WEP 64 configuration for the WLAN.

**Figure 6-7** WLAN Security - WEP 64 screen

7. Configure the following WEP 64 settings:

<b>Generate Keys</b>	Specify a 4 to 32 character pass key and select the <i>Generate</i> button. The pass key can be any alphanumeric string. The wireless controller, other proprietary routers, and Motorola Solutions clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola Solutions adapters need to use WEP keys manually configured as hexadecimal numbers.
<b>Keys 1-4</b>	Use the Key #1-4 fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. Select one of these keys for default activation by selecting its radio button. Select <i>Show</i> to display the actual characters comprising the key.
<b>Restore Default WEP Keys</b>	Select this radio button to restore the WEP algorithm back to its default settings.

Default WEP 64 keys are as follows:

- Key 1 1011121314
  - Key 2 2021222324
  - Key 3 3031323334
  - Key 4 4041424344
8. Select **OK** when completed to update the WLAN's WEP 64 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

## WEP 64 Deployment Considerations

Before defining a WEP 64 supported configuration on a WLAN, refer to the following deployment guideline to ensure the configuration is optimally effective:

- Motorola Solutions recommends additional layers of security (beyond WEP 64) be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with Firewall policies restricting access to hosts and suspicious network applications.

### 6.1.2.11 WEP 128 and KeyGuard

#### ▶ *Configuring WLAN Security*

*Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

KeyGuard is a Motorola Solutions encryption option used with legacy clients capable of supporting it. It closely resembled WEP 128 in key structure.

WEP can be used with *open*, *shared*, *MAC* and *802.1X EAP* authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication.

WEP 128 and KeyGuard use a 104 bit key which is concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices that are incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

WEP 128 or Keyguard provide a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.

To configure WEP 128 encryption on a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or select **Edit** to modify the properties of an existing WLAN.
5. Select **Security**.
6. Select either the **WEP 128** or **Keyguard** radio button from within the **Select Encryption** field.

The screen populates with the parameters required to define a WEP 128 or KeyGuard configuration for the WLAN.

**Figure 6-8** WLAN Security - WEP 128 screen

7. Configure the following WEP 128 or Keyguard settings:

<b>Generate Keys</b>	Specify a 4 to 32 character pass key and select the <i>Generate</i> button. The pass key can be any alphanumeric string. The access point, other proprietary routers, and Motorola Solutions clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola Solutions adapters need to use WEP keys manually configured as hexadecimal numbers.
<b>Keys 1-4</b>	Use the Key #1-4 areas to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by selecting its radio button. Select <i>Show</i> to display the actual characters comprising the key.
<b>Restore Default WEP Keys</b>	If you feel it necessary to restore the WEP algorithm back to its default settings, select the Restore Default WEP Keys button.

Default WEP 128 or Keyguard keys are as follows:

- Key 1 101112131415161718191A1B1C
  - Key 2 202122232425262728292A2B2C
  - Key 3 303132333435363738393A3B3C
  - Key 4 404142434445464748494A4B4C
8. Select **OK** when completed to update the WLAN's WEP 128 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

## WEP 128 and Keyguard Deployment Considerations

### ▶ [WEP 128 and KeyGuard](#)

Before defining a WEP 128 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends additional layers of security (beyond WEP) be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with Firewall policies restricting access to hosts and suspicious network applications.
- WEP enabled WLANs should only be permitted access to resources required by legacy devices.
- KeyGuard is not supported on AP6511 model access points.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

## 6.1.3 Configuring WLAN Firewall Support

### ▶ [Wireless LANs](#)

A Firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within an access point managed WLAN. The means by which this is accomplished varies, but in principle, a Firewall is a mechanism that blocks and permits data traffic. For a Firewall overview, see [Wireless Firewall on page 8-2](#).

WLANs use Firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on Layer 2 ports. An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical because the access point stops testing conditions after the first match.

IP based Firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

A MAC Firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical *allow*, *deny* or *mark* designation to WLAN packet traffic.

Keep in mind, IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

To review existing Firewall configurations, create a new Firewall configuration or edit the properties of a WLAN's existing Firewall:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create a new WLAN or **Edit** to modify the properties of an existing wireless controller WLAN.
5. Select **Firewall** from the WLAN options.

<b>IP Firewall Rules</b>	
Inbound IP Firewall Rules	<input type="text" value=""/>  
Outbound IP Firewall Rules	<input type="text" value=""/>  
<b>MAC Firewall Rules</b>	
Inbound MAC Firewall Rules	<input type="text" value=""/>  
Outbound MAC Firewall Rules	<input type="text" value=""/>  
<b>Association ACL</b>	
Association ACL	<input type="text" value=""/>  
<b>Trust Parameters</b>	
ARP Trust	<input type="checkbox"/>
Validate ARP Header Mismatch	<input checked="" type="checkbox"/>
DHCP Trust	<input type="checkbox"/>
<b>Wireless Client Deny</b>	
Wireless Client Denied Traffic Threshold	<input type="checkbox"/> <input type="text" value="1"/> (1 to 1,000,000 packets per second)
Action	<input type="text" value="None"/>
Blacklist Duration	<input type="checkbox"/> <input type="text" value="0"/> (0 to 86,400 seconds)
<b>Advanced</b>	
Firewall Session Hold Time	<input type="text" value="30"/> <input type="text" value="Seconds"/> (1 to 86,400)
<input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Exit"/>	

**Figure 6-9** WLAN Security - WLAN Firewall screen

6. Select an existing **Inbound IP Firewall Rules** or **Outbound IP Firewall Rules** using the drop-down menu. If no rules exist, select the **Create** icon to create a new firewall rule configuration. Select the **Edit** icon to modify the configuration of a selected firewall.

If creating a new rule, provide a name up to 32 characters long.

7. Select the **Add** button.

	Precedence	Action	Source	Destination	Protocol	Mark	Log	Status	Description
1	1	Deny	192.168.13.0/24	Any	TCP	N/A	Log	Enable	
2	2	Allow	\$NGA_01	192.168.13.10	TCP	Mark	Log	Enable	

**Figure 6-10** WLAN Security - IP Firewall Rules screen

8. IP Firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.
  - a. Select the **Edit Rule** icon to the left of a particular IP Firewall rule configuration to update its parameters collectively.

4

Allow

\$NGA\_01

192.168.13.10

6

Precedence: 4

Allow:  Allow:  Deny:

Source: alias

Source Network Group Alias: \$NGA\_01

Destination: host 192, 168, 13, 10

Network Service Alias:

Protocol: tcp 6

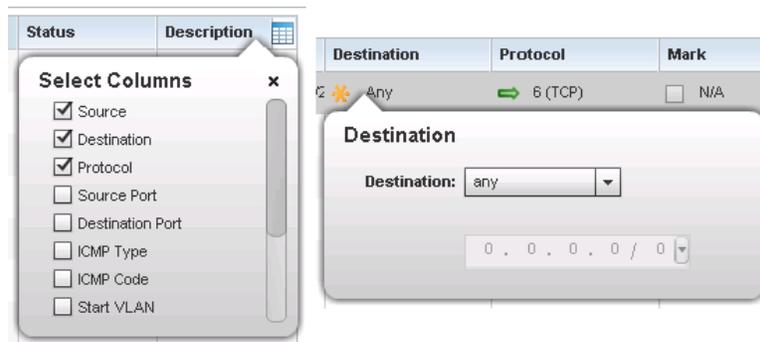
Source Port: any

Destination Port: any

Show More Options

**Figure 6-11** WLAN Security - IP Firewall Rules - Edit Rule screen

- b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.



**Figure 6-12** WLAN Security - IP Firewall Rules - IP Firewall Rules Add Criteria screen



**NOTE:** Only those selected IP ACL filter attributes display. Each value can have its current settings adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

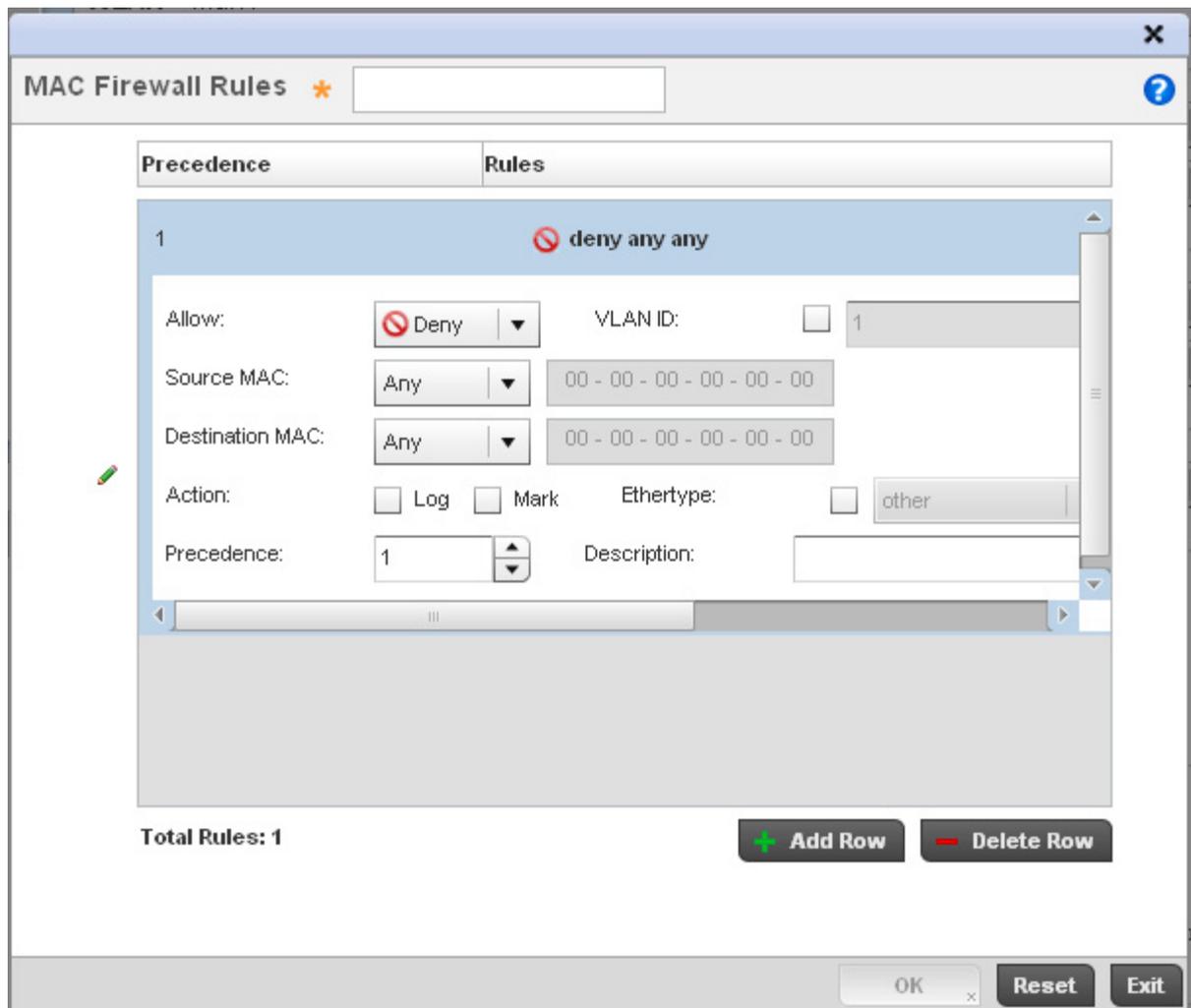
9. Define the following parameters for either inbound or outbound IP firewall rules:

<b>Precedence</b>	Specify or modify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
<b>Action</b>	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: <ul style="list-style-type: none"> <li>• <i>Deny</i> - Instructs the firewall to prohibit a packet from proceeding to its destination.</li> <li>• <i>Allow</i> - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
<b>Source</b>	Select the source IP address or network group configuration used as a basis matching criteria for this IP ACL rule. Source options include: <ul style="list-style-type: none"> <li>• <i>Any</i> – Indicates any host device in any network.</li> <li>• <i>Network</i> – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.</li> <li>• <i>Host</i> – Indicates a single host with a specific IP address.</li> <li>• <i>Alias</i> – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.</li> </ul>
<b>Destination</b>	Select the destination IP address or network group configuration used as a basis matching criteria for this IP ACL rule. Destination options include: <ul style="list-style-type: none"> <li>• <i>Any</i> – Indicates any host device in any network.</li> <li>• <i>Network</i> – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.</li> <li>• <i>Host</i> – Indicates a single host with a specific IP address.</li> <li>• <i>Alias</i> – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of ACL configuration. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.</li> </ul>

<b>Network Service Alias</b>	The service alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a \$ character and containing one special character) and include the protocol as relevant. Selecting either <i>tcp</i> or <i>udp</i> displays an additional set of specific TCP/UDP source and destinations port options.
<b>Source Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the source port for incoming IP ACL rule application is <i>any</i> , <i>equals</i> or an administrator defined <i>range</i> . If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting <i>equals</i> invokes a spinner control for setting a single numeric port. Selecting <i>range</i> displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings. A source port cannot be a destination port.
<b>Destination Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the destination port for incoming IP ACL rule application is <i>any</i> , <i>equals</i> or an administrator defined <i>range</i> . If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting <i>equals</i> invokes a spinner control for setting a single numeric port. Selecting <i>range</i> displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings.
<b>ICMP Type</b>	Selecting <i>ICMP</i> as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The <i>Internet Control Message Protocol</i> (ICMP) uses messages identified by numeric <i>type</i> . ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
<b>ICMP Code</b>	Selecting <i>ICMP</i> as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding <i>code</i> , helpful for troubleshooting network issues (0 - Net Unreachable, 1- Host Unreachable, 2 - Protocol Unreachable etc.).
<b>Start VLAN</b>	Select a <i>Start VLAN</i> icon within a table row to set (apply) a start VLAN range for this IP ACL filter. Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
<b>End VLAN</b>	Select an <i>End VLAN</i> icon within a table row to set (apply) an end VLAN range for this IP ACL filter. End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
<b>Protocol</b>	Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number.
<b>Mark</b>	Select this option to mark certain fields inside a packet before allowing them. Mark is only applicable for <i>Allow</i> rules. Mark sets the rule's 802.1p or <i>dscp</i> level (from 0 - 7)
<b>Log</b>	Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed.
<b>Enabled</b>	Select this option to enable or disable this particular IP Firewall rule in this rule set.
<b>Description</b>	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a <i>Select Columns</i> screen used to add or remove IP ACL criteria from the table.

The **Precedence** column sets the priority of a IP Firewall rule within its rule set. Click on this column and drag the rule to its appropriate place in the ruleset to set its precedence.

10. Click the **OK** button to save all changes made to the **IP Firewall Rules** dialog. Click **Exit** to close the dialog and return to the previous screen.
11. Select existing inbound or outbound **MAC Firewall Rules** using the drop-down menu. If no rules exist, select **Create** to display a screen where Firewall rules can be created.
12. Select the **+ Add Row** button.
13. Select the added row to expand it into configurable parameters.



**Figure 6-13** WLAN Security - MAC Firewall Rules screen

14. Define the following parameters for either the inbound or outbound **MAC Firewall Rules**:

<b>Allow</b>	<p>Every MAC firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:</p> <ul style="list-style-type: none"> <li>• <i>Deny</i> - Instructs the firewall to prohibit a packet from proceeding to its destination.</li> <li>• <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
--------------	---

<b>Source and Destination MAC</b>	Enter both <i>Source</i> and <i>Destination</i> MAC addresses. The access point uses the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.
<b>Action</b>	The following actions are supported: <ul style="list-style-type: none"> <li>• <i>Log</i> - Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted.</li> <li>• <i>Mark</i> - Modifies certain fields inside the packet, and then permits them. Therefore, mark is an action with an implicit permit.</li> <li>• <i>Mark, Log</i> - Conducts both mark and log functions.</li> </ul>
<b>Precedence</b>	Use the spinner control to specify a precedence for this MAC Firewall rule from 1-1500. Access policies with lower precedence are always applied first to packets.
<b>VLAN ID</b>	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the access point's local RADIUS server). Set the VLAN from 1 - 4094.
<b>Match 802.1P</b>	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting from 0 - 7.
<b>Ethertype</b>	Use the drop-down menu to specify an Ethertype of either <i>ipv6</i> , <i>arp</i> , <i>wisp</i> or <i>monitor 8021q</i> . An Ethertype is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame.
<b>Description</b>	Provide a description (up to 64 characters) for this rule to help differentiate it from others with similar configurations.

15. Save the changes to the new MAC rule, or reset to the last saved configuration as needed.
16. Define the following parameters for **Association ACL**. An Association ACL defines the rules used to allow/deny association to devices for this wireless LAN. If no Association ACL exists, select the **Create** button to display a new window where new ACL can be created.
17. Select the **+ Add Row** button.
18. Define the following parameters for **Association ACL**:

<b>Precedence</b>	Enter a numerical value indicating the precedence of rule execution.
<b>Starting MAC Address</b>	Enter a MAC address to define the start of range. This field is mandatory.
<b>Ending MAC Address</b>	Enter a MAC address to define the end of range.
<b>Allow/Deny</b>	Every Association ACL rule consists of matching criteria rules. The action defines what to do with the device if it matches the specified criteria. The following actions are supported: <ul style="list-style-type: none"> <li>• <i>Deny</i> - Instructs the Firewall to not to allow the device to associate with this WLAN.</li> <li>• <i>Permit</i> - Instructs the Firewall to allow the device to associate with this WLAN.</li> </ul>

19. Set the following **Trust Parameters**:

<b>ARP Trust</b>	Select this radio button to enable ARP trust on this WLAN. ARP packets received on this WLAN are considered trusted and information from these packets is used to identify rogue devices within the network. This setting is disabled by default.
------------------	---

<b>Validate ARP Header Mismatch</b>	Select this radio button to check for a source MAC mismatch in the ARP header and Ethernet header. This setting is enabled by default.
<b>DHCP Trust</b>	Select this radio button to enable DHCP trust on this WLAN. This setting is disabled by default.

20. Set the following **Wireless Client Deny** configuration:

<b>Wireless Client Denied Traffic Threshold</b>	If enabled, any associated client, exceeding the thresholds configured for storm traffic, is either <i>deauthenticated</i> or <i>blacklisted</i> depending on the selected action. The threshold range is from 1- 1000000 packets per second. This feature is disabled by default.
<b>Action</b>	If enabling a wireless client threshold, use the drop-down menu to determine whether clients are <i>deauthenticated</i> when the threshold is exceeded, or <i>blacklisted</i> from connectivity for a user-defined interval. Selecting <i>None</i> applies no consequence to an exceeded threshold.
<b>Blacklist Duration</b>	Select this option and define a setting from 0 - 86,400 seconds. Offending clients can reauthenticate, once this blacklist duration has been exceeded.

21. Set a **Firewall Session Hold Time** in either *Seconds* (1 - 300) or *Minutes* (1 - 5). This is the hold time for caching user credentials and Firewall state information when a client roams. The default setting is 30 seconds.
22. Select **OK** when completed to update this WLAN's Firewall settings. Select **Reset** to revert the screen back to its last saved configuration.

### WLAN Firewall Deployment Considerations

Before defining an access control configuration on a WLAN, refer to the following deployment guideline to ensure the configuration is optimally effective:

- IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

## 6.1.4 Configuring Client Settings

### ► Wireless LANs

Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations. AP6562, AP6532, AP6522, AP6522M, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 clients per access point. AP6511 and AP6521 models can support up to 128 clients per access point. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed.

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create a new WLAN, or select an existing WLAN and **Edit** to modify its properties.
5. Select the **Client Settings** tab.

**Client Settings**

- Enable Client-to-Client Communication
- Wireless Client Power  (0 to 20 dBm)
- Wireless Client Idle Time  Minutes (1 to 1,440)
- Max Firewall Sessions per Client  (10 to 10,000)
- Max Clients Allowed Per Radio  (0 to 256)
- Radio Resource Measurement
- Radio Resource Measurement Channel Report
- Enforce Client Load Balancing
- Enforce DHCP Client Only
- Proxy ARP Mode
- Enforce DHCP-Offer Validation

**Motorola Solutions Client Extensions**

- Move Operations
- Smart Scan
- Symbol Information Element
- WMM Load Information Element

**Timeout Settings**

- Credential Cache Timeout  Days (1 to 1)
- VLAN Cache Timeout  Hours (1 to 24)

**Mobility**

- Controller Assisted Mobility

OK Reset Exit

**Figure 6-14** WLAN - Client Settings screen

6. Define the following **Client Settings** for the WLAN:

<b>Enable Client-to-Client Communication</b>	Select this option to allow client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. Disabling this setting does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is disabled on the other WLAN, clients are not permitted to interoperate.
<b>Wireless Client Power</b>	Use this parameter to set the maximum transmit power (from 0 - 20 dBm) available to wireless clients for transmission. The default value is 20 dBm.
<b>Wireless Client Idle Time</b>	Set the maximum amount of time wireless clients are allowed to be idle within this WLAN. Set the idle time in either <i>Seconds</i> (60 - 86,400), <i>Minutes</i> (1 - 1,440), <i>Hours</i> (0 - 24) or <i>Days</i> (0 - 1). When this setting is exceeded, the client is no longer able to access resources and must re-authenticate. The default value is 1,800 seconds.
<b>Max Firewall Sessions per Client</b>	Select this option to set the maximum number of sessions (from 10 - 10,000 clients) over the Firewall. When enabled, this parameter limits the number of simultaneous sessions allowed by the Firewall per wireless client. This feature is disabled by default.
<b>Max Clients Allowed Per Radio</b>	Select this option to set the maximum number of clients (from 1- 256 clients) allowed to connect using a single radio. When enabled, this parameter limits the number of clients that are allowed to connect to a single radio. This feature is set to 256 by default.
<b>Radio Resource Measurement</b>	Select this option to enable radio resource measurement capabilities (IEEE 802.11k) on this WLAN. 802.11k improves how traffic is distributed. In a WLAN, each device normally connects to an access point with the strongest signal. Depending on the number and locations of the clients, this arrangement can lead to excessive demand on one access point and under utilization of others, resulting in degradation of overall network performance. With 802.11k, if the access point with the strongest signal is loaded to its capacity, a client connects to a under utilized access point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This setting is disabled by default.
<b>Radio Resource Measurement Channel Report</b>	Select this option to enable radio resource measurement channel reporting (IEEE 802.11k) on this WLAN. This setting is enabled by default.
<b>Enforce Client Load Balancing</b>	Select this option to distribute clients evenly amongst associated access point radios. This feature is disabled by default. An AP6562, AP6532, AP6522, AP6522M, AP71XX, AP75XX, AP81XX or AP82XX model access point can support up to 256 clients per access point. An AP6511 or AP6521 model can support up to 128 clients per access point. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed. Loads are balanced by ignoring association and probe requests. Probes and association requests are not responded to forcing a client to associate with another access point.
<b>Enforce DHCP Client Only</b>	Select this option to enforce that the access point only allows packets from clients using DHCP to obtain an IP address, disallowing static IP addresses. This feature is disabled by default.
<b>Proxy ARP Mode</b>	Use the drop-down menu to define the proxy ARP mode as either <i>Strict</i> or <i>Dynamic</i> . Proxy ARP is the technique used by the AP to answer ARP requests intended for another system. By faking its identity, the AP accepts responsibility for routing packets to the actual destination. Dynamic is the default value.

<b>Enforce DHCP-Offer Validation</b>	Select this option to enforce DHCP offer validation. The default setting is disabled.
--------------------------------------	---

7. Define the following **Motorola Solutions Client Extensions** for the WLAN:

<b>Move Operations</b>	Select the option to enable the use of <i>Motorola Solutions Fast Roaming</i> (HFSR) for clients on this WLAN. This feature applies only to certain Motorola Solutions client devices. This feature is disabled by default.
<b>Smart Scan</b>	Enable a smart scan to refine a clients channel scans to just a few channels as opposed to all available channels. This feature is disabled by default.
<b>Symbol Information Element</b>	Select this option to support the Symbol Information Element with legacy Symbol Technology clients. The default setting is enabled.
<b>WMM Load Information Element</b>	Select this option to support a WMM Load Information Element in radio transmissions with legacy Motorola Solutions clients. The default setting is disabled.

8. Define the following **Timeout Settings** for the WLAN:

<b>Credential Cache Timeout</b>	Set a timeout period for the credential cache in <i>Days</i> (0-1), <i>Hours</i> (0-24), <i>Minutes</i> (1-1440) or <i>Seconds</i> (60-86,4000). The default setting is 1 day.
<b>VLAN Cache Timeout</b>	Set a timeout period for the VLAN cache in <i>Days</i> (0-1), <i>Hours</i> (0-24), <i>Minutes</i> (1-1440) or <i>Seconds</i> (60-86,4000). The default setting is 1 hour.

9. Select **Controller Assisted Mobility** to use a controller or service platform's mobility database to assist in roaming between RF Domains. This feature is disabled by default.
10. Select **OK** when completed to update the WLAN's client setting configuration. Select **Reset** to revert the screen back to the last saved configuration.

## 6.1.5 Configuring WLAN Accounting Settings

### ► Wireless LANs

Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports and logs user activity to a RADIUS security server in the form of accounting records. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA.

Accounting can be enabled and applied to managed WLANs, to uniquely log accounting events specific to the WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a remote location for periodic network and user permission administration.

To configure WLAN accounting settings:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.
5. Select **Accounting**.

**Figure 6-15** WLAN Accounting screen

6. Set the following **Syslog Accounting** information:

<b>Enable System Log Accounting</b>	Select this option for the access point to generate accounting records in standard syslog format (RFC 3164). The feature is disabled by default.
<b>Syslog Host</b>	Specify the IP address (or hostname) of the external syslog host where accounting records are routed.
<b>Syslog Port</b>	Use the spinner control to set the destination UDP port of the external syslog host where accounting records are routed. The default port is 514.
<b>Proxy Mode</b>	Use the drop-down menu to define how syslog accounting is conducted. Options include <i>None</i> , <i>Through Wireless Controller</i> and <i>Through RF Domain Manager</i> .
<b>Format</b>	Select the format used to include (pack) the MAC address in a syslog request. Options include <i>No Delimiter (aabbccddeeff)</i> , <i>Colon Delimiter (aa:bb:cc:dd:ee:ff)</i> , <i>Dash Delimiter (aa-bb-cc-dd-ee-ff)</i> , <i>Dot Delimiter per four (aabb.ccdd.eef)</i> and <i>Middle Dash Delimiter (aabbcc-ddeeff)</i> . The default setting is Dash Delimiter (aa-bb-cc-dd-ee-ff).
<b>Case</b>	Use the drop-down menu to specify whether the MAC address format supplied is specified in <i>upper</i> or <i>lower</i> case. The default setting is upper case.

7. Select **Enable RADIUS Accounting** to use an external RADIUS resource for AAA accounting. When the radio button is selected, a **AAA Policy** field displays. Either use the default AAA policy with the WLAN, or select **Create** to define a new AAA configuration that can be applied to the WLAN. This setting is disabled by default.
8. Select **OK** when completed to update this WLAN's accounting settings. Select **Reset** to revert the screen back to its last saved configuration.

### **Accounting Deployment Considerations**

Before defining a AAA configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- When using RADIUS authentication, Motorola Solutions recommends the WAN port round trip delay not exceed 150 ms. Excessive delay over a WAN can cause authentication and roaming issues. When excessive delays exist, a distributed RADIUS service should be used.
- Motorola Solutions recommends authorization policies be implemented when users need to be restricted to specific WLANs, or time and date restrictions need to be applied.
- Authorization policies can also apply bandwidth restrictions and assign Firewall policies to users and devices.

### **6.1.6 Configuring Service Monitoring Settings**

#### ▶ *Wireless LANs*

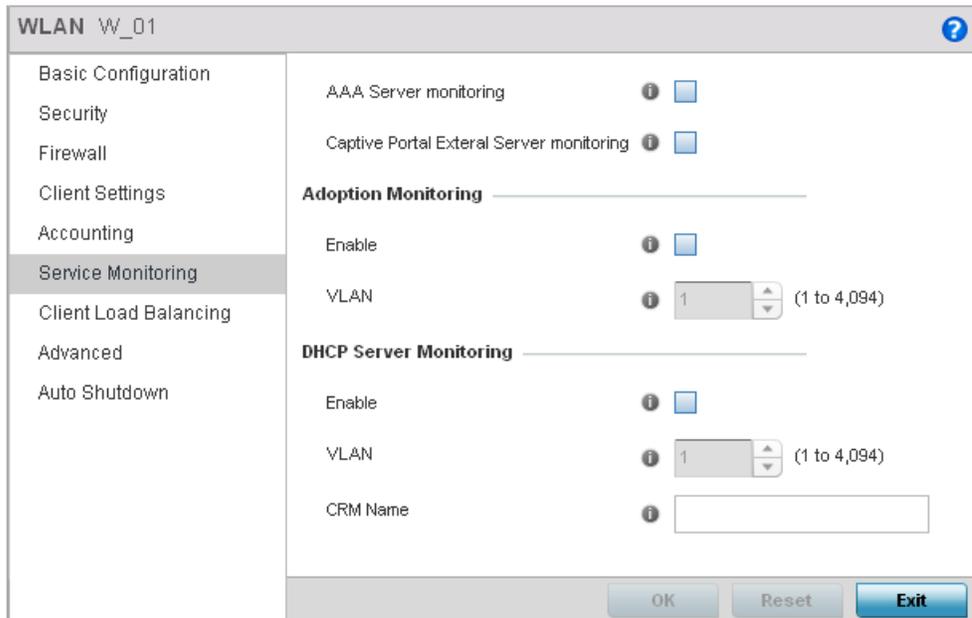
When a captive portal goes offline for any reason, the *Service Monitoring* feature enables the captive portal administrators to indicate to all users that the service is temporarily unavailable. As the service unavailable information is immediately displayed to the users, users are less likely to complain.

The reasons a captive portal service becomes unavailable can be broadly classified as:

- *When the RADIUS authentication server becomes unavailable. The RADIUS server could be on board the device (the wireless controller or the access point) or external to the device.*
- *When the configured external captive portal service is unavailable for any reason.*
- *In the case of an access point, if the wireless controller to which the access point is adopted becomes unavailable.*
- *When a monitored DHCP server becomes unavailable.*

To configure Service Monitoring settings:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.
5. Select **Service Monitoring**. The following screen displays:



**Figure 6-16** WLAN – Service Monitoring screen

6. Refer the following for more information on Service Monitoring fields.

<b>AAA Server Monitoring</b>	Select to enable monitoring the configured RADIUS server. Configure a RADIUS server through an AAA Policy. See <a href="#">AAA Policy on page 7-12</a> for more information.
<b>Captive Portal External Server Monitoring</b>	Select to enable monitoring the configured external captive portal server.
<b>Adoption Monitoring - Enable</b>	Select this option to verify if the device is adopted to its controller. When the connection to its controller is lost, all captive portal users are automatically migrated to the VLAN defined in the <i>Adoption Monitoring:VLAN</i> field.
<b>Adoption Monitoring - VLAN</b>	Use the spinner control to select the VLAN that users are migrated to when a device's connection to its adopting controller is lost.
<b>DHCP Server Monitoring - Enable</b>	Select to enable monitoring the configured DHCP Server. When the connection to the monitored DHCP server is lost, all captive portal are automatically migrated to the VLAN defined in the <i>DHCP Server Monitoring:VLAN</i> field.
<b>DHCP Server Monitoring - VLAN</b>	Use the spinner control to select the VLAN that users are migrated to when the configured DHCP becomes unavailable.
<b>DHCP Server Monitoring - CRM Name</b>	Configure the DHCP server to monitor. When this DHCP server becomes unavailable, the device falls back to the VLAN configured in the <i>DHCP Server Monitoring:VLAN</i> field. This VLAN has a DHCP server that provides a pool of IP addresses with a lease time lesser than the main DHCP server.

7. Select **OK** when completed to update this WLAN's service monitoring settings. Select **Reset** to revert the screen back to its last saved configuration.

## 6.1.7 Configuring Client Load Balancing

### ▶ Wireless LANs

Client load balance settings can be defined generically for both the 2.4 GHz and 5.0 GHz bands, and specifically for either of the 2.4 GHz or 5.0 GHz bands.

To configure client load balancing settings on an access point managed WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.
5. Select **Client Load Balancing**.

**Load Balancing Settings**

- Enforce Client Load Balancing**
- Band Discovery Interval**  **Seconds** ( 0 to 10,000 )
- Capability Ageout Time**  **Seconds** ( 0 to 10,000 )

**Load Balancing Settings (2.4GHz)**

- Single Band Clients**
- Max Probe Requests**  (0 to 10,000)
- Probe Request Interval**  **Seconds** ( 0 to 10,000 )

**Load Balancing Settings (5GHz)**

- Single Band Clients**
- Max Probe Requests**  (0 to 10,000)
- Probe Request Interval**  **Seconds** ( 0 to 10,000 )

**OK** **Reset** **Exit**

**Figure 6-17** WLAN - Client Load Balancing screen

6. Set the following **Load Balance Settings** generic to both the 2.4 GHz and 5.0 GHz bands:

<b>Enforce Client Load Balancing</b>	Select this radio button to enforce a client load balance distribution on this WLAN. This setting is disabled by default. Loads are balanced by ignoring association and probe requests. Probes and association requests are not responded to, forcing a client to associate with another access point.
<b>Band Discovery Interval</b>	Define a value in either <i>Seconds</i> (0 - 10,000), <i>Minutes</i> (0 -166) or <i>Hours</i> (0 -2) the access point uses to discover a client's band capabilities before associating. The default is 10 seconds.
<b>Capability Ageout Time</b>	Define a value in either <i>Seconds</i> (0 - 10,000), <i>Minutes</i> (0 -166) or <i>Hours</i> (0 -2) to ageout a client's capabilities from the access point's internal table. The default is 1 hour.

7. Set the following **Load Balancing Settings (2.4 GHz)**:

<b>Single Band Clients</b>	Select this option to enable single band client associations on the 2.4 GHz frequency, even if load balancing is available. The default setting is enabled.
<b>Max Probe Requests</b>	Enter a value (from 0 - 10,000) for the maximum number of probe requests for client associations on the 2.4 GHz frequency. The default value is 60.
<b>Probe Request Interval</b>	Enter a value in seconds (from 0 - 10,000) to set an interval for client probe requests, beyond which association is allowed for clients on the 2.4 GHz frequency. The default setting is 10 seconds.

8. Set the following **Load Balancing Settings (5 GHz)**:

<b>Single Band Clients</b>	Select this option to enable single band client associations on the 5.0 GHz frequency, even if load balancing is available. The default setting is enabled.
<b>Max Probe Requests</b>	Enter a value (from 0 - 10,000) for the maximum number of probe requests for client associations on the 5.0 GHz frequency. The default value is 60.
<b>Probe Request Interval</b>	Enter a value in seconds (from 0 - 10,000) to set an interval for client probe requests, beyond which association is allowed for clients on the 5.0 GHz frequency. The default setting is 10 seconds.

9. Select **OK** when completed to update this WLAN's client load balance settings. Select **Reset** to revert the screen back to its last saved configuration.

## 6.1.8 Configuring Advanced WLAN Settings

### ▶ *Wireless LANs*

To configure advanced RADIUS configuration and radio rate settings for a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.
5. Select **Advanced**.

**Figure 6-18** WLAN - Advanced Configuration screen

- Refer to the **Advanced RADIUS Configuration** field to set the WLAN's NAS configuration and RADIUS Dynamic Authorization.

<b>NAS Identifier</b>	Specify what is included in the RADIUS NAS-Identifier field for authentication and accounting packets. This is an optional setting, and defaults are used if no values are provided.
<b>NAS Port</b>	The profile database on the RADIUS server consists of user profiles for each connected <i>network access server</i> (NAS) port. Each profile is matched to a user name representing a physical port. When the access point authorizes users, it queries the user profile database using a user name representative of the physical NAS port making the connection.
<b>RADIUS Dynamic Authorization</b>	Select this radio button to enable the RADIUS protocol to support unsolicited messages sent from the RADIUS server. These messages allow administrators to issue <i>change of authorization</i> (CoA) messages, which affect session authorization, or <i>Disconnect Message</i> (DM), which cause a session to terminate immediately. This feature is disabled by default.

- Refer to the **Radio Rates** field to define selected data rates for both the 2.4 GHz and 5.0 GHz bands.

**Rate Settings 2.4GHz-wlan** [X]

**Radio Transmission Data Rates**

b-only rates   
 bg rates   
 bgn rates   
 Default  
 g-only rates   
 gn rates   
 Custom Rates

**802.11b Rates**

	1Mbps	2Mbps	5.5Mbps	11Mbps
Basic:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**802.11g Rates**

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input type="checkbox"/>							
Supported:	<input type="checkbox"/>							

**802.11n Rates**

	MCS0-7	MCS8-15	MCS16-23
Basic:	<input type="checkbox"/>		
Supported:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK    Reset    Cancel

**Figure 6-19** Advanced WLAN - Rate Settings 2.4 GHz-WLAN screen

8. For 2.4 GHz WLAN radio transmission rate settings, define the minimum *Basic* and *Supported* rates in the **802.11b Rates**, **802.11g Rates** and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

**Figure 6-20** Advanced WLAN - Rate Settings 5 GHz-WLAN screen

9. For 5.0 GHz WLAN radio transmission rate settings, define the minimum *Basic* and *Supported* rates in the **802.11a Rates**, and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

802.11n MCS rates are defined as follows both with and without *short guard intervals* (SGI):

**Table 6.1** MCS-1Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30
2	1	19.5	21.7	40.5	45
3	1	26	28.9	54	60
4	1	39	43.4	81	90
5	1	52	57.8	108	120
6	1	58.5	65	121.5	135
7	1	65	72.2	135	150

**Table 6.2** MCS-2Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240
6	2	117	130	243	270
7	2	130	144.4	270	300

**Table 6.3** MCS-3Stream

<b>MCS Index</b>	<b>Number of Streams</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>
0	3	19.5	21.7	40.5	45
1	3	39	43.3	81	90
2	3	58.5	65	121.5	135
3	3	78	86.7	162	180
4	3	117	130.7	243	270
5	3	156	173.3	324	360
6	3	175.5	195	364.5	405
7	3	195	216.7	405	450

802.11ac MCS rates are defined as follows both with and without *short guard intervals* (SGI):

**Table 6.4** MCS-802.11ac (theoretical throughput for single spatial streams)

<b>MCS Index</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>	<b>80 MHz No SGI</b>	<b>80MHz With SGI</b>
0	6.5	7.2	13.5	15	29.3	32.5
1	13	14.4	27	30	58.5	65
2	19.5	21.7	40.5	45	87.8	97.5
3	26	28.9	54	60	117	130
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260

**Table 6.4** MCS-802.11ac (theoretical throughput for single spatial streams)

<b>MCS Index</b>	<b>20 MHz No SGI</b>	<b>20 MHz With SGI</b>	<b>40 MHz No SGI</b>	<b>40MHz With SGI</b>	<b>80 MHz No SGI</b>	<b>80MHz With SGI</b>
6	58.5	65	121.5	135	263.3	292.5
7	65	72.2	135	150	292.5	325
8	78	86.7	162	180	351	390
9	n/a	n/a	180	200	390	433.3

10. Select the **Fast BSS Transition** option to enable 802.11r fast BSS transition support.

Fast BSS (802.11r) is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks.

11. Select **Enable** to enable HTTP analysis.

12. Set the following HTTP Analysis **Forward to Syslog Server** configuration:

<b>Enable</b>	Select this option to forward logging messages to an external syslog server.
<b>Host</b>	Use the field to provide a hostname/IP address of the remote syslog server. Use the drop-down menu to select the type of host address.
<b>Port</b>	Use the spinner control to configure the port on which the external syslog server can be reached.
<b>Proxy Mode</b>	Use the drop-down menu to select the proxy configuration.

13. Set the following **Filter** configuration for filtering specific contents from the information sent to a remote syslog server for HTTP analysis:

<b>Filter Out Images</b>	Select this option to filter images from the information logged to the remote syslog server.
<b>Filter Post</b>	Select this option to filter HTTP POST information from the information logged to the remote syslog server.
<b>Strip Query String</b>	Select this option to strip the query string in the information logged to the remote syslog server.

14. Select **OK** when completed to update this WLAN's Advanced settings. Select **Reset** to revert to the last saved configuration.

## 6.1.9 Configuring Auto Shutdown Settings

### ▶ Wireless LANs

Auto shutdown provides a mechanism to regulate the availability of a WLAN based on time. WLANs can be enabled or disabled depending on the day of the week and time of day.

A WLAN can be made available during a particular time of the day to prevent misuse and reduce the vulnerability of the wireless network. WLANs can be disabled when there are no users on the network, such as after hours or during the weekends/holidays. This enables the network administrator to have more time to manage the network as the mundane task of shutting down/starting up a WLAN is automated.

You can also use the *Auto Shutdown* screen to configure network parameters, which if not met, can force the WLAN to shut down. These parameters are:

- *Shutdown on Mesh Point Loss* – If an access point is a member in a meshed network and its connection to the mesh is lost, then all WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Primary Port Link Loss* – When there is a loss of link on the primary wired link on the access point, all the WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Critical Resource Down* – If critical resource monitoring is enabled on the access point and one or all of the monitored critical resource goes down, the all WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Unadoption* – If the access point is unadopted from its wireless controller, then all WLANs on the access point that have this option enabled are shut down.

To configure auto shutdown parameters for the selected WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LANs** to display a high level display of existing WLANs.
4. Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.
5. Select **Auto Shutdown**.

**Auto Shutdown**

Shutdown on Mesh Point Loss

Shutdown on Primary Port Link Loss

Shutdown on Critical Resource

Shutdown on Unadoption

**Time Based Access**

Days	Start Time	End Time	

+ Add Row

OK Reset Exit

**Figure 6-21** WLAN - Auto Shutdown screen

6. Refer to the following to configure **Auto Shutdown** parameters:

<b>Shutdown on Mesh Point Loss</b>	Select to enable the WLAN to shutdown if the access point's connection to the mesh network is lost. This setting is disabled by default.
<b>Shutdown on Primary Port Link Loss</b>	Select to enable the WLAN to shutdown if the access point's connection on its primary wired port is lost. This setting is disabled by default.
<b>Shutdown on Critical Resource Down</b>	Select to enable the WLAN to shutdown if any one or all of the access point's configured critical resources are not reachable or available. This setting is disabled by default.
<b>Shutdown on Unadoption</b>	Select to enable the WLAN to shutdown if the access point is unadopted from its wireless controller. This setting is disabled by default.

7. Select the **+ Add Row** button to add time based access configuration for the WLAN.  
 8. Refer to the following to configure **Time Based Access** parameters:

<b>Days</b>	Configure the days on which the WLAN is accessible. Select from one of the following: <ul style="list-style-type: none"> <li>• <i>All</i> – Select this option to make the WLAN available on all days of the week.</li> <li>• <i>Weekends</i> – Select this option to make the WLAN available only during weekends (Saturday and Sunday).</li> <li>• <i>Weekdays</i> – Select this option to make the WLAN available only during weekdays (from Monday to Friday).</li> <li>• <i>Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday</i> – Select a week day to make the WLAN available only during that specific day.</li> </ul>
<b>Start Time</b>	Configure the time when the WLAN is available. Start time is configured as HH:MM AM/PM.
<b>End Time</b>	Configure the time when the WLAN is unavailable. End time is configured as HH:MM AM/PM.

9. Select **OK** when completed to update this WLAN's Advanced settings. Select **Reset** to revert to the last saved configuration. Select **Exit** to exit the screen.



4. Refer to the following read-only information to determine whether an existing policy can be used as is, an existing policy requires edit or a new policy requires creation:

<b>WLAN QoS Policy</b>	Displays the name assigned to each listed WLAN QoS. The policy name cannot be edited.
<b>Wireless Client Classification</b>	Lists each policy's Wireless Client Classification as defined for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to a radio. Classification types include: <ul style="list-style-type: none"> <li>• <i>WMM</i> – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). The WMM classification is required to support the high throughput data rates required of 802.11n device support.</li> <li>• <i>Voice</i> – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <i>Video</i> – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <i>Normal</i> – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <i>Low</i> – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> </ul>
<b>SVP Prioritization</b>	A green check mark defines the policy as having <i>Spectralink Voice Prioritization (SVP)</i> enabled to allow the access point to identify and prioritize traffic from Spectralink/ Polycomm phones using the SVP protocol. Phones using regular WMM and SIP are not impacted by SVP prioritization. A red "X" defines the QoS policy as not supporting SVP prioritization.
<b>WMM Power Save</b>	Enables support for the WMM based power-save mechanism, also known as <i>Unscheduled Automatic Power Save Delivery (U-APSD)</i> . This is primarily used by WMM capable voice devices. The default setting is enabled.
<b>Multicast Mask Primary</b>	Displays the primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional, and only needed if there are traffic types requiring special handling.
<b>Multicast Mask Secondary</b>	Displays the secondary multicast mask defined for each listed QoS policy.



**NOTE:** When using a wireless client classification other than WMM, only legacy rates are supported on that WLAN.

5. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** its configuration. Existing QoS policies can also be selected and deleted as needed.

A **Quality of Service (QoS)** policy screen displays for the new or selected WLAN. The screen displays the **WMM** tab by default, but additional tabs also display for WLAN and wireless client rate limit configurations. For more information, refer to the following:

- [Configuring QoS WMM Settings](#)
- [Configuring a WLAN's QoS Rate Limit Settings](#)
- [Configuring Multimedia Optimizations](#)

## 6.2.1 Configuring QoS WMM Settings

### ► [WLAN QoS Policy](#)

Using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher priority.

WMM's prioritization capabilities are based on four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over the access point managed WLAN. ACs were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled access points coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized by default as having best effort priority. Applications assign each data packet to a given access category packets are then added to one of four independent transmit queues (one per access category - *voice*, *video*, *best effort* or *background*) in the client. The client has a collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client should be granted the *opportunity to transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category.

- The minimum inter-frame space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- The contention window, sometimes referred to as the random backoff wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest backoff value gets the TXOP.

To configure a WMM configuration for a WLAN:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.
4. Select the **Add** button to create a new QoS policy, or **Edit** to modify the properties of an existing WLAN QoS policy.

The **WMM** tab displays by default.

WLAN QoS Policy test ?

**WMM** Rate Limit Multimedia Optimizations

---

**Settings**

Wireless Client Classification WMM

Non-Unicast Classification Default

Enable Voice Prioritization

Enable SVP Prioritization

Enable WMM Power Save

Enable QBSS Load IE

Configure Non WMM Client Traffic Normal

---

**Voice Access**

Transmit Ops 47 (0 to 65,535)

AIFS Min 2 (2 to 15)

ECW Min 2 (0 to 15)

ECW Max 3 (0 to 15)

---

**Normal (Best Effort) Access**

Transmit Ops 0 (0 to 65,535)

AIFS Min 3 (2 to 15)

ECW Min 4 (0 to 15)

ECW Max 10 (0 to 15)

---

**Video Access**

Transmit Ops 94 (0 to 65,535)

AIFS Min 2 (2 to 15)

ECW Min 3 (0 to 15)

ECW Max 4 (0 to 15)

---

**Low (Background) Access**

Transmit Ops 0 (0 to 65,535)

AIFS Min 7 (2 to 15)

ECW Min 4 (0 to 15)

ECW Max 10 (0 to 15)

---

**Other Settings**

Trust IP DSCP

Trust 802.11 WMM QoS

OK Reset Exit

Figure 6-23 WLAN - WLAN QoS Policy screen - WMM tab

5. Configure the following **Settings** in respect to the WLAN's intended WMM radio traffic and user requirements:

<p><b>Wireless Client Classification</b></p>	<p>Use the drop-down menu to select the Wireless Client Classification for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to the radio. The Wireless Client Classification types are:</p> <ul style="list-style-type: none"> <li>• <i>WMM</i> – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). The WMM classification is required to support the high throughput data rates required of 802.11n device support.</li> <li>• <i>Voice</i> – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <i>Video</i> – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <i>Normal</i> – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <i>Low</i> – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> </ul>
--	---

<b>Non-Unicast Classification</b>	Use this drop-down menu to define how traffic matching multicast masks is classified relative to prioritization on the radio. Options include <i>Video</i> , <i>Voice</i> , <i>Normal</i> , <i>Low</i> and <i>Default</i> . The default setting is <i>Default</i> .
<b>Enable Voice Prioritization</b>	Select this option if <i>Voice</i> traffic is prioritized on the WLAN. This gives priority to voice and voice management packets and is supported only on certain legacy Motorola Solutions VOIP phones. This feature is disabled by default.
<b>Enable SVP Prioritization</b>	Enabling <i>Spectralink Voice Prioritization (SVP)</i> allows the access point to identify and prioritize traffic from Spectralink/Polycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy Motorola VOIP phones. If the <i>Wireless Client Classification</i> is <i>WMM</i> , non-WMM devices recognized as voice devices have all their traffic transmitted at voice priority. Devices are classified as voice, when they emit <i>SIP</i> , <i>SCCP</i> or <i>H323</i> traffic. Thus, selecting this option has no effect on devices supporting WMM. This feature is disabled by default.
<b>Enable WMM Power Save</b>	Enables support for the WMM based power-save mechanism, also known as <i>Unscheduled Automatic Power Save Delivery (U-APSD)</i> . This is primarily used by WMM capable voice devices. This feature is enabled by default.
<b>Enable QBSS Load IE</b>	Select this option to enable support for WMM QBSS load information element in beacons and probe response packets. This feature is enabled by default.
<b>Configure Non WMM Client Traffic</b>	Use the drop-down menu to specify how non-WMM client traffic is classified on this access point WLAN if the <i>Wireless Client Classification</i> is set to <i>WMM</i> . Options include <i>Video</i> , <i>Voice</i> , <i>Normal</i> and <i>Low</i> . The default setting is <i>Normal</i> .

6. Set the following **Video Access** settings for the WLAN's QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 94.
<b>AIFSN</b>	Set the current <i>Arbitrary Inter-frame Space Number (AIFSN)</i> from 2 - 15. Higher-priority video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

7. Set the following **Voice Access** settings for the WLAN's QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 47.
<b>AIFSN</b>	Set the current <i>Arbitrary Inter-frame Space Number (AIFSN)</i> from 2 - 15. Higher-priority voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.

<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

8. Set the following **Normal (Best Effort) Access** settings for the WLAN's QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0.
<b>AIFSN</b>	Set the current <i>Arbitrary Inter-frame Space Number</i> (AIFSN) from 2 - 15. The default value is 3. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access.
<b>ECW Min</b>	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic. The available range is from 0-15. The default value is 4.
<b>ECW Max</b>	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic. The available range is from 0-15. The default value is 10.

9. Set the following **Low (Background) Access** settings for the WLAN's QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
<b>AIFSN</b>	Set the current AIFSN from 2 - 15. The default value is 7. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access.
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic. The available range is from 0-15. The default value is 4.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic. The available range is from 0-15. The default value is 10.

10. Set the following **Other Settings** for the WLAN's QoS policy:

<b>Trust IP DSCP</b>	Select this option to trust IP DSCP values for WLANs. This feature is enabled by default.
<b>Trust 802.11 WMM QoS</b>	Select this option to trust 802.11 WMM QoS values for WLANs. This feature is enabled by default.

11. Select **OK** when completed to update this WLAN's QoS settings. Select **Reset** to revert the screen back to its last saved configuration.

## 6.2.2 Configuring a WLAN's QoS Rate Limit Settings

### ▶ *WLAN QoS Policy*

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. An administrator can set separate QoS rate limit configurations for data transmitted from the access point (upstream) and data transmitted from a WLAN's wireless clients back to their associated access point radios (downstream). AP6511 and AP6521 model access points do not support rate limiting on an individual client basis.

Before defining rate limit thresholds for WLAN upstream and downstream traffic, Motorola Solutions recommends you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

To configure a QoS rate limit configuration for a WLAN and connected clients:

1. Select the **Configuration** tab from the Web UI.
2. Select **Wireless**.
3. Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.
4. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** to modify its configuration.
5. Select the **Rate Limit** tab.

WLAN QoS Policy test ?

**WMM** **Rate Limit** **Multimedia Optimizations**

---

**Wireless LAN**

**Upstream Rate Limit**

Enable

Rate  (50 to 1,000,000 kbps)

Maximum Burst Size  (2 to 1,024 kbytes)

**Downstream Rate Limit**

Enable

Rate  (50 to 1,000,000 kbps)

Maximum Burst Size  (2 to 1,024 kbytes)

**Upstream Random Early Detection Threshold**

Background Traffic  (0 to 100 %)

Best Effort Traffic  (0 to 100 %)

Video Traffic  (0 to 100 %)

Voice Traffic  (0 to 100 %)

**Downstream Random Early Detection Threshold**

Background Traffic  (0 to 100 %)

Best Effort Traffic  (0 to 100 %)

Video Traffic  (0 to 100 %)

Voice Traffic  (0 to 100 %)

---

**Wireless Client**

**Upstream Rate Limit**

Enable

Rate  (50 to 1,000,000 kbps)

Maximum Burst Size  (2 to 1,024 kbytes)

**Downstream Rate Limit**

Enable

Rate  (50 to 1,000,000 kbps)

Maximum Burst Size  (2 to 1,024 kbytes)

**Upstream Random Early Detection Threshold**

Background Traffic  (0 to 100 %)

Best Effort Traffic  (0 to 100 %)

Video Traffic  (0 to 100 %)

Voice Traffic  (0 to 100 %)

**Downstream Random Early Detection Threshold**

Background Traffic  (0 to 100 %)

Best Effort Traffic  (0 to 100 %)

Video Traffic  (0 to 100 %)

Voice Traffic  (0 to 100 %)

**Figure 6-24** WLAN - WLAN QoS Policy screen - Rate Limit tab

6. Configure the following intended **Upstream Rate Limit** parameters for the selected WLAN:

<b>Enable</b>	Select this radio button to enable rate limiting for data transmitted from access point radios to associated clients on this WLAN. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.
<b>Rate</b>	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the WLAN (from all access categories). Traffic exceeding the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's wireless client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.
---------------------------	--

7. Set the following **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for the selected WLAN.

<b>Background Traffic</b>	Set a percentage for WLAN background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage for WLAN best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value, once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage for WLAN video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage for WLAN voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

8. Configure the following parameters in respect to the WLAN's intended **Downstream Rate Limit**, or traffic from wireless clients to associated access point radios:

<b>Enable</b>	Select this radio button to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
<b>Rate</b>	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the WLANs wireless client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.
---------------------------	---

9. Set the following **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when a traffic stream falls below the set threshold for the selected WLAN.

<b>Background Traffic</b>	Set a percentage for WLAN background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage for WLAN best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage for WLAN video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage for WLAN voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

10. Configure the following intended **Upstream Rate Limit** parameters for wireless client traffic:

<b>Enable</b>	Select this radio button to enable rate limiting for data transmitted from access point radios to associated clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.
<b>Rate</b>	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received from clients (from all access categories). Traffic exceeding the defined rate is dropped and a log message is generated. The default setting is 1000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes.
---------------------------	---

11. Set the following **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

<b>Background Traffic</b>	Set a percentage for client background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage for client best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value, once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage for client video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage for WLAN voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

12. Configure the following intended **Downstream Rate Limit** parameters for wireless client traffic:

<b>Enable</b>	Select this radio button to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
<b>Rate</b>	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received from clients. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 1,000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes.
---------------------------	---

13. Set the following **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

<b>Background Traffic</b>	Set a percentage for client background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage for client best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage for client video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage for client voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

## 6.2.3 Configuring Multimedia Optimizations

### ► WLAN QoS Policy

To configure multimedia optimizations for a WLAN:

1. Select **Configuration**.
2. Select **Wireless**.
3. Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.
4. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** to modify its configuration.
5. Select the **Multimedia Optimizations** tab.

WLAN QoS Policy test

WMM Rate Limit Multimedia Optimizations

**Multicast Mask**

Multicast Mask Primary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

Multicast Mask Secondary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

**Accelerated Multicast**

Disable Accelerated Multicast

Automatically Detect Multicast Streams

Forwarding QoS Classification Trust QoS Values

Manually Configure Multicast Addresses

Multicast IP Address	Classification	

+ Add Row

OK Reset Exit

**Figure 6-25** WLAN - WLAN QoS Policy Screen - Multimedia Optimizations

6. Configure the following parameters in respect to the intended **Multicast Mask**:

<b>Multicast Mask Primary</b>	Configure the primary multicast mask for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
<b>Multicast Mask Secondary</b>	Set a secondary multicast mask for the WLAN QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.

7. Set the following **Accelerated Multicast** settings:

<b>Disable Multicast Streaming</b>	Select this option to disable all Multicast Streaming on the WLAN.
------------------------------------	--

<b>Automatically Detect Multicast Streams</b>	Select this option to convert multicast packets to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are converted to unicast. When the stream is converted and queued for transmission, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they want.
<b>Manually Configure Multicast Addresses</b>	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

8. Select **OK** when completed to update this WLAN's Multimedia Optimizations settings. Select **Reset** to revert the screen back to its last saved configuration.

### 6.2.3.1 WLAN QoS Deployment Considerations

Before defining a QoS configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WLAN QoS configurations differ significantly from QoS policies configured for associated access point radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these access point radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must be also able to support WMM and use the parameters correctly while accessing the wireless network to truly benefit.
- Rate limiting is disabled by default on WLANs. To enable rate limiting, a threshold must be defined for WLAN.
- Before enabling rate limiting on a WLAN, a baseline for each traffic type should be performed. Once a baseline has been determined, a minimum 10% margin should be added to allow for traffic bursts.
- The bandwidth required for real-time applications such as voice and video are very fairly easy to calculate as the bandwidth requirements are consistent and can be realistically trended over time. Applications such as Web, database and E-mail are harder to estimate, since bandwidth usage varies depending on how the applications are utilized.

## 6.3 Radio QoS Policy

### ► *Wireless Configuration*

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customization best suited to each QoS policy's intended wireless client base.

Motorola Solutions access point radios and wireless clients support several *Quality of Service* (QoS) techniques enabling real-time applications (such as voice and video) to co-exist simultaneously with lower priority background applications (such as web, E-mail and file transfers). A well designed QoS policy should:

- *Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.*
- *Minimize the network delay and jitter for latency sensitive traffic.*
- *Ensure high priority traffic has a better likelihood of delivery in the event of network congestion.*
- *Prevent the ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.*

Within a Motorola Solutions wireless network, wireless clients supporting low and high priority traffic contend with one another for data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner than lower priority traffic. The EDCA defines four traffic classes (or access categories); voice (highest), video (next highest), best effort and background (lowest). The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported by connected radios.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they improve battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. An access point managed wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must be also able to support WMM and use the values correctly while accessing WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Access points support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. An access point allows flexible WLAN mapping with a static WMM access control value. When enabled on a WLAN, traffic forwarded from to a client is prioritized and forwarded based on the WLAN's WMM access control setting.



**NOTE:** Statically setting a WLAN WMM access category value only prioritizes traffic to the client.

---



---



<b>Implicit TPSEC</b>	A green check mark defines the policy as requiring wireless clients to send their traffic specifications to an access point before they can transmit or receive data. If enabled, this setting applies to just this radio's QoS policy. When enabled, the access point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If a client sends more traffic than configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TPSEC frames only.
<b>Voice</b>	A green check mark indicates voice prioritization QoS is enabled on the radio. A red X indicates voice prioritization QoS is disabled on the radio.
<b>Best Effort</b>	A green check mark indicates best effort QoS is enabled on the radio. A red X indicates best effort QoS is disabled on the radio.
<b>Video</b>	A green check mark indicates video prioritization QoS is enabled on the radio. A red X indicates video prioritization QoS is disabled on the radio.
<b>Background</b>	A green check mark indicates background prioritization QoS is enabled on the radio. A red X indicates that background prioritization QoS is disabled on the radio.

5. Either select **Add** to create a new radio QoS policy, or select an existing policy and select **Edit** to modify its configuration.

The screenshot shows the 'Radio QoS Policy' configuration screen with the 'WMM' tab selected. The screen is divided into four sections: Voice Access, Video Access, Normal (Best Effort) Access, and Low (Background) Access. Each section contains four configuration fields: Transmit Ops, AIFSN, ECW Min, and ECW Max. The values are as follows:

Access Category	Transmit Ops	AIFSN	ECW Min	ECW Max
Voice Access	47	1	2	3
Video Access	94	1	3	4
Normal (Best Effort) Access	0	3	4	6
Low (Background) Access	0	7	4	10

At the bottom right of the screen are three buttons: OK, Reset, and Exit.

**Figure 6-27** Radio QoS Policy screen - WMM tab

The **Radio QoS Policy** screen displays the **WMM** tab by default. Use the WMM tab to define the access category configuration (*CWMin*, *CWMax*, *AIFSN* and *TXOP* values) in respect to the type of wireless data planned for this new or updated radio QoS policy.

6. Set the following **Voice Access** settings for the radio QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. When resources are shared between a <i>Voice over IP</i> (VoIP) call and a low priority file transfer, bandwidth is normally exploited by the file transfer, thus reducing call quality or even causing the call to disconnect. With voice QoS, a VoIP call (a real-time session), receives priority, maintaining a high level of voice quality. For higher-priority traffic categories (like voice), the <i>Transmit Ops</i> value should be set to a low number. The default value is 47.
<b>AIFSN</b>	Set the current AIFSN value from 1 - 15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0 - 15. The default value is 2.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0 - 15. The default value is 3.

7. Set the following **Normal (Best Effort) Access** settings for the radio QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
<b>AIFSN</b>	Set the current AIFSN from 1 - 15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 3.
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like normal). The available range is from 0-15. The default value is 4.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like normal). The available range is from 0-15. The default value is 6.

8. Set the following **Video Access** settings for the radio QoS policy:

<b>Transmit Ops</b>	Use the spinner control to set the maximum duration a radio can transmit after obtaining a transmit opportunity. For higher-priority traffic categories (like video), this value should be set to a low number. The default value is 94.
<b>AIFSN</b>	Set the current AIFSN from 1 - 15. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.

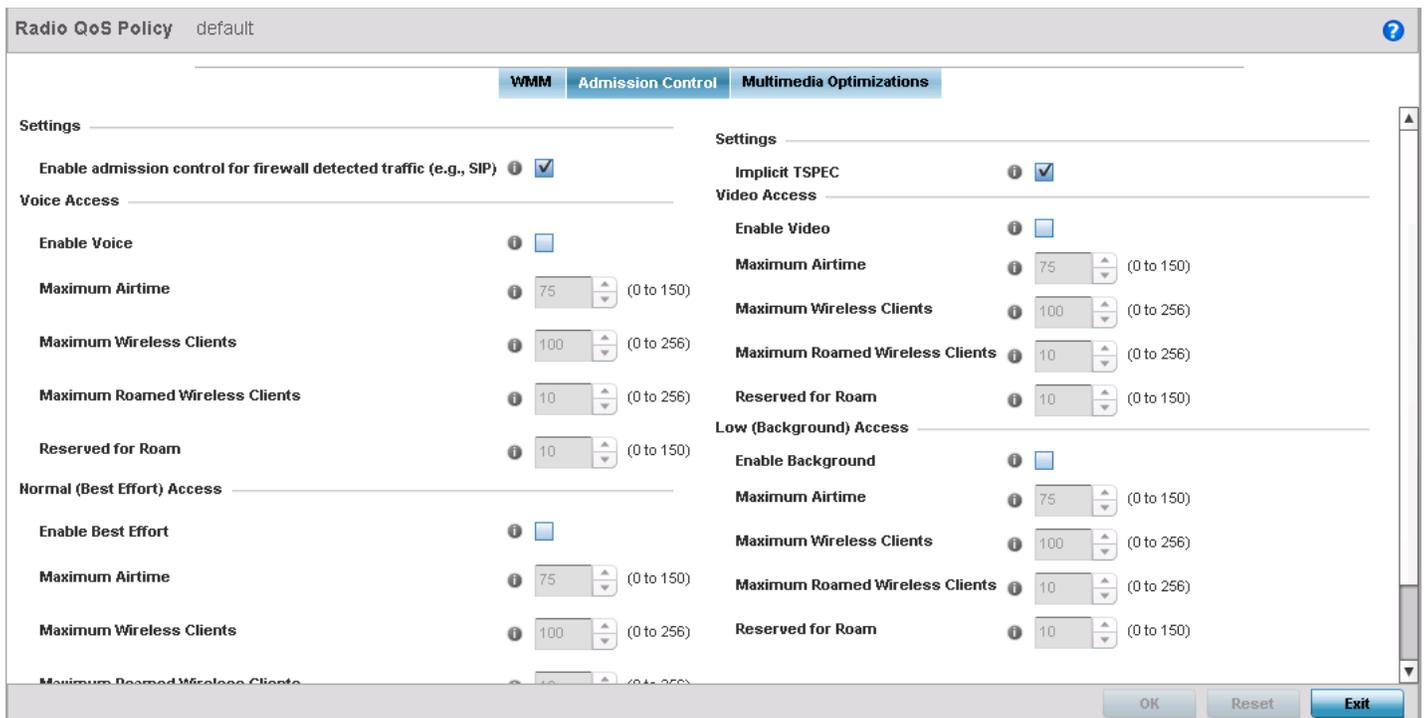
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

9. Set the following **Low (Background) Access** settings for the radio QoS policy:

<b>Transmit Ops</b>	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
<b>AIFSN</b>	Set the current AIFSN from 1- 15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 7.
<b>ECW Min</b>	<i>ECW Min</i> is combined with <i>ECW Max</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like low). The available range is from 0-15. The default value is 4.
<b>ECW Max</b>	<i>ECW Max</i> is combined with <i>ECW Min</i> to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 10.

10. Select **OK** when completed to update the radio QoS settings for this policy. Select **Reset** to revert back to last saved configuration.
11. Select the **Admission Control** tab to configure an admission control configuration for selected radio QoS policy. Admission control requires clients send their *traffic specifications* (TSPEC) to a managed access point before they can transmit or receive data within the access point managed network.

The name of the radio QoS policy, for which the admission control settings apply, displays in the banner of the QoS Policy screen.



**Figure 6-28** Radio QoS Policy screen - Admission Control tab

12. Select the **Enable admission control for firewall detected traffic (e.g., SIP)** option to apply radio QoS settings to traffic detected by the access point's firewall. This feature is enabled by default.
13. Select the **Implicit TPSEC** option to require wireless clients to send their traffic specifications to the access point before they can transmit or receive data. This feature is enabled by default.
14. Set the following **Voice Access** admission control settings for the radio QoS policy:

<b>Enable Voice</b>	Select this option to enable admission control for voice traffic. Only voice traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
<b>Maximum Airtime</b>	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. The available percentage range is from 0 - 150%, with 150% being available to account for over-subscription. This value ensures the radio's bandwidth is available for high bandwidth voice traffic (if anticipated on the wireless medium) or other access category traffic if voice support is not prioritized. Voice traffic requires longer radio airtime to process, so set a longer airtime value if the radio is intended to support voice. The default is 75%.
<b>Maximum Wireless Clients</b>	Set the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0 - 256 clients. Consider setting this value proportionally to the number of other QoS policies supporting the voice access category, as wireless clients supporting voice use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default is 100.
<b>Maximum Roamed Wireless Clients</b>	Set the number of voice supported wireless clients allowed to roam to a different access point radio. Select from 0 - 256 clients. The default value is 10.

<b>Reserved for Roam</b>	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different access point radio. The available percentage range is from 0 - 150%, with 150% available to account for over-subscription. The default value is 10%.
--------------------------	---

15. Set the following **Normal (Best Effort) Access** admission control settings for the radio QoS policy:

<b>Enable Best Effort</b>	Select this option to enable admission control for video traffic. Only normal background traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
<b>Maximum Airtime</b>	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background client traffic. The available percentage range is from 0 - 150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Normal background traffic only needs a short radio airtime to process, so set an intermediate airtime value if the radio QoS policy is reserved for background data support. The default value is 75%.
<b>Maximum Wireless Clients</b>	Set the number of wireless clients supporting background traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from 0 - 256 clients. The default value is 100.
<b>Maximum Roamed Wireless Clients</b>	Set the number of normal background supported wireless clients allowed to roam to a different managed access point radio. Select from 0 - 256 clients. The default value is 10.
<b>Reserved for Roam</b>	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background supported clients who have roamed to a different managed radio. The available percentage range is from 0 - 150%, with 150% available to account for over-subscription. The default value is 10%.

16. Set the following **Video Access** admission control settings for the radio QoS policy:

<b>Enable Video</b>	Select this option to enable admission control for video traffic. Only video traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
<b>Maximum Airtime</b>	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported client traffic. The available percentage range is from 0 - 150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for high bandwidth video traffic (if anticipated on the wireless medium) or other access category traffic if video support is not prioritized. Video traffic requires longer radio airtime to process, so set a longer airtime value if the radio QoS policy is intended to support video. The default value is 75%.
<b>Maximum Wireless Clients</b>	Set the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. Consider setting this value proportionally to the number of other QoS policies supporting the video access category, as wireless clients supporting video use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default value is 100.
<b>Maximum Roamed Wireless Clients</b>	Set the number of video supported wireless clients allowed to roam to a different access point radio. Select from 0-256 clients. The default value is 10.

<b>Reserved for Roam</b>	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different managed radio. The available percentage range is from 0 - 150%, with 150% accounting for over-subscription. The default value is 10%.
--------------------------	--

17. Set the following **Low (Background) Access** admission control settings for the radio QoS policy:

<b>Enable Background</b>	Select this option to enable admission control for lower priority traffic. Only low traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
<b>Maximum Airtime</b>	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low client traffic. The available percentage range is from 0 - 150%, with 150% being available to account for over-subscription. Best effort traffic only needs a short radio airtime to process, so set an intermediate airtime value if the radio QoS policy is reserved to support background data. The default value is 75%.
<b>Maximum Wireless Clients</b>	Set the number of low priority wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from 0 - 256 clients. The default value is 100.
<b>Maximum Roamed Wireless Clients</b>	Set the number of low priority supported wireless clients allowed to roam to a different access point radio. Select from 0-256 clients. The default value is 10.
<b>Reserved for Roam</b>	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for clients who have roamed to a different access point radio. The available percentage range is from 0 - 150%, with 150% available to account for over-subscription. The default value is 10%.

18. Select the **Multimedia Optimization** tab to configure advanced multimedia QoS configuration and Smart Aggregation configuration for the radio's QoS policy.

**Radio QoS Policy** default

**WMM** **Admission Control** **Multimedia Optimizations**

**Accelerated Multicast**

Maximum multicast streams allowed: 25 (0 to 256)

When wireless client count exceeds the above limit: Reject

Maximum multicast streams per client: 2 (1 to 4)

Packets per second for multicast flow for it to be accelerated: 25 (1 to 500)

Timeout for wireless clients: 60 (5 to 6,000)

**Smart Aggregation**

Smart Aggregation:

Max Delay for Best Effort: 150 (0 to 1,000)

Max Delay for Background: 250 (0 to 1,000)

Max Delay for Streaming Video: 150 (0 to 1,000)

Max Delay for Video Conferencing: 40 (0 to 1,000)

Max Delay for Voice: 0 (0 to 1,000)

Minimum Frames per Aggregate limit: 8 (0 to 64)

Max Mesh Links: 3 (1 to 10)

OK Reset Exit

**Figure 6-29** Radio QoS Policy screen - Multimedia Optimizations tab

19. Set the following **Accelerated Multicast** settings:

<b>Maximum number of wireless clients allowed</b>	Specify the maximum number of wireless clients (from 0 - 256) allowed to use accelerated multicast. The default value is 25.
<b>When wireless client count exceeds the above limit</b>	When the wireless client count using accelerated multicast exceeds the maximum number set the radio to either <i>Reject</i> new wireless clients or to <i>Revert</i> existing clients to a non-accelerated state. The default setting is <i>Reject</i> .
<b>Maximum multicast streams per client</b>	Specify the maximum number of multicast streams (from 1 - 4) wireless clients can use. The default value is 2.
<b>Packets per second for multicast flow for it to be accelerated</b>	Specify the threshold of multicast packets per second (from 1 - 500) that triggers acceleration for wireless clients. The default value is 25.
<b>Timeout for wireless clients</b>	Specify a timeout value in seconds (from 5 - 6,000) for wireless clients to revert back to a non-accelerated state. The default value is 60.

20. Set the following **Smart Aggregation** settings.

Smart Aggregation enhances the existing implementation of frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In the normal implementation of frame aggregation, an aggregated frame is sent when it meets one of these conditions:

- *When a preconfigured number of frames to aggregate is reached.*
- *When a preconfigured interval of time has elapsed since the first frame - of a set of frames to be aggregated - was received.*

- *When a preconfigured interval has elapsed since the last frame, not necessarily the final frame, - of a set of frames to be aggregated - was received.*

In this enhancement to the standard frame aggregation, the time delay for aggregation is set individually for each traffic class. For example, voice traffic might not be aggregated but sent immediately, whereas, background data traffic is set a time delay for aggregating frames and these aggregated frames are sent.

<b>Smart Aggregation</b>	Select to enable Smart Aggregation and dynamically set the time when an aggregated frame is transmitted.
<b>Max Delay for Best Effort</b>	Specify the maximum time in milliseconds to delay best effort traffic. The default setting is 150 millisecond.
<b>Max Delay for Background</b>	Specify the maximum time in milliseconds to delay background traffic. The default setting is 250 millisecond.
<b>Max Delay for Streaming Video</b>	Specify the maximum time in milliseconds to delay streaming video traffic. The default setting is 150 millisecond.
<b>Max Delay for Video Conferencing</b>	Specify the maximum time in milliseconds to delay video conferencing traffic. The default setting is 40 millisecond.
<b>Max Delay for Voice</b>	Specify the maximum time in milliseconds to delay voice traffic. The default setting is 0 millisecond.
<b>Minimum frames per Aggregate limit</b>	Specify the minimum number of frames to aggregate in a frame before it is transmitted. The default setting is 8 frames.
<b>Max Mesh Links</b>	Specify the maximum number of mesh links for Smart Aggregation. The default setting is 3.

21. Select **OK** to update radio QoS multimedia optimization settings Select **Reset** to revert to the last saved configuration.

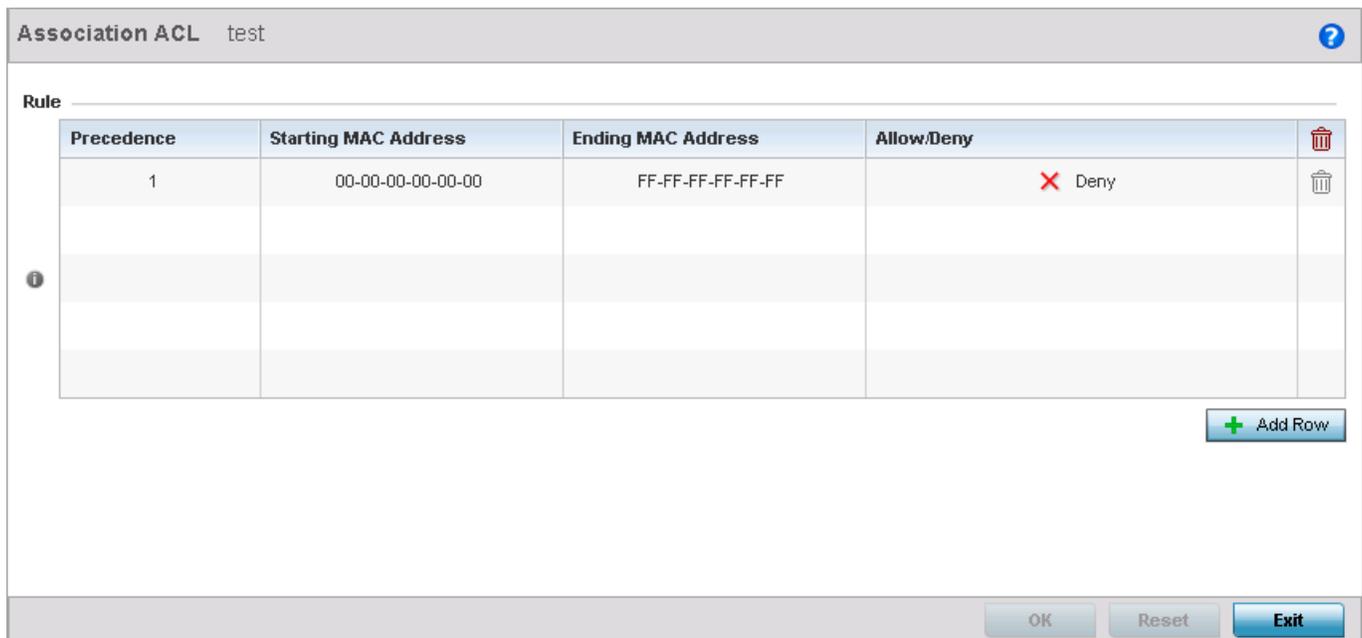
## Radio QoS Configuration and Deployment Considerations

### ▶ *Radio QoS Policy*

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client and WLAN is required to support WMM.
  - WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a best effort access category.
  - Motorola Solutions recommends default WMM values be used for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
  - Overloading an access point radio with too much high priority traffic (especially voice) degrades the overall service quality for all users.
  - TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TSPEC or even support WMM traffic prioritization.
-





**Figure 6-31** Association ACL screen

5. Select the **+ Add Row** button to add an association ACL template.
6. If creating a new **Association ACL**, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.
7. Set the following parameters for the creation or modification of the Association ACL:

<b>Precedence</b>	The rules within a WLAN's ACL are applied to packets based on their precedence values. Every rule has a unique sequential precedence value you define. You cannot add two rules's with the same precedence value. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.
<b>Starting MAC Address</b>	Provide a starting client MAC address for non unicast and multicast packet transmissions.
<b>Ending MAC Address</b>	Provide an ending MAC address for non unicast and multicast packet transmissions.
<b>Allow/Deny</b>	Use the drop-down menu to either <i>Allow</i> or <i>Deny</i> access if a MAC address matches this rule.

8. Select the **+ Add Row** radio button to add MAC address ranges and allow/deny designations.
9. Select **OK** to update the Association ACL settings. Select **Reset** to revert to the last saved configuration.

## 6.4.1 Association ACL Deployment Considerations

### ▶ Association ACL

Before defining an Association ACL configuration and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends using the Association ACL screen strategically to name and configure ACL policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
  - You cannot apply more than one MAC based ACL to a Layer 2 interface. If a MAC ACL is already configured on a Layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.
-

## 6.5 SMART RF

### ► *Wireless Configuration*

*Self Monitoring At Run Time RF Management* (SMART RF) is a Motorola Solutions innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization radio performance improvements.

Smart RF can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).



**NOTE:** Unlike a controller or service platform, an access point utilizes a single Smart RF configuration it can use with other access points of the same model. However, the Smart RF policy needs to be activated from any one of the Smart RF screens. Numerous Smart RF policies cannot be defined on behalf of the access point.

---



---

Smart RF also provides self-healing functions by monitoring the network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Motorola Solutions recommends you keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- *If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.*
- *If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channels specified in the Smart RF policy*
- *If no SMART RF policy is mapped, the radio selects a random channel*

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a `no dfs-rehome` command from the CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.



**NOTE:** RF planning must be performed to ensure overlapping coverage exists at a deployment site for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.



**CAUTION:** The access point's Smart RF feature is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections and communication disruptions.

---



---

To define the Smart RF configuration:

1. Select the **Configuration** tab from the Web UI.

2. Select **Wireless**.
3. Select **Smart RF**.

The **Basic Configuration** screen displays by default.

4. Select the **Activate SMART RF Policy** option to enable the parameters on the screen for configuration. The configuration cannot be applied to the access point profile unless this settings is selected and remains enabled.

**Figure 6-32** SMART RF - Basic Configuration screen

5. Refer to the **Basic Settings** field to enable a Smart RF policy and define its sensitivity and detector status.

<b>Sensitivity</b>	Select the radio button corresponding to the desired Smart RF sensitivity. Options include <i>Low, Medium, High</i> and <i>Custom</i> . The default setting is <i>Medium</i> .
<b>SMART RF Policy Enable</b>	Select this radio button to enable Smart RF for immediate inclusion within a RF Domain. Smart RF is enabled by default.
<b>Interference Recovery</b>	Select this radio button to enable compensations from neighboring radios when radio interference is detected. When interference is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This setting is enabled by default.
<b>Coverage Hole Recovery</b>	Select this radio button to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart RF supported radio coverage area. When coverage hole is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client as seen by the access point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold.
<b>Neighbor Recovery</b>	Select this radio button to enable automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss.

6. Refer to the **Calibration Assignment** field to define whether Smart RF Calibration and radio grouping is conducted by the floor the access point is deployed on or building in its entirety. Both options are disabled by default.
7. Select **OK** to update the access point's Smart RF Basic configuration. Select **Reset** to revert to the last saved configuration. The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand side, portion of the access point user interface.
8. Select **Channel and Power**. Ensure the **Activate SMART RF Policy** remains selected so the screen's parameters can be updated.

Use the Channel and Power screen to refine Smart RF power settings over both the 5.0 GHz and 2.4 GHz radio bands and select channel settings in respect to the access point's channel usage.



**NOTE:** The **Power Settings** and **Channel Settings** parameters are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

**Power Settings**

5 GHz Minimum Power  (1 to 20 dBm)

5 GHz Maximum Power  (1 to 20 dBm)

2.4 GHz Minimum Power  (1 to 20 dBm)

2.4 GHz Maximum Power  (1 to 20 dBm)

**Channel Settings**

5 GHz Channels

5 GHz Channel Width  20MHz  40MHz  Automatic

2.4 GHz Channels

2.4 GHz Channel Width  20MHz  40MHz  Automatic

**Area Based Channel Settings**

Area	Band	Channel List

OK Reset

**Figure 6-33** SMART RF - Channel and Power screen

9. Refer to the **Power Settings** field to define Smart RF recovery settings for the access point's 5.0 GHz (802.11a) and 2.4 GHz (802.11bg) radio.

<b>5 GHz Minimum Power</b>	Use the spinner control to select a 1 - 20 dBm minimum power level for Smart RF to assign to a radio in the 5.0 GHz band. The default setting is 4 dBm.
<b>5 GHz Maximum Power</b>	Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 5.0 GHz band. The default setting is 17 dBm.

<b>2.4 GHz Minimum Power</b>	Use the spinner control to select a 1 - 20 dBm minimum power level Smart RF can assign a radio in the 2.4 GHz band. The default setting is 4 dBm.
<b>2.4 GHz Maximum Power</b>	Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 2.4 GHz band. The default setting is 17 dBm.

10. Set the following **Channel Settings** for the access point's 5.0 GHz and 2.4 GHz radio bands:

<b>5 GHz Channels</b>	Use the <i>Select</i> drop-down menu to select the 5.0 GHz channels used in Smart RF scans.
<b>5 Channel Width</b>	20 MHz and 40 MHz channel widths are supported by the 802.11a radio. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both 2.4 GHz and 5.0 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of "wider channels." 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select Automatic to enable the automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. The default setting is 40 MHz.
<b>2.4 GHz Channels</b>	Use the <i>Select</i> drop-down menu to select the 2.4 GHz channels used in Smart RF scans.
<b>2.4 GHz Channel Width</b>	20 and 40 MHz channel widths are supported by the 802.11a radio. 20 MHz is the default setting for 2.4 GHz radios. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both 2.4 GHz and 5.0 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of "wider channels." 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select Automatic to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 20 MHz is the default setting.

11. Select the **+Add Row** button to add **Area Based Channel Settings**.
12. Set the following **Area Based Channel Settings** for the access point:

<b>Area</b>	Use the text area to provide a name for the area being configured.
<b>Band</b>	Use the drop-down menu to select the radio band to use in the area being configured.
<b>Channel List</b>	Use the <i>Select</i> drop-down menu to select the channels used in Smart RF area based channel settings.

13. Select **OK** to update the Smart RF Channel and Power settings for this policy. Select **Reset** to revert to the last saved configuration. The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand side, of the access point user interface.
14. Select **Scanning Configuration**. Ensure **Activate SMART RF Policy** remains selected so the screen's parameters can be updated. Additionally, the Smart RF configuration cannot be applied to the access point profile unless this setting remains selected.

**Monitoring Configuration**

Smart Monitoring Enable

**OCS Monitoring Awareness**

Threshold  10 (10 to 10,000)

Index	Day	Start Time	End Time	

**Scanning Configuration for 5.0 GHz**

Mesh Point

Duration  50 (20 to 150 milliseconds)

Frequency  6 Seconds (1 to 120)

Extended Scan Frequency  5 (0 to 50)

Sample Count  5 (1 to 15)

**Figure 6-34** SMART RF - Scanning Configuration screen



**NOTE:** The monitoring and scanning parameters within the Scanning Configuration screen are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

15. Enable or disable **Smart Monitoring Enable** by selecting the option. The feature is enabled by default. When enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.
16. Select this option and specify a threshold number between 10 and 10,000. When this threshold is reached, awareness settings will be overridden with the values specified.
17. Select an index value from 1-3 for awareness overrides. The overrides are executed based on index as defined in the table, with the lowest index being executed first.

<b>Day</b>	Use the drop-down menu to select a day of the week to apply the override. Selecting <i>All</i> will apply the policy every day. Selecting <i>weekends</i> will apply the policy on Saturdays and Sundays only. Selecting <i>weekdays</i> will apply the policy on Monday, Tuesday, Wednesday, Thursday and Friday. Selecting individual days of the week will apply the policy only on the selected day.
<b>Start Time</b>	This value sets the starting time of day(s) that the overrides will be activated. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose <i>AM</i> or <i>PM</i> .

<b>End Time</b>	This value sets the ending time of day(s) the overrides will be disabled. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose <i>AM</i> or <i>PM</i> .
-----------------	--

18. Set the following **Scanning Configurations** for *both* the 2.4 GHz and 5.0 GHz radio bands:

<b>Duration</b>	Set a channel scan duration (from 20 - 150 milliseconds) access point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain. The default setting is 50 milliseconds for both 2.4 GHz and 5.0 GHz bands.
<b>Frequency</b>	Set the scan frequency using the drop-down menu. Set a scan frequency in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (0 - 2). The default setting is 6 seconds for both 2.4 GHz and 5.0 GHz bands.
<b>Extended Scan Frequency</b>	Use the spinner control to set an extended scan frequency from 0 - 50. This is the frequency radios scan channels on non-peer radios. The default setting is 5 for both 2.4 GHz and 5.0 GHz bands.
<b>Sample Count</b>	Use the spinner control to set a sample scan count value from 1 - 15. This is the number of radio RF readings gathered before data is sent to the Smart RF master. The default setting is 5 for both 2.4 GHz and 5.0 GHz bands.
<b>Client Aware Scanning</b>	Use the spinner control to set a client awareness count (1 - 255) during off channel scans for either the 2.4 or 5.0 GHz radio. The default setting is 1 for both radio bands.
<b>Power Save Aware Scanning</b>	Select either the <i>Dynamic</i> , <i>Strict</i> or <i>Disable</i> radio button to define how power save scanning is set for Smart RF. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is Dynamic for both 2.4 GHz and 5.0 GHz bands.
<b>Voice Aware Scanning</b>	Select either <i>Dynamic</i> , <i>Strict</i> or <i>Disable</i> to define how voice aware recognition is set for Smart RF. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio. The default setting is Dynamic for both 2.4 GHz and 5.0 GHz bands.

19. Select **OK** to update the Smart RF Scanning Configuration settings. Select **Reset** to revert to the last saved configuration.

20. Select **Recovery**.

The **Neighbor Recovery** tab displays by default. Use the *Neighbor*, *Interference* and *Coverage Hole* recovery tabs to define how 2.4 and 5.0 GHz radios compensate for failed neighbor radios, interference, coverage holes and loss of root path requiring neighbor radio intervention.

**Neighbor Recovery** | **Interference Recovery** | **Coverage Hole Recovery**

**Hold Time**

Power Hold Time  Seconds (0 to 3,600)

**Neighbor Recovery**

5 GHz Neighbor Power Threshold  (-85 to -55 dBm)

2.4 GHz Neighbor Power Threshold  (-85 to -55 dBm)

**Dynamic Sample Recovery**

Dynamic Sample Enabled

Dynamic Sample Retries  (1 to 10)

Dynamic Sample Threshold  (1 to 30)

**Note:** The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.

**OK** **Reset**

**Figure 6-35** SMART RF Recovery Configuration screen - Neighbor Recovery tab

<b>Power Hold Time</b>	Defines the minimum time between two radio power changes during neighbor recovery. Set the time in either <i>Seconds</i> (0 - 3,600), <i>Minutes</i> (0 - 60) or <i>Hours</i> (0 - 1). The default setting is 0 seconds.
------------------------	--

21. Set the following **Neighbor Recovery** variables for the Smart RF configuration:



**NOTE:** The recovery parameters within the *Neighbor Recovery*, *Interference* and *Coverage Hole Recovery* tabs are only enabled when *Custom* is selected as the Sensitivity setting from the Smart RF Basic Configuration screen.

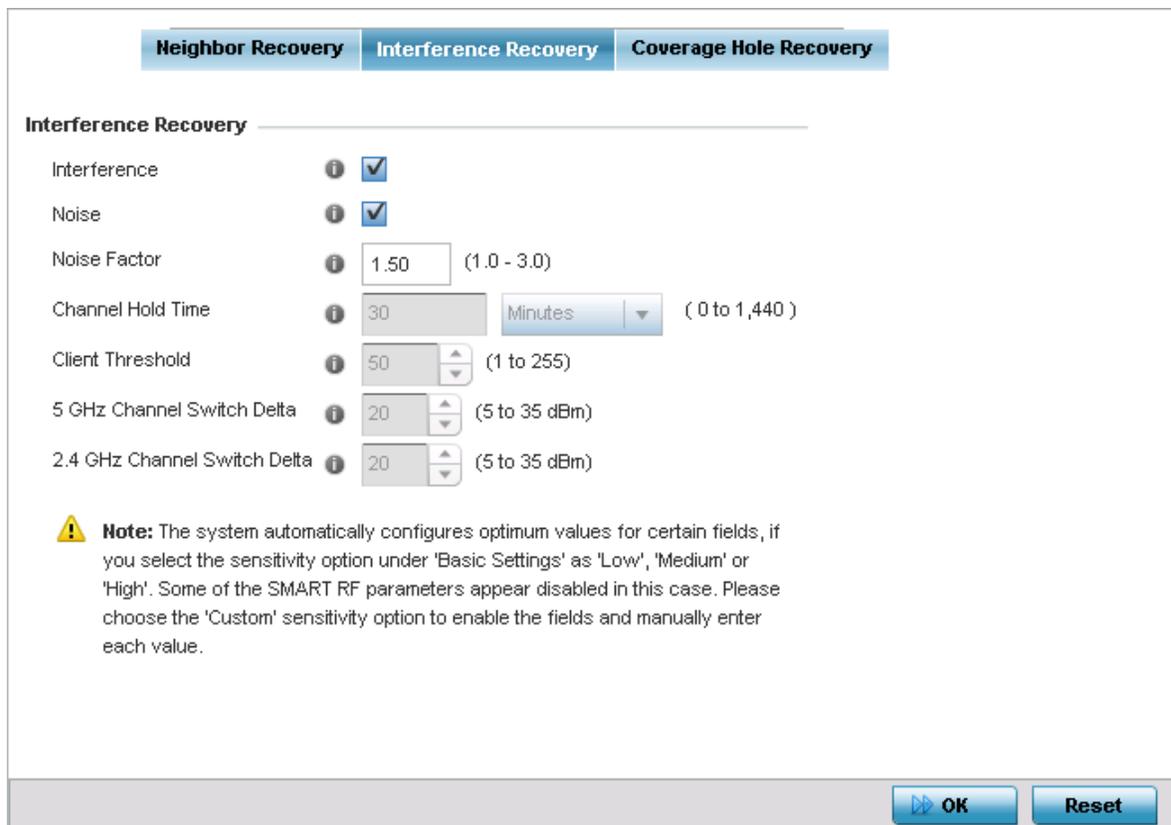
<b>5GHz Neighbor Power Threshold</b>	Use the spinner control to set a value from -85 to -55 dBm the access point's 5.0 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm.
<b>2.4 GHz Neighbor Power Threshold</b>	Use the spinner control to set a value from -85 to -55 dBm the access point's 2.4 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm.

22. Set the following **Dynamic Sample Recovery** parameters:

<b>Dynamic Sample Enabled</b>	Select this option to enable dynamic sampling. Dynamic sampling enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This setting is disabled by default.
<b>Dynamic Sample Retries</b>	Use the spinner control to set the number of retries (1 - 10) before a power change is allowed to compensate for a potential coverage hole. The default setting is 3.
<b>Dynamic Sample Threshold</b>	Use the spinner control to set the number of sample reports (1 - 30) used before dynamic sampling is invoked for a potential power change adjustment. The default setting is 5.

23. Select **OK** to update the Smart RF Neighbor Recovery settings. Select **Reset** to revert to the last saved configuration.

24. Select the **Interference Recovery** tab.



**Figure 6-36** SMART RF Recovery Configuration screen - Interference Recovery tab

25. Set the following **Interference Recovery** parameters:

<b>Interference</b>	Select this radio button to allow Smart RF to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default.
<b>Noise</b>	Select this radio button to allow Smart RF to scan for excess noise from WiFi devices. When detected, Smart RF supported access points can change their channel and move to a cleaner channel. This feature is enabled by default.

<b>Channel Hold Time</b>	Defines the minimum time between channel changes during neighbor recovery. Set the time in either <i>Seconds</i> (0 - 86,400), <i>Minutes</i> (0 - 1,440) or <i>Hours</i> (0 - 24) or <i>Days</i> (0 - 1). The default setting is 30 minutes.
<b>Client Threshold</b>	Use the spinner to set a client threshold from 1 - 255. If the threshold defined number of clients are connected to a radio, the radio does not change its channel, even though required, based on the interference recovery determination made by the smart master. The default setting is 50.
<b>5 GHz Channel Switch Delta</b>	Use the spinner to set a channel switch delta (from 5 - 35 dBm) for the 5.0 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm.
<b>2.4 GHz Channel Switch Delta</b>	Use the spinner to set a channel switch delta (from 5 - 35 dBm) for the 2.4 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm.

26. Select **OK** to update the Smart RF Interference Recovery settings. Select **Reset** to revert to the last saved configuration.
27. Select the **Coverage Hole Recovery** tab.

The screenshot displays the 'Coverage Hole Recovery' configuration window. At the top, there are three tabs: 'Neighbor Recovery', 'Interference Recovery', and 'Coverage Hole Recovery', with the latter being the active tab. The window is divided into two main sections: 'Coverage Hole Recovery for 5.0 GHz' and 'Coverage Hole Recovery for 2.4 GHz'. Each section contains four settings: 'Client Threshold' (spinner from 1 to 255), 'SNR Threshold' (spinner from 1 to 75 dB), 'Coverage Interval' (spinner from 1 to 120 with a unit dropdown set to 'Seconds'), and 'Interval' (spinner from 1 to 120 with a unit dropdown set to 'Seconds'). All settings are currently set to their default values. At the bottom of the window, there is a 'Note' with a warning icon: 'Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.' At the bottom right, there are two buttons: 'OK' and 'Reset'.

**Figure 6-37** SMART RF Recovery Configuration screen - Coverage Hole Recovery tab

28. Set the following **Coverage Hole Recovery for 5.0 GHz** and **2.4 GHz** parameters:

<b>Client Threshold</b>	Use the spinner to set a client threshold from 1 - 255. This is the minimum number of clients a radio should have associated for coverage hole recovery to trigger. AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points can support up to 256 clients per access point or radio. AP6511 and AP6521 model access points can support up to 128 clients per access point or radio. The default setting is 1.
<b>SNR Threshold</b>	Use the spinner control to set a <i>signal to noise</i> (SNR) threshold (from 1 - 75 dB). This is the SNR threshold for an associated client as seen by its associated AP radio. When exceeded, the radio increases its transmit power to increase coverage for the associated client. The default value is 20 dB.
<b>Coverage Interval</b>	Define the interval when coverage hole recovery should be initiated after a coverage hole is detected. The default is 10 seconds for both 2.4 GHz and 5.0 GHz radios.
<b>Interval</b>	Define the interval coverage hole recovery should be conducted after a coverage hole is detected. The default is 30 seconds for both 2.4 GHz and 5.0 GHz radios.

29. Select **OK** to update the Smart RF Coverage Hole Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

## 6.5.1 Smart RF Configuration and Deployment Considerations

### ▶ SMART RF

Before defining a Smart RF supported configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections
- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Motorola Solutions recommends that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channels specified in the Smart RF policy
- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a **no dfs-rehome** command from the CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.



<b>Mesh ID</b>	Displays the IDs of all mesh identifiers for the configured mesh points.
<b>Mesh Point Status</b>	Specifies the status of each configured mesh point, either <i>Enabled</i> or <i>Disabled</i> .
<b>Descriptions</b>	Displays any descriptive text entered for each of the configured mesh points.
<b>Control VLAN</b>	Displays VLAN number for the control VLAN on each of the configured mesh points.
<b>Allowed VLANs</b>	Displays the list of VLANs allowed on each of the configured mesh points.
<b>Security Mode</b>	Displays the security for each of the configured mesh points. The field will display <i>none</i> for no security or <i>psk</i> for pre-shared key authentication.
<b>Mesh QoS Policy</b>	Displays the list of Mesh Quality of Service policies associated with each of the configured mesh points.

5. Select **Add** to create a new MeshConnex policy, **Edit** to modify the attributes of a existing policy or **Delete** to remove obsolete policies from the list of those available. Use **Copy** to create a copy of an existing policy for further modification. Use **Rename** to rename an existing MeshConnex policy.

The **Configuration** screen displays by default for the new or modified MeshConnex policy.

**Figure 6-39** MeshConnex - Basic Configuration screen

6. Refer to the **Basic Configuration** section to define a MeshConnex profile.

<b>Mesh Point Name</b>	Specify a name for the new mesh point. The name should be descriptive of the mesh point to easily differentiate it from other mesh points. This field is mandatory.
<b>Mesh ID</b>	Specify a mesh identifier for this mesh point. This field is optional.

<b>Mesh Point Status</b>	To enable this mesh point, select the <i>Enabled</i> radio button. To disable the mesh point select the <i>Disabled</i> button. The default value is enabled.
<b>Mesh QoS Policy</b>	Use the drop-down menu to specify the mesh QoS policy to use on this mesh point. This value is mandatory. If no suitable Mesh QoS policies exist, click the create icon to create a new Mesh QoS policy.
<b>Beacon Format</b>	Use the drop-down menu to specify the format that beacons from the mesh point are sent. To use access point style beacons select <i>access-point</i> from the drop-down menu. To use mesh point style beacons select <i>mesh-point</i> from the drop-down menu. The default value is mesh-point.
<b>Is Root</b>	Select this option to specify the mesh point as a root.
<b>Control VLAN</b>	Use the spinner control to specify a VLAN to carry mesh point control traffic. The valid range for control VLAN is from 1 - 4094. The default value is VLAN 1.
<b>Allowed VLAN</b>	Specify the VLANs allowed to pass traffic on the mesh point. Separate all VLANs with a comma. To specify a range of allowed VLANs separate the starting VLAN and the ending VLAN with a hyphen.
<b>Neighbor Inactivity Timeout</b>	Specify a Neighbor Inactivity Timeout in <i>seconds, minutes, hours</i> or <i>days</i> , up to a maximum of 1 day. <i>Neighbor Inactivity Timeout</i> is the allowed amount of time between frames received from a neighbor before their client privileges are revoked. The default value is 2 minutes.
<b>Description</b>	Enter any descriptive text about the mesh point.

7. Select **OK** to update the MeshConnex Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.
8. Select the **Security** tab.

**Figure 6-40** MeshConnex - Security screen

9. Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

<b>Security Mode</b>	Select a security authentication mode for the mesh-point. Select <i>none</i> to set no authentication for the mesh point. Select <i>psk</i> to set a pre-shared key as the authentication for the mesh-point. If <i>psk</i> is selected enter a pre-shared key in the Key Settings field.
----------------------	---

10. Set the following **Key Settings** for the mesh point:

<b>Pre-Shared Key</b>	When the security mode is set as <i>psk</i> , enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.
-----------------------	---

11. Set the following **Key Rotation** for the mesh point:

<b>Unicast Rotation Interval</b>	Define an interval for unicast key transmission in <i>seconds</i> (30 - 86,400).
<b>Broadcast Rotation Interval</b>	When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in <i>seconds</i> (30 - 86,400). Key rotation enhances the broadcast traffic security on the WLAN.

12. Select **OK** to save the changes made to the configuration. Select **Reset** to revert to the last saved configuration.  
 13. Select the **Radio Rates** tab.

14. Set the following **Radio Rates** for both the 2.4 and 5.0 GHz radio bands:

<p><b>2.4 GHz Mesh Point</b></p>	<p>Choose the <i>Select</i> button to configure radio rates for the 2.4 GHz band. Define both minimum <i>Basic</i> and optimal <i>Supported</i> rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band.</p> <p>If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates).</p> <p>The selected rates apply to associated client traffic within this mesh point only.</p>
<p><b>5.0 GHz Mesh Point</b></p>	<p>Choose the <i>Select</i> button to configure radio rates for the 5.0 GHz band. Define both minimum <i>Basic</i> and optimal <i>Supported</i> rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band.</p> <p>If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates).</p> <p>The selected rates apply to associated client traffic within this mesh point only.</p>

**Rate Settings 2.4GHz-MeshPoint**

**Radio Transmission Data Rates**

b-only rates   
 bg rates   
 bgn rates   
 Default  
 g-only rates   
 gn rates   
 Custom Rates

**802.11b Rates**

	1Mbps	2Mbps	5.5Mbps	11Mbps
Basic:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**802.11g Rates**

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input type="checkbox"/>							
Supported:	<input type="checkbox"/>							

**802.11n Rates**

	MCS0-7	MCS8-15	MCS16-23
Basic:	<input type="checkbox"/>		
Supported:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK    Reset    Cancel

**Figure 6-41** Advanced Rate Settings 2.4 GHz screen

**Rate Settings 5GHz-MeshPoint** [X]

**Radio Transmission Data Rates**

a-only rates     Default  
 an rates         Custom Rates

**802.11a Rates**

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input type="checkbox"/>							
Supported:	<input type="checkbox"/>							

**802.11n Rates**

	MCS0-7	MCS8-15	MCS16-23
Basic:	<input type="checkbox"/>		
Supported:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK    Reset    Cancel

**Figure 6-42** Advanced Rate Settings 5 GHz screen

15. Define both minimum *Basic* and optimal *Supported* rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band and 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point.

If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

16. Select **OK** to save the changes made to the configuration. Select **Reset** to revert to the last saved configuration.



<b>Mesh Rx Rate Limit</b>	Displays whether or not a <i>Mesh Rx Rate Limit</i> is enabled for each Mesh QoS policy. This indicates rate limiting is enabled or disabled for all data transmitted by the device to any mesh point in the mesh. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
<b>Neighbor Tx Rate Limit</b>	Displays whether a <i>NeighborTx Rate Limit</i> is enabled for each Mesh QoS policy. This indicates rate limiting is enabled for data transmitted from connected wireless clients. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
<b>Neighbor Rx Rate Limit</b>	Displays whether a <i>NeighborRx Rate Limit</i> is enabled for each Mesh QoS policy. This indicates rate limiting is enabled or disabled for data transmitted from the client to its associated access point radio and connected wireless controller. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
<b>Classification</b>	Displays the forwarding QoS classification for each Mesh QoS policy.

5. Select the **Add** button to define a new Mesh QoS policy, or select an existing Mesh QoS policy and select **Edit** to modify its existing configuration. Existing QoS policies can be selected and deleted as needed.

The **Rate Limit** screen displays by default for the new or modified QoS policy.

Excessive traffic can cause performance issues or bring down the network completely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and mesh point) per neighbor. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the managed network and data transmitted from a mesh point's neighbor back to their associated access point radios and controller.

Before defining rate limit thresholds for mesh point transmit and receive traffic, Motorola Solutions recommends you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) will be dropped resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

Mesh QoS Policy test ?

**Rate Limit**   **Multimedia Optimizations**

---

**Mesh Point Settings**

**From Air Upstream Rate Limit**

**Mesh Tx Rate Limit**

**Rate**  (50 to 1,000,000 kbps)

**Maximum Burst Size**  (2 to 1,024 kbytes)

**To Air Downstream Rate Limit**

**Mesh Rx Rate Limit**

**Rate**  (50 to 1,000,000 kbps)

**Maximum Burst Size**  (2 to 1,024 kbytes)

**From Air Upstream Random Early Detection Threshold**

**Background Traffic**  (0 to 100 %)

**Best Effort Traffic**  (0 to 100 %)

**Video Traffic**  (0 to 100 %)

**Voice Traffic**  (0 to 100 %)

**To Air Downstream Random Early Detection Threshold**

**Background Traffic**  (0 to 100 %)

**Best Effort Traffic**  (0 to 100 %)

**Video Traffic**  (0 to 100 %)

**Voice Traffic**  (0 to 100 %)

---

**Neighbor Settings**

**From Air Upstream Rate Limit**

**Neighbor Rx Rate Limit**

**Rate**  (50 to 1,000,000 kbps)

**Maximum Burst Size**  (2 to 1,024 kbytes)

**To Air Downstream Rate Limit**

**Neighbor Tx Rate Limit**

**Rate**  (50 to 1,000,000 kbps)

**Maximum Burst Size**  (2 to 1,024 kbytes)

**From Air Upstream Random Early Detection Threshold**

**Background Traffic**  (0 to 100 %)

**Best Effort Traffic**  (0 to 100 %)

**Video Traffic**  (0 to 100 %)

**Voice Traffic**  (0 to 100 %)

**To Air Downstream Random Early Detection Threshold**

**Background Traffic**  (0 to 100 %)

**Best Effort Traffic**  (0 to 100 %)

**Video Traffic**  (0 to 100 %)

**Voice Traffic**  (0 to 100 %)

**Figure 6-44** Mesh QoS Policy - Rate Limit screen

6. Configure the following parameters in respect to the intended **From Air Upstream Rate Limit**, or traffic from the controller to associated access point radios and their associated neighbor:

<b>Mesh Tx Rate Limit</b>	Select this option to enable rate limiting for all data received from any mesh point in the mesh. This feature is disabled by default.
<b>Rate</b>	Define a receive rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes.
---------------------------	--

7. Set the following **Receive Random Early Detection Threshold** settings for each access category. An early random drop is done when a traffic stream falls below the set threshold.

<b>Background Traffic</b>	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

8. Configure the following parameters in respect to the intended **To Air Downstream Rate Limit**, or traffic from neighbors to associated access point radios and the controller:

<b>Mesh Rx Rate Limit</b>	Select this option to enable rate limiting for all data transmitted by the device to any mesh point in the mesh. This feature is disabled by default.
<b>Rate</b>	Define an transmit rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the mesh point's wireless client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.
---------------------------	---

9. Set the following **To Air Downstream Random Early Detection Threshold** settings for each access category. An early random drop is done when the amount of tokens for a traffic stream falls below the set threshold.

<b>Background Traffic</b>	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

10. Configure the following parameters in respect to the intended **From Air Upstream Rate Limit** for the **Neighbor Settings** field.

<b>Neighbor Rx Rate Limit</b>	Select this radio button to enable rate limiting for data transmitted from the client to its associated access point radio and connected wireless controller. Enabling this option does not invoke client rate limiting for data traffic in the receive direction. This feature is disabled by default.
<b>Rate</b>	Define an transmit rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.
<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

11. Set the following **Neighbor Receive Random Early Detection Threshold** settings for each access category:

<b>Background Traffic</b>	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
<b>Best Effort Traffic</b>	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
<b>Video Traffic</b>	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.
<b>Voice Traffic</b>	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%. 0% implies no early random drops will occur.

12. Configure the following parameters in respect to the intended **Neighbor To Air Downstream Rate Limit**, or traffic from a controller to associated access point radios and the wireless client:

<b>Neighbor Tx Rate Limit</b>	Select this radio button to enable rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the transmit direction. This feature is disabled by default.
<b>Rate</b>	Define a receive rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.
<b>Maximum Burst Size</b>	Set a maximum burst size from 2 - 64 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

13. Set the following **Neighbor To Air Downstream Random Early Detection Threshold** settings for each access category:

<b>Background Traffic</b>	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.
<b>Best Effort Traffic</b>	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.
<b>Video Traffic</b>	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 25%.

<b>Voice Traffic</b>	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% means no early random drops will occur.
----------------------	--

- Select **OK** when completed to update this mesh QoS rate limit settings. Select **Reset** to revert the screen back to its last saved configuration.
- Select the **Multimedia Optimizations** tab.

**Figure 6-45** Mesh QoS Policy - Multimedia Optimizations screen

- Set the following **Accelerated Multicast** settings:

<b>Disable Multicast Streaming</b>	Select this option to disable Multicast Streaming on the mesh point.
<b>Automatically Detect Multicast Streams</b>	Select this option to have bridged multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they would want.
<b>Manually Configure Multicast Addresses</b>	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

- Select **OK** when completed to update the *Mesh Multimedia Optimizations* settings. Select **Reset** to revert to the last saved configuration.



5. Select the **Add** button to define a new Passpoint policy, or select an existing Passpoint policy and select **Edit** to modify its existing configuration. Existing Passpoint policies can be selected and deleted as needed.

The screenshot shows a configuration window for a Passpoint policy. The title bar indicates the policy name is 'PassPoint\_Test'. The 'Basic Configuration' section includes a dropdown for 'Access Network Type' currently set to 'private', and text input fields for 'Operator Name' and 'Venue Name'. Below these is a table for 'Venue Name Lang' with columns for 'Code' and 'Name', and a red trash icon for deleting rows. An 'Add Row' button is located below the table. At the bottom of the window, there are 'OK', 'Reset', and 'Exit' buttons.

**Figure 6-47** Passpoint Policy - Add new policy

6. Configure the following parameters in respect to the **Basic Configuration** fields:

<b>Access Network Type</b>	Select the network type from the drop-down. This is the type of network that is advertised to requesting clients.
<b>Operator Name</b>	Enter a friendly name for the operator running the hotspot service. Enter a string not longer than 64 characters.
<b>Venue Name</b>	Enter a friendly name for the venue in which this hotspot service is running. Enter a string not longer than 252 characters.
<b>Venue Name Lang</b>	Use this table to provide encoding information to display the Venue Name in other languages. Use this table to provide the language <i>Code</i> and the hexadecimal representation of the venue name in the <i>Name</i> field. Multiple values can be entered in this table.

7. Configure the following parameters with respect to the **Operator Network Parameters** fields:

<b>Operator Name Lang</b>	Use this table to provide encoding information to display the Operator Name in other languages. Use this table to provide the language <i>Code</i> and the hexadecimal representation of the operator name in the <i>Name</i> field. Multiple values can be entered in this table.
<b>PLMNID</b>	Use the PLMNID table to provide the <i>Mobile Country Code</i> (MCC) and the <i>Mobile Network Code</i> (MNC) for the operator along with a brief description of this information.

8. Select **OK** when completed to update the Passpoint policy settings. Select **Reset** to revert to the last saved configuration.



# CHAPTER 7

## NETWORK CONFIGURATION

The access point allows packet routing customizations and additional route resources.

For more information on the network configuration options available to the access point, refer to the following:

- [Policy Based Routing \(PBR\)](#)
- [L2TP V3 Configuration](#)
- [AAA Policy](#)
- [AAA TACACS Policy](#)
- [Alias](#)

For configuration caveats specific to **Configuration > Network** path, refer to [Network Deployment Considerations on page 7-42](#).

---

## 7.1 Policy Based Routing (PBR)

### ► Network Configuration

Define a *policy based routing* (PBR) configuration to direct packets to selective paths. PBR can optionally mark traffic for preferential services (QoS). PBR minimally provides the following:

- A means to use source address, protocol, application and traffic class as traffic routing criteria
- The ability to load balance multiple WAN uplinks
- A means to selectively mark traffic for QoS optimization

Since PBR is applied to incoming routed packets, a route-map is created containing a set of filters and associated actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Route-maps are configurable under a global policy called *routing-policy*, and applied to profiles and devices.

Route-maps contain a set of filters which select traffic (match clauses) and associated actions (set clauses) for routing. A route-map consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value). If it matches, the routing decision is based on this route-map. If the packet does not match the route-map, the route-map entry with next highest precedence is matched. If the incoming packet does not match any of the route-map entries, it's subjected to typical destination based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- *IP Access List* - A typical IP ACL can be used for traffic permissions. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.
- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP DSCP field. One DSCP value is configurable per route map entry. If IP ACLs on a WLAN, ports or SVI mark the packet, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered by the incoming WLAN. There are two ways to match the WLAN:
  - If the device doing policy based routing has an onboard radio and a packet is received on a local WLAN, then this WLAN is used for selection.
  - If the device doing policy based routing does not have an onboard radio and a packet is received from an extended VLAN, then the device which received the packet passes the WLAN information in the MINT packet for the PBR router to use as match criteria.
- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the host originating the packet is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing policy based routing, and not the originating connected device.

Each route map entry has a set of *match* and *set* (action) clauses. ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

Set (or action) clauses determine the routing function when a packet satisfies match criteria. If no set clauses are defined, the default is to fallback to destination based routing for packets satisfying the match criteria. If no set clause is configured and fallback to destination based routing is disabled, then the packet is dropped. The following can be defined within set clauses:

- *Next hop* - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used, but if all the next hops aren't reachable, typical destination based route lookup is performed.



- If creating a new PBR policy assign it a **Policy Name** up to 32 characters to distinguish this route map configuration from others with similar attributes. Select **Continue** to proceed to the Policy Name screen where route map configurations can be added, modified or removed. Select **Exit** to exit without creating a PBR policy.

Policy Name test ?

**Route Maps** **General**

Precedence	DSCP	Role Policy	User Role	Access Control List	WLAN	Incoming Interface
1	0			BROADCAST-MULTICA	1	wwan1

Type to search in tables Row Count: 1

**Figure 7-2** Policy Based Routing screen - Route Maps tab

- Refer to the following to determine whether a new route-map configuration requires creation or an existing route-map requires modification or removal:

<b>Precedence</b>	Lists the numeric precedence (priority) assigned to each listed PBR configuration. A route-map consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).
<b>DSCP</b>	Displays each policy's DSCP value used as matching criteria for the route map. DSCP is the <i>Differentiated Services Code Point</i> field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry.
<b>Role Policy</b>	Lists each policy's role policy used as matching criteria.
<b>User Role</b>	Lists the user role defined in the Role Policy.
<b>Access Control List</b>	Displays each policy's IP ACL used as an access/deny filter criteria for the route map.
<b>WLAN</b>	Displays each policy's WLAN used as an access/deny filter for the route map.
<b>Incoming Interface</b>	Display the name of the access point WWAN or VLAN interface on which the packet is received for the listed PBR policy.

- Select **Add** or **Edit** to create or modify a route-map configuration.

**Figure 7-3** Policy Based Routing screen - Add a Route Map

8. Use the spinner control to set a numeric precedence (priority) for this route-map. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).
9. Refer to the **Match Clauses** field to define the following matching criteria for the route-map configuration:

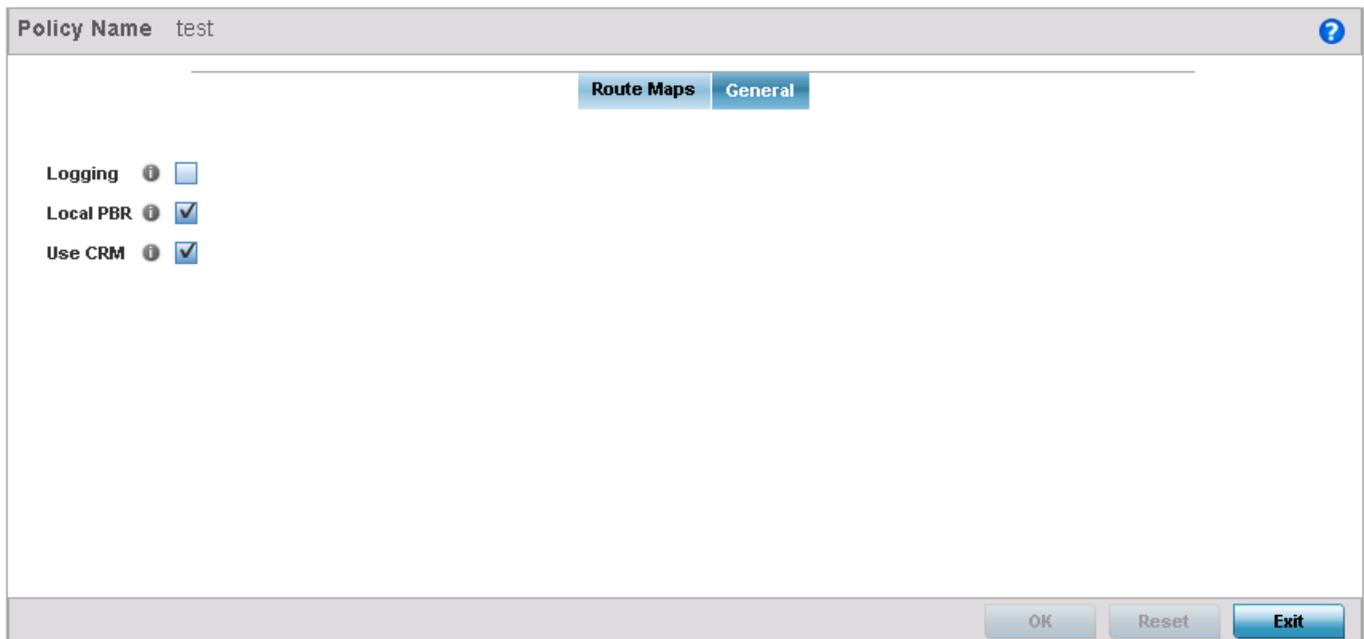
<b>DSCP</b>	Select this option to enable a spinner control to define the DSCP value used as matching criteria for the route map. DSCP is the <i>Differentiated Services Code Point</i> field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry.
<b>Role Policy</b>	Use the drop-down to select a Role Policy to use with this route-map. Click the <i>Create</i> icon to create a new Role Policy. To view and modify an existing policy, click the <i>Edit</i> icon.
<b>User Role</b>	Use the drop-down menu to select a role defined in the selected Role Policy. This user role is used while deciding the routing.
<b>Access Control List</b>	Use the drop-down menu to select an IP based ACL used as matching criteria for this route-map. Click the <i>Create</i> icon to create a new ACL. To view and modify an existing ACL, click the <i>Edit</i> icon.
<b>WLAN</b>	Use the drop-down menu to select the access point WLAN used as matching criteria for this route-map. Click the <i>Create</i> icon to create a new WLAN. To view and modify an existing WLAN, click the <i>Edit</i> icon.

<b>Incoming Interface</b>	Select this option to enable radio buttons used to define the interfaces required to receive route-map packets. Use the drop-down menu to define either the access point's <i>wwan1</i> or <i>pppoe1</i> interface. Neither is selected by default. Or, select the VLAN ID option to define the access point VLAN to receive route-map-packets.
---------------------------	---

10. Set the following **Action Clauses** to determine the routing function performed when a packet satisfies match criteria. Optionally fallback to destination based routing if no hop resource is available.

<b>Next Hop (Primary)</b>	Define a first hop priority request. Set either the <i>IP</i> address of the virtual resource or select the <i>Interface</i> option and define either a <i>wwan1</i> , <i>pppoe1</i> or a <i>VLAN</i> interface. In the simplest terms, if this primary hop resource is available, its used with no additional considerations.
<b>Next Hop (secondary)</b>	If the primary hop request were unavailable, a second resource can be defined. Set either the <i>IP</i> address of the virtual resource or select the <i>Interface</i> option and define either a <i>wwan1</i> , <i>pppoe1</i> or a <i>VLAN</i> interface.
<b>Default Next Hop</b>	If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse. Set either the next hop IP address or define either a <i>wwan1</i> , <i>pppoe1</i> or a <i>VLAN</i> interface.
<b>Use Destination Routing</b>	It may be a good idea to select this option to default back to destination based routing if none of the defined hop resources are reachable. Packets are dropped if a next hop resource is unavailable and fallback to destination routing is disabled. This option is enabled by default.
<b>Mark</b>	Select this option and use the spinner control to set IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

11. Select **OK** to save the updates to the route-map configuration. Select **Reset** to revert to the last saved configuration.
12. Select the **General** tab from within the Policy Based Routing screen.



**Figure 7-4** Policy Based Routing screen - General tab

13. Set the following **General** PBR configuration settings:

<b>Logging</b>	Select this option to log events generated by route-map configuration rule enforcement. This setting is disabled by default.
<b>Local PBR</b>	Select this option to implement policy based routing for this access point's packet traffic. This setting is enabled by default, so the match and action clauses defined within the <i>Route Maps</i> tab are implemented until disabled using this setting.
<b>Use CRM</b>	Select the <i>Use CRM (Critical Resource Management)</i> option to monitor access point link status. Selecting this option determines the disposition of the route-map next hop via monitored critical resources. Link monitoring is used to determine a potential failover to the secondary next hop. This setting is enabled by default.

14. Select **OK** to save the updates to the route-map general configuration. Select **Reset** to revert to the last saved configuration.

## 7.2 L2TP V3 Configuration

### ► Network Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network. L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables WING supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WING devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WING supported access points support an Ethernet VLAN pseudowire type exclusively.



**NOTE:** A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

---

---

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.



**NOTE:** If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

---

---

To define an L2TP V3 tunnel configuration:

1. Select **Configuration** > **Network** > **L2TP V3**.



<b>Force L2 Path Recovery</b>	Indicates if L2 Path Recovery is enabled to learn servers, gateways and other network devices behind a L2TPV3 tunnel.
-------------------------------	---

- Select **Add** to create a new L2TP V3 policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

The screenshot shows a configuration window for an L2TP V3 policy. At the top, there is a 'Name' field containing the text 'policy'. Below this is the 'Policy Details' section, which contains several configuration options:

- Cookie Size:** A spinner control set to 0.
- Hello Interval:** A text input set to 1, followed by a dropdown menu set to 'Minutes' and a range indicator '( 1 to 60 )'.
- Reconnect Attempt:** A spinner control set to 0, with a range indicator '(0 to 8)'.
- Reconnect Interval:** A text input set to 2, followed by a dropdown menu set to 'Minutes' and a range indicator '( 1 to 60 )'.
- Retry Count:** A spinner control set to 5, with a range indicator '(1 to 10)'.
- Retry Time Out:** A text input set to 5, followed by a dropdown menu set to 'Seconds' and a range indicator '( 1 to 250 )'.
- Rx Window Size:** A spinner control set to 10, with a range indicator '(1 to 15)'.
- Tx Window Size:** A spinner control set to 10, with a range indicator '(1 to 15)'.
- Failover Delay:** A text input set to 5, followed by a dropdown menu set to 'Seconds' and a range indicator '( 5 to 60 )'.
- Force L2 Path Recovery:** A checkbox that is currently unchecked.

At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 7-6** L2TP V3 Policy Creation screen

- If creating a new L2TP V3 policy, assign it a **Name** up to 31 characters in length. Remember, a single L2TP V3 policy can be used by numerous L2TP V3 tunnels.
- Define the following **Policy Details** to add a device to a list of devices sanctioned for network operation:

<b>Cookie size</b>	L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. Use the spinner control to set the size of the cookie field present within each L2TP V3 data packet. Options include 0, 4 and 8. The default setting is 0. If using the CLI, cookie size cannot be configured per session, and are the same size for all sessions with in a tunnel.
<b>Hello Interval</b>	Define an interval in either <i>Seconds</i> (1 - 3,600), <i>Minutes</i> (1 -60) or <i>Hours</i> (1) between L2TP V3 hello keep alive messages exchanged within the L2TP V3 control connection. The default setting is 1 minute.

<b>Reconnect Attempts</b>	Use the spinner control to set a value (from 0 - 250) representing the maximum number of reconnection attempts initiated to reestablish the tunnel. The default interval is 0.
<b>Reconnect Interval</b>	Define an interval in either <i>Seconds</i> (1 - 3,600), <i>Minutes</i> (1 -60) or <i>Hours</i> (1) between two successive reconnection attempts. The default setting is 2 minutes.
<b>Retry Count</b>	Use the spinner control to define how many retransmission attempts are made before determining a target tunnel peer is not reachable. The available range is from 1 - 10, with a default value of 5.
<b>Retry Time Out</b>	Use the spinner control to define the interval (in seconds) before initiating a retransmission of a L2TP V3 signaling message. The available range is from 1 - 250, with a default value of 5.
<b>Rx Window Size</b>	Specify the number of packets that can be received without sending an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
<b>Tx Window Size</b>	Specify the number of packets that can be transmitted without receiving an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
<b>Failover Delay</b>	Specify the wait time (in seconds) before re-establishing a failed tunnel. The available duration is 5 - 60 seconds or 1 minute with a default setting of 5 seconds.
<b>Force L2 Path Recovery</b>	Select to enable forcing the discovery of servers, gateways and other networks behind a L2TPV3 tunnel when a tunnel is being established or when a failed tunnel is being reestablished.

6. Select **OK** to save the updates to the L2TP V3 Policy Details. Select **Reset** to revert to the last saved configuration.

## 7.3 AAA Policy

### ► Network Configuration

*Authentication, Authorization, and Accounting (AAA)* is the mechanism network administrators use to define access control within the access point managed network.

The access point can optionally use an external RADIUS and LDAP Servers (AAA Servers) to provide user database information and user authentication data. Each WLAN managed by the access point can maintain its own unique AAA configuration. AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points have an onboard RADIUS server resource, while AP6511 and AP6521 models do not.

AAA provides a modular way of performing following services:

- *Authentication* — Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the access point managed network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various access point interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.
- *Authorization* — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally on the access point or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating attribute-value (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces on the access point.
- *Accounting* — Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on an access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated for the access point, it's applied equally to all interfaces on the access point's access servers.

To define unique WLAN AAA configurations:

1. Select the **Configuration** tab from the Web UI.
2. Select **Network**.
3. Select **AAA Policy** to display a high level display of existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA)** screen lists existing AAA policies. Any of these policies can be selected and applied to the access point.





<b>NAI Routing Enable</b>	Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an E-mail address as either user or user@ but it need not be a valid E-mail address or a fully qualified domain name. NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each user credential.
<b>NAC Enable</b>	A green check mark defines NAC as enabled, while a red X defines NAC disabled with this AAA policy.

7. Select a server ID from the table and select **Edit**, or select **Add** to create a new policy.

**Authentication Server**

Server Id 1 (1 to 6)

**Settings**

Host \*  Hostname ▾

Port ⓘ 1812 (1 to 65,535)

Server Type ⓘ Host ▾

Secret \*  Show

Request Proxy Mode ⓘ None ▾

Proxy Mint Host ⓘ

Request Attempts ⓘ 3 (1 to 10)

Request Timeout ⓘ 3 Seconds (1 to 60)

Retry Timeout Factor ⓘ 100 (50 to 200)

DSCP ⓘ 46 (0 to 63)

**Network Access Identifier Routing**

NAI Routing Enable ⓘ

Realm ⓘ

Realm Type ⓘ  Prefix  Suffix

OK Reset Exit

**Figure 7-9** AAA Policy - RADIUS Authentication tab - Authentication Server screen

8. Define the following settings to add or modify AAA RADIUS authentication server configuration:

<b>Server Id</b>	Define the numerical server index (1-6) for the authentication server to differentiate it from others available to the access point's AAA policy.
<b>Host</b>	Specify the IP address or hostname of the RADIUS authentication server.
<b>Port</b>	Define or edit the port on which the RADIUS server listens to traffic within then access point managed network. The port range is 1 to 65,535. The default port is 1812.
<b>Server Type</b>	Select the type of AAA server as either <i>Host</i> , <i>onboard-self</i> or <i>onboard-controller</i> . AP6511 and AP6521 models do not have an onboard authentication resource and must use an external server or Virtual Controller AP resource.
<b>Secret</b>	Specify the secret used for authentication on the selected RADIUS server. By default the secret will be displayed as asterisks.
<b>Request Proxy Mode</b>	Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be <i>None</i> , <i>Through Wireless Controller</i> or <i>Through RF Domain Manager</i> .
<b>Proxy Mint Host</b>	Specify the hostname (if the device is a Level-1 MiNT neighbor) or the Mint-ID of the Mint device to proxy hosts through.
<b>Request Attempts</b>	Specify the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
<b>Request Timeout</b>	Specify the time from 1 - 60 seconds for the access point's re-transmission of request packets. If this time is exceeded, the authentication session is terminated. The default is 3 seconds.
<b>Retry Timeout Factor</b>	Specify the time from 50 - 200 seconds between retry timeouts for the access points's re-transmission of request packets. The default is 100.
<b>DSCP</b>	Specify the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is from 0 - 63, with a default value of 46.

9. Set the following **Network Address Identifier (NAI) Routing** settings:

<b>NAI Routing Enable</b>	Select this check box to enable NAI routing. AAA servers identify clients using the NAI. The NAI is a character string in the format of an E-mail address as either <i>user</i> or <i>user@</i> but it need not be a valid E-mail address or a fully qualified domain name. NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each user credential.
<b>Realm</b>	Enter the realm name in the field. The name cannot exceed 64 characters. When the access point RADIUS server receives a request for a user name the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server.
<b>Realm Type</b>	Specify the type of realm that is being used, either <i>Prefix</i> or <i>Suffix</i> .



<b>NAI Routing Enable</b>	Displays the NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an E-mail address as either user or user@ but it need not be a valid E-mail address or a fully qualified domain name. NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each user credential.
---------------------------	--

12. To edit an existing accounting profile, select the profile then select the **Edit** button. To add a new policy, select the **Add** button.

The screenshot shows the 'Accounting Server' configuration window. At the top, there is a 'Server Id' dropdown menu set to '1' (range 1 to 6). Below this is the 'Settings' section with the following fields:

- Host:** A text input field with a 'Hostname' dropdown menu.
- Port:** A numeric spinner set to 1813 (range 1 to 65,535).
- Server Type:** A dropdown menu set to 'Host'.
- Secret:** A text input field with a 'Show' checkbox.
- Request Proxy Mode:** A dropdown menu set to 'None'.
- Proxy Mint Host:** A text input field.
- Request Attempts:** A numeric spinner set to 3 (range 1 to 10).
- Request Timeout:** A numeric spinner set to 5 with a 'Seconds' dropdown menu (range 1 to 60).
- Retry Timeout Factor:** A numeric spinner set to 100 (range 50 to 200).
- DSCP:** A numeric spinner set to 34 (range 0 to 63).

Below the 'Settings' section is the 'Network Access Identifier Routing' section with the following options:

- NAI Routing Enable:** A checkbox that is currently unchecked.
- Realm:** A text input field.
- Realm Type:** Radio buttons for 'Prefix' (selected) and 'Suffix'.
- Strip Realm:** A checkbox that is currently unchecked.

At the bottom of the window are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 7-11** AAA Policy - RADIUS Accounting tab - Accounting Server screen

13. Define the following settings to add or modify AAA RADIUS accounting server configuration:

<b>Server Id</b>	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
------------------	---

<b>Host</b>	Specify the IP address or hostname of the RADIUS authentication server.
<b>Port</b>	Define or edit the port on which the RADIUS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 1813.
<b>Server Type</b>	Select the type of AAA server as either <i>Host</i> , <i>onboard-self</i> or <i>onboard-controller</i> .
<b>Secret</b>	Specify the secret (password) used for authentication on the selected RADIUS server. By default the secret is displayed as asterisks.
<b>Request Proxy Mode</b>	Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be <i>None</i> , <i>Through Wireless Controller</i> or <i>Through RF Domain Manager</i> .
<b>Proxy Mint Host</b>	Specify a 64 character maximum hostname or the Mint ID of the Mint device used for proxying requests.
<b>Request Attempts</b>	Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
<b>Request Timeout</b>	Specify the time for the access point's re-transmission of request packets. The default is 5 seconds. If this time is exceeded, the authentication session is terminated.
<b>Retry Timeout Factor</b>	Specify the interval, in seconds, between two successive re-transmission attempts of request packets. Specify a value from 50 - 200 seconds. The default is 100 seconds.
<b>DSCP</b>	Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is from 0 - 63 with a default value of 34.
<b>NAI Routing Enable</b>	Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an E-mail address as either <i>user</i> or <i>user@</i> but it need not be a valid E-mail address or a fully qualified domain name. NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.
<b>Realm</b>	Enter the realm name. The name cannot exceed 64 characters. When the access point's RADIUS server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server.
<b>Realm Type</b>	Specify the realm as either <i>Prefix</i> or <i>Suffix</i> .
<b>Strip Realm</b>	Select this option to remove information from the packet when NAI routing is enabled.

14. Select the **Settings** tab.

**AAA Policy** AAA\_Policy\_HQ

**RADIUS Authentication** | **RADIUS Accounting** | **Settings**

**RADIUS Authentication**

Protocol for MAC, Captive-Portal Authentication  PAP  CHAP  MS-CHAP  MS-CHAPv2

**RADIUS Accounting**

Accounting Packet Type  (Start/Stop)

Request Interval   (1 to 60)

Accounting Server Preference  (Prefer Same Authentication Server Host)

**RADIUS Address Format**

Format  (Dash Delimiter (aa-bb-cc-dd-ee-ff))

Case  (Uppercase)

Attributes  (Username / Password)

**Server Pooling**

Server Pooling Mode  Failover  Load Balanced

**EAP Wireless Client Settings**

Client Attempts  (1 to 10)

Request Timeout  (1 to 60 seconds)

OK Reset Exit

**Figure 7-12** AAA-Policy - Settings screen

15. Set the following RADIUS server configuration parameters:

<b>Protocol for MAC, Captive-Portal Authentication</b>	Set the authentication protocol when the server is used for any non-EAP authentication. Options include <i>Password Authentication Protocol (PAP)</i> , <i>Challenge Handshake Authentication Protocol (CHAP)</i> , <i>MSPAP</i> and <i>MSCHAP-V2</i> . The default setting is PAP.
<b>Accounting Packet Type</b>	Set the type of RADIUS Accounting Request packets generated. Options include <i>Stop Only</i> , <i>Start/Stop</i> and <i>Start/Interim/Stop</i> . The default setting is Start/Stop.
<b>Request Interval</b>	Set the periodicity of the interim accounting requests. The default is 30 minutes.
<b>Accounting Server Preference</b>	Select the server preference for RADIUS Accounting. The options are: <ul style="list-style-type: none"> <li>• <i>Prefer Same Authentication Server Host</i> - Uses the authentication server hostname as the host used for RADIUS accounting. This is the default setting.</li> <li>• <i>Prefer Same Authentication Server Index</i> - Uses the same index as the authentication server for RADIUS accounting.</li> <li>• <i>Select Accounting Server Independently</i>- Allows users to specify a RADIUS accounting server separate from the RADIUS authentication server.</li> </ul>
<b>Format</b>	Select the format of the MAC address used in the RADIUS accounting packets.
<b>Case</b>	Lists whether the MAC address is sent using <i>uppercase</i> or <i>lowercase</i> letters. The default setting is uppercase.

<b>Attributes</b>	Lists whether the format specified applies only to the user name/password in mac-auth or for all attributes that include a MAC address, such as calling-station-id or called-station-id.
<b>Server Pooling Mode</b>	Controls how requests are transmitted across RADIUS servers. <i>Failover</i> implies traversing the list of servers if any server is unresponsive. <i>Load Balanced</i> uses all servers in a round-robin fashion. The default setting is Failover.
<b>Client Attempts</b>	Defines the number of times (1 - 10) an EAP request is transmitted to a wireless client before giving up. The default setting is 3.
<b>Request Timeout</b>	Defines the time after which an EAP Request to a wireless client is retried.
<b>ID Request Timeout</b>	Defines the time (1 - 60 seconds) after which an EAP ID Request to a wireless client is retried. The default setting is 30 seconds.
<b>Retransmission Scale Factor</b>	Configures the scaling of the retransmission attempts. Timeout at each attempt is a function of the request timeout factor and client attempts number. 100 (default setting) implies a constant timeout at each retry; smaller values indicate more aggressive (shorter) timeouts, larger numbers indicate more conservative (longer) timeouts on each successive attempt.
<b>Cisco VSA Audit Session Id</b>	Configures a <i>vendor specific attribute</i> (VSA) for CISCO to allow CISCO's <i>Identity Services Engine</i> (ISE) to validate the compliance of a client to the network's policies such as the validity of the virus definition files for the antivirus software or the definition files for an anti-spy ware software.

16. Select **OK** to save the updates. Select **Reset** to revert to last saved configuration.

## 7.4 AAA TACACS Policy

### ► *Network Configuration*

*Terminal Access Controller Access - Control System+* (TACACS+) is a protocol created by CISCO Systems which provides access control to network devices such as routers, network access servers and other networked computing devices through one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services running on different servers.

TACACS+ controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS+ are:

- *Authorizing each command with the TACACS+ server before execution*
- *Accounting each session's logon and log off event*
- *Authenticating each user with the TACACS+ server before enabling access to network resources.*



**NOTE:** For the rest of this section, the term TACACS will be used instead of TACACS+.

---

---

To define unique AAA TACACS configurations:

1. Select the **Configuration** tab from the Web UI.
2. Select **Network**.
3. Select **AAA TACACS Policy** to display a high level display of existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA) TACACS** screen lists existing AAA policies. Any of these policies can be selected and applied to the access point.







**Figure 7-16** AAA TACACS Policy - New Authentication Server



**NOTE:** Only 2 AAA TACACS Authentication servers can be configured at a time.

9. Define the following settings to add or modify AAA TACACS authentication server configuration:

<b>Server Id</b>	Displays the numerical server index (1-2) for the authentication server when added to the list available to the access point.
<b>Host</b>	Specify the IP address or hostname of the AAA TACACS authentication server.
<b>Port</b>	Define or edit the port on which the AAA TACACS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 49.
<b>Secret</b>	Specify the secret (password) used for authentication on the selected AAA TACACS server. By default the secret is displayed as asterisks. When a secret is entered, it must be confirmed in the <i>Reconfirm</i> text box.
<b>Request Attempts</b>	Displays the number of attempts a client can retransmit a missed frame to the AAA TACACS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
<b>Request Timeout</b>	Specify the time for the access point's re-transmission of request packets. The default is 3 seconds. If this time is exceeded, the authentication session is terminated.
<b>Retry Timeout Factor</b>	Specifies the interval, in seconds, between two successive re-transmission attempts. Specify a value from 50 - 200 seconds. The default is 100 seconds.

10. Click **OK** to close the *Authentication Server* dialog and save the changes. Click **Reset** to revert to the last saved configuration. Click **Exit** to close the *Authentication Server* dialog.
11. Click the **Accounting** tab. The following screen displays:



**Figure 7-18** AAA TACACS Policy - New Accounting Server



**NOTE:** Only 2 AAA TACACS accounting servers can be configured at a time.

14. Define the following settings to add or modify AAA TACACS accounting server configuration:

<b>Server Id</b>	Displays the numerical server index (1-2) for the accounting server when added to the list available to the access point.
<b>Host</b>	Specify the IP address or hostname of the AAA TACACS accounting server.
<b>Port</b>	Define or edit the port on which the AAA TACACS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 49.
<b>Secret</b>	Specify the secret (password) used for authentication on the selected AAA TACACS server. By default the secret is displayed as asterisks. When a secret is entered, it must be confirmed in the <i>Reconfirm</i> text box.
<b>Request Attempts</b>	Displays the number of attempts a client can retransmit a missed frame to the AAA TACACS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
<b>Request Timeout</b>	Specify the time for the access point's re-transmission of request packets. The default is 3 seconds. If this time is exceeded, the authentication session is terminated.
<b>Retry Timeout Factor</b>	Specifies the interval, in seconds, between two successive re-transmission attempts of request packets. Specify a value from 50 - 200 seconds. The default is 100 seconds.

15. Click **OK** to close the *Accounting Server* dialog and save the changes. Click **Reset** to revert to the last saved configuration. Click **Exit** to close the *Accounting Server* dialog.

16. Click the **Authorization** tab.



**Figure 7-20** AAA TACACS Policy - New Authorization Server



**NOTE:** Only 2 AAA TACACS authorization servers can be configured at a time.

19. Define the following to add or modify AAA TACACS authorization server configuration:

<b>Server Id</b>	Displays the numerical server index (1-2) for the authorization server when added to the list available to the access point.
<b>Host</b>	Specify the IP address or hostname of the AAA TACACS authorization server.
<b>Port</b>	Define or edit the port on which the AAA TACACS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 49.
<b>Secret</b>	Specify the secret (password) used for authentication on the selected AAA TACACS server. By default the secret is displayed as asterisks. When a secret is entered, it must be confirmed in the <i>Reconfirm</i> text box.
<b>Request Attempts</b>	Displays the number of attempts a client can retransmit a missed frame to the AAA TACACS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
<b>Request Timeout</b>	Specify the time for the access point's re-transmission of request packets. The default is 3 seconds. If this time is exceeded, the authentication session is terminated.
<b>Retry Timeout Factor</b>	Specifies the interval, in seconds, between two successive re-transmission attempts of request packets. Specify a value from 50 - 200 seconds. The default is 100 seconds.

20. Click **OK** to close the *Authorization Server* dialog and save the changes. Click **Reset** to revert to the last saved configuration. Click **Exit** to close the *Authorization Server* dialog.

21. Click the **Settings** tab.

AAA TACACS Policy TTT

Authentication Accounting Authorization Settings

**Accounting**

Access Method

Server Preference

Authentication Failure

CLI Commands

Session

**Authentication**

Access Method

Directed Request

**Authorization**

Access Method

Server

Allow Privileged Commands

**Service Protocol Settings**

Service Name	Service Protocol	

**Figure 7-21** AAA TACACS Policy - Settings tab

22. Set the following AAA TACACS **Accounting** server configuration parameters:

<p><b>Accounting Access Method</b></p>	<p>Specify the access methods for which accounting must be performed. From the drop-down select one of:</p> <ul style="list-style-type: none"> <li>• <i>all</i> – Accounting is performed for all types of access.</li> <li>• <i>console</i> – Accounting is performed only for console access</li> <li>• <i>ssh</i> – Accounting is performed only for access through SSH.</li> <li>• <i>telnet</i> – Accounting is performed only for access through Telnet</li> </ul>
--	--

<b>Server Preference</b>	Specifies how an accounting server is selected from the server pool for sending accounting requests. Select one of the following: <ul style="list-style-type: none"> <li>• <i>NONE</i> – No preference in selection of server used for accounting.</li> <li>• <i>authenticated-server-host</i> – Prefers the same server host used as the authentication server.</li> <li>• <i>authenticated-server-number</i> – Prefers the server with the same index as used as the authentication server. For example, if the index of the server used for authentication server was one (1), then use the accounting server with the index one (1).</li> <li>• <i>authorized-server-host</i> – Prefers the server host used as the authorization server.</li> <li>• <i>authorized-server-number</i> – Prefers the server with the same index as used as the authorization server. For example, if the index of the server used for authorization server was one (1), then use the accounting server with the index one (1).</li> </ul>
<b>Authentication Failure</b>	Select to enable accounting for authentication failure.
<b>CLI Commands</b>	Select to enable accounting for CLI commands.
<b>Session</b>	Select to enable accounting for session start and session stop events.

23. Set the following AAA TACACS **Authentication** server configuration parameters:

<b>Authentication Access Method</b>	Specify the access methods for authentication. <ul style="list-style-type: none"> <li>• <i>all</i> – Authentication is performed for all types of access.</li> <li>• <i>console</i> – Authentication is performed only for console access</li> <li>• <i>ssh</i> – Authentication is performed only for access through SSH.</li> <li>• <i>telnet</i> – Authentication is performed only for access through Telnet</li> <li>• <i>web</i> – Authentication is performed only for access through the Web interface.</li> </ul>
<b>Directed Request</b>	Select to enable the AAA TACACS authentication server to be used with the '@<servername>' nomenclature. The specified server must be present in the list of defined Authentication servers.

24. Set the following AAA TACACS **Authorization** server configuration parameters:

<b>Authorization Access Method</b>	Specify the access methods for authorization: <ul style="list-style-type: none"> <li>• <i>all</i> – Authorization is performed for all types of access.</li> <li>• <i>console</i> – Authorization is performed only for console access</li> <li>• <i>ssh</i> – Authorization is performed only for access through SSH.</li> <li>• <i>telnet</i> – Authorization is performed only for access through Telnet</li> </ul>
<b>Server</b>	Specifies how an authorization server is selected from the server pool: <ul style="list-style-type: none"> <li>• <i>NONE</i> – No preference in selection of server used for accounting.</li> <li>• <i>authenticated-server-host</i> – Prefer the same server host used as the authentication server.</li> <li>• <i>authenticated-server-number</i> – Prefer the server with the same index as used as the authentication server. For example, if the index of the server used for authentication server was one (1), then use the authorization server with the index one (1).</li> </ul>

<b>Allow Privileged Commands</b>	Select this option to enable privileged commands executed without command authorization. Privileged commands can alter/change the authorization server configuration.
----------------------------------	---

25. Set the following AAA TACACS **Service Protocol Settings** parameters:

<b>Service Name</b>	Configure a shell service for user authorization.
<b>Service Protocol</b>	Configure a protocol for user authentication using the service in the <i>Service Name</i> field.



**NOTE:** 5 entries can be made in the **Service Protocol Settings** table.

---

---

26. Select **OK** to save the updates. Select **Reset** to revert to last saved configuration.

## 7.5 Alias

### ► Network Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An *alias* enables an administrator to define a configuration item, such as a hostname, as an *alias* once and use the defined *alias* across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the *Alias* used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration > Network > Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from **Configuration > Devices > System Profile > Network > Alias** screen. These aliases are available for use to a specific group of wireless controllers or access points. *Alias* values defined in this profile override alias values defined within global aliases.
- *RF Domain aliases* are defined from **Configuration > Devices > RF Domain > Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an *Network Alias* defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias works with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias can be classified as:

- *Network Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

### 7.5.1 Network Basic Alias

#### ► Alias

A *basic alias* is a set of configurations that consist of VLAN, host, network and address range alias configurations. VLAN configuration is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

A basic alias configuration can contain multiple instances for each of the five (5) alias types.

To edit or delete a basic alias configuration:

1. Select **Configuration** tab from the web user interface.
2. Select **Network**.
3. Select the **Alias** item, the **Basic Alias** screen displays.

The screenshot shows the 'Basic Alias' configuration screen. It contains four tables for defining aliases:

- Vlan Alias:** A table with columns 'Name' and 'Vlan'. It contains one entry: Name '\$TPLL', Vlan '1'.
- Host Alias:** A table with columns 'Name' and 'Host'. It contains one entry: Name '\$DNS\_Main', Host '192.168.13.2'.
- Address Range Alias:** A table with columns 'Name', 'Start IP', and 'End IP'. It contains one entry: Name '\$IPRange\_S', Start IP '172.16.10.11', End IP '172.16.10.100'.
- Network Alias:** A table with columns 'Name' and 'Network'. It contains one entry: Name '\$NW\_01', Network '192.168.13.0/24'.

Each table has an 'Add Row' button and a trash icon. At the bottom of the screen are 'OK' and 'Reset' buttons.

**Figure 7-22** Network - Basic Alias Screen

4. Select **+ Add Row** to define **VLAN Alias** settings:

Use the **VLAN Alias** field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

<b>Name</b>	If adding a new <i>VLAN Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>VLAN</b>	Use the spinner control to set a numeric VLAN from 1 - 4094.

A *VLAN Alias* can be used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3

- Switchport
  - Wireless LANs
5. Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

<b>Name</b>	If adding a new <i>Address Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Start IP</b>	Set a starting IP address used with a range of addresses utilized with the address range alias.
<b>End IP</b>	Set a ending IP address used with a range of addresses utilized with the address range alias.

An *address range alias* can be used to replace an IP address range in IP firewall rules.

6. Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	Set the IP address of the host machine.

A *host alias* can be used to replace hostnames in the following locations:

- IP Firewall Rules
  - DHCP
7. Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	Provide a network address in the form of <i>host/mask</i> .

A *network alias* can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

8. Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called *loc1.domain.com* and at another deployment location it is called *loc2.domain.com*, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the *loc1.domain.com* domain and at the other with the *loc2.domain.com* domain.

<b>Name</b>	If adding a new <i>String Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	Provide a string value to use in the alias.

A *string alias* can be used to replace domain name strings in DHCP.

9. Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

## 7.5.2 Network Group Alias

### ► Alias

A *network group alias* is a set of configurations that consist of host and network configurations. Network configurations are complete networks in the form 192.168.10.0/24 or IP address range in the form 192.168.10.10-192.168.10.20. Host configuration is in the form of single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for host, network, and IP address range. A maximum of eight (8) host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

A network group alias is used in IP firewall rules to substitute hosts, subnets and IP address ranges:

To edit or delete a network alias configuration:

1. Select **Configuration** tab from the user interface.
2. Select **Network**.
3. Select the **Alias** item. The **Basic Alias** screen displays.
4. Select the **Network Group Alias** tab. The following screen displays:



Name \$NGA\_01 ?

Host

1.2.3.4  
2.3.4.5  
3.4.5.6

Network

192.168.13.0/24

Range

Start IP	End IP	
1.2.3.4	4.3.2.1	<input type="button" value="🗑"/>
		<input type="button" value="🗑"/>

**Figure 7-24** Network - Alias - Network Group Alias Add screen

6. If adding a new **Network Group Alias**, provide it a name of up to 32 characters.



**NOTE:** The **Network Group Alias Name** always starts with a dollar sign (\$).

7. Define the following network group alias parameters:

<b>Host</b>	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
<b>Network</b>	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

8. Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.
9. Select **OK** when completed to update the network group alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### 7.5.3 Network Service Alias

#### ► Alias

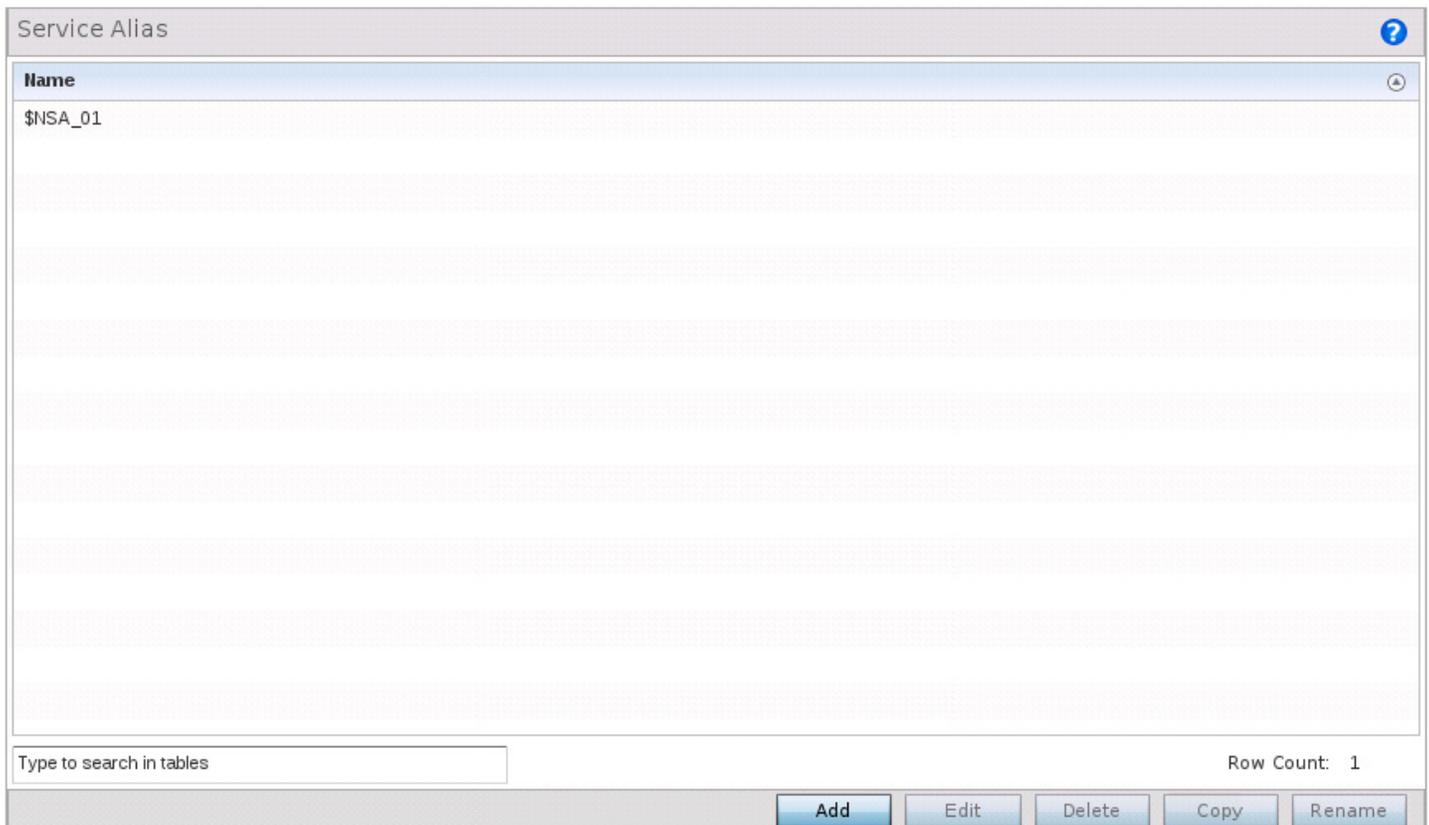
A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

A *network service alias* can be used in IP firewall rules to substitute protocols and ports:

To edit or delete a service alias configuration:

1. Select **Configuration** tab from the web user interface.
2. Select **Network**.
3. Select the **Alias** item, the **Basic Alias** screen displays.
4. Select the **Network Service Alias** tab. The following screen displays:



**Figure 7-25** Network - Alias - Network Service Alias screen

5. Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Service Alias**.

Name \$NSA\_01 ?

Entry

Protocol	Source Port(Low and High)	Destination Port(Low and High)	
* igmp	2	Enter R	
6	80-92	80	

+ Add Row

OK
Reset
Exit

**Figure 7-26** Network - Alias - Network Service Alias Add screen

6. If adding a new **Network Service Alias**, provide it a name up to 32 characters.



**NOTE:** The **Network Service Alias Name** always starts with a dollar sign (\$).

7. Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

<b>Protocol</b>	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from <i>eigrp</i> , <i>gre</i> , <i>icmp</i> , <i>igmp</i> , <i>ip</i> , <i>rrp</i> , <i>igp</i> , <i>ospf</i> , <i>tcp</i> and <i>udp</i> . Select <i>other</i> if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
<b>Source Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
<b>Destination Port (Low and High)</b>	<b>Note:</b> Use this field only if the protocol is <i>tcp</i> or <i>udp</i> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Range</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

8. Select **OK** when completed to update the network service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

## 7.6 Network Deployment Considerations

Before defining an access point network configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- In respect to L2TP V3, data transfers on the pseudowire can start as soon as session establishment corresponding to the pseudowire is complete.
  - In respect to L2TP V3, the control connection keep-alive mechanism of L2TP V3 can serve as a monitoring mechanism for the pseudowires associated with a control connection.
-

# CHAPTER 8

## SECURITY CONFIGURATION

When taking precautions to secure wireless traffic from a client to an access point, the network administrator should not lose sight of the security solution in its entirety, since the network's chain is as weak as its weakest link. An access point managed wireless network provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network. This security is offered at the most granular level, with role and location based secure access available to users based on identity as well as the security posture of the client device.

There are multiple dimensions to consider when addressing the security of an access point managed wireless network, including:

- *Wireless Firewall*
  - *Configuring IP Firewall Rules*
  - *Configuring MAC Firewall Rules*
  - *Wireless IPS (WIPS)*
  - *Device Categorization*
  - *Device Fingerprinting*
  - *Security Deployment Considerations*
-

## 8.1 Wireless Firewall

### ► [Security Configuration](#)

A firewall enforces access control, and is considered a first line of defense in protecting proprietary information within the access point managed network. The means by which this is accomplished varies, but in principle firewalls are mechanisms that block and permit data traffic within the network. Firewalls implement uniquely defined access control policies, so if you do not have an idea of what kind of access to allow or deny, a firewall is of little value, and in fact could provide a false sense of security.

With Motorola Solutions' access points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing wireless clients within the network. Well designed firewalls block traffic from outside the network, but permit authorized users to communicate freely outside the network.

Firewalls can be implemented in both hardware and software, or a combination of both. All traffic entering or leaving the network passes through the firewall, which examines each message and blocks those not meeting the defined security criteria (rules).

Firewall rules define traffic permitted or denied within the network. Rules are processed by a firewall device from first to last. When a rule matches the network traffic processed by an access point, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise of conditions and actions. A condition describes a packet traffic stream. A condition defines constraints on the source and destination devices, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching set conditions. For example, if a packet stream meets all conditions, traffic is permitted, authenticated and sent to the destination device.

Additionally, IP and MAC rule based firewall filtering can be deployed to apply firewall policies to traffic being bridged by radios. IP and MAC filtering can be employed to permit or restrict traffic exchanged between hosts, hosts residing on separate WLANs or hosts forwarding traffic to wired devices.

For more information, refer to the following:

- [Defining a Firewall Configuration](#)
- [Configuring IP Firewall Rules](#)
- [Configuring MAC Firewall Rules](#)

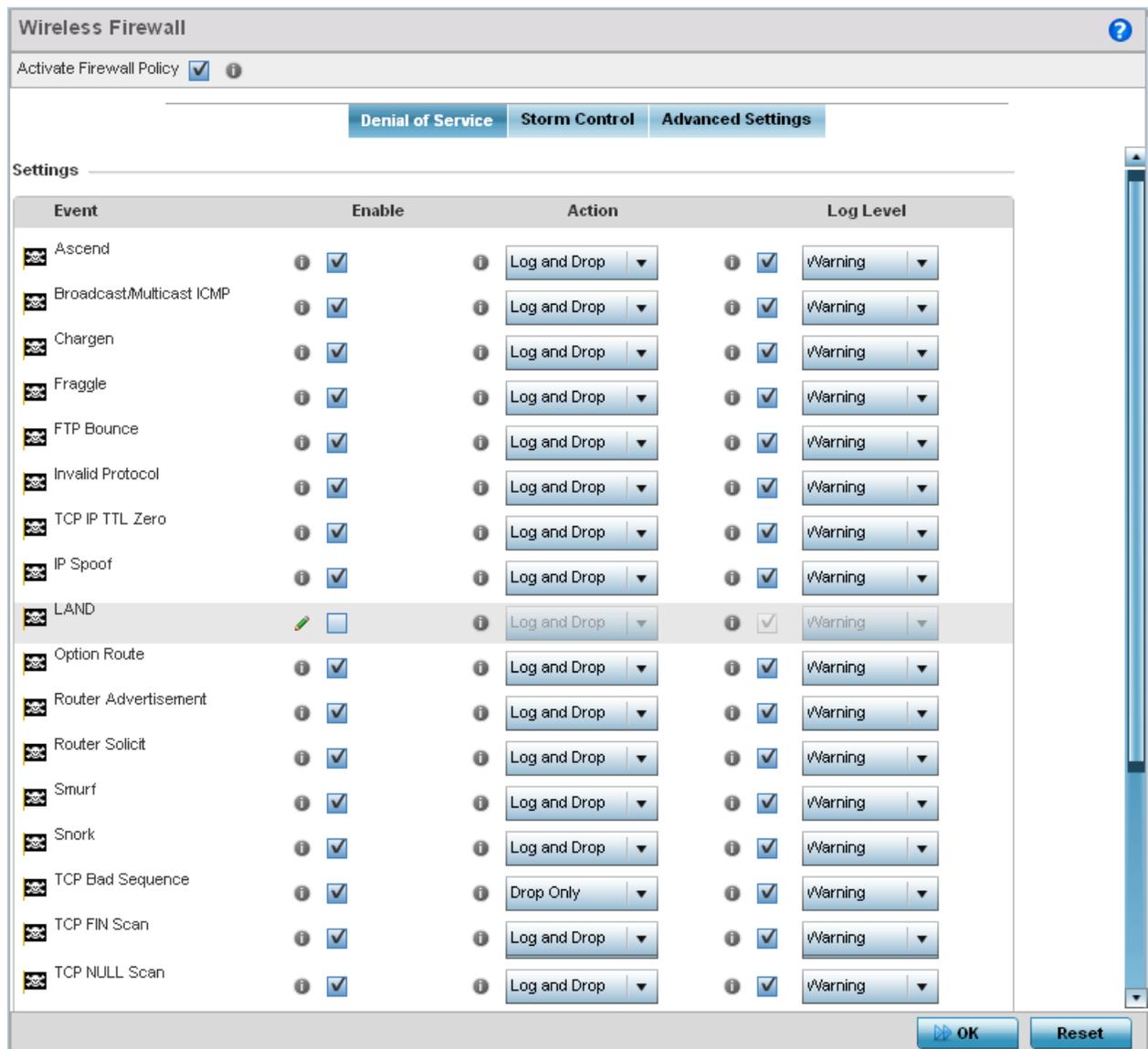
### 8.1.1 Defining a Firewall Configuration

#### ► [Wireless Firewall](#)

To configure a firewall:

1. Select **Configuration** tab from the Web user interface.
2. Select **Security**.
3. Select **Wireless Firewall** to display existing firewall policies.

The **Wireless Firewall** screen lists *Denial of Service*, *Storm Control* and *Advanced Setting* tabs used to create the single Firewall policy used by the access point and its connected devices. The **Denial of Service** tab displays by default.



**Figure 8-1** Wireless Firewall screen - Denial of Service tab

A *denial of service* (DoS) attack is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out a DoS attack will vary, it generally consists of a concerted effort of one or more persons attempting to prevent a device, site or service from functioning temporarily or indefinitely.

Most DoS attacks involve saturating the target device with external communications requests so it cannot respond to legitimate traffic or respond so slowly the device becomes unavailable in respect to its defined data rate. DoS attacks are implemented by either forcing targeted devices to reset or consuming the devices resources so it can no longer provide service.

4. Select the **Activate Firewall Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.

The **Settings** field lists all of the DoS attacks the firewall has filters for. Each DoS filter contains the following four items:

<b>Event</b>	Lists the name of each DoS attack.
<b>Enable</b>	Select <i>Enable</i> to set the firewall to filter the associated DoS attack based on the selection in the <i>Action</i> column.

<b>Action</b>	<p>If a DoS filter is enabled, chose an action from the drop-down menu to determine how the firewall treats the associated DoS attack. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Log and Drop</i> - An entry for the associated DoS attack is added to the log and then the packets are dropped.</li> <li>• <i>Log Only</i> - An entry for the associated DoS attack is added to the log. No further action is taken.</li> <li>• <i>Drop Only</i> - The DoS packets is dropped. No further action is taken.</li> </ul>
<b>Log Level</b>	Select this option to enable logging to the system log. Then select a standard Syslog level from the <i>Log Level</i> drop-down menu.

5. The following **Events** can be filtered on behalf of the firewall:

<b>Ascend</b>	Ascend DoS attacks are a series of attacks that target known vulnerabilities in various versions of Ascend routers.
<b>Broadcast/ Multicast ICMP</b>	Broadcast or Multicast ICMP DoS attacks are a series of attacks that take advantage of ICMP behavior in response to echo requests. These usually involve spoofing the source address of the target and sending ICMP broadcast or multicast echo requests to the rest of the network and in the process flooding the target machine with replies.
<b>Chargen</b>	The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services.
<b>Fraggle</b>	The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic.
<b>FTP Bounce</b>	The FTP Bounce DoS attack uses a vulnerability in the FTP "PORT" command as a way to scan ports on a target machine by using another machine in the middle.
<b>Invalid Protocol</b>	Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack.
<b>TCP IP TTL Zero</b>	The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a <i>Time To Live</i> (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload.
<b>IP Spoof</b>	IP Spoof is an attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.
<b>LAND</b>	The LAND DoS attack sends spoofed packets containing the SYN flag to the target destination using the target port and IP address as both the source and destination. This will either crash the target system or result in high resource utilization slowing down all other processes.
<b>Option Route</b>	Enables the IP Option Route denial of service check in the firewall.

<b>Router Advertisement</b>	In this attack, the attacker uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).
<b>Router Solicit</b>	<p>The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network.</p> <p>ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122).</p> <p>By sending ICMP Router Solicitation packets (ICMP type 9) on the network and listening for ICMP Router Discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.</p>
<b>Smurf</b>	The Smurf DoS Attack sends ICMP echo requests to a list of broadcast addresses in a row, and then repeats the requests, thus flooding the network.
<b>Snork</b>	The Snork DoS attack uses UDP packet broadcasts to consume network and system resources.
<b>TCP Bad Sequence</b>	Enables a TCP Bad Sequence denial of service check in the firewall.
<b>TCP FIN Scan</b>	<p>Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the <i>Finish</i> (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting.</p> <p>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply.</p>

<b>TCP Intercept</b>	<p>A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection.</p> <p>Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing E-mail, using FTP service, and so on.</p> <p>The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP <i>synchronization</i> (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.</p> <p>When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.</p>
<b>TCP Null Scan</b>	<p>Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings.</p> <p>If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.</p>
<b>TCP Post SYN</b>	<p>A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an <i>Intrusion Detection System</i> (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.</p>
<b>TCP Packet Sequence</b>	<p>This is an attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number used by the sending host. If successful, they can send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may originate from some third host controlled by the attacker.</p>
<b>TCP XMAS Scan</b>	<p>The TCP XMAS Scan floods the target system with TCP packets including the FIN, URG, and PUSH flags. This is used to determine details about the target system and can crash a system.</p>
<b>TCP Header Fragment</b>	<p>Enables the TCP Header Fragment denial of service check in the firewall.</p>

<b>Twinge</b>	The Twinge DoS attack sends ICMP packets and cycles through using all ICMP types and codes. This can crash some Windows systems.
<b>UDP Short Header</b>	Enables the UDP Short Header denial of service check in the firewall.
<b>WINNUKE</b>	The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the Net BIOS service on windows and can also result on high CPU utilization on the target machine.

6. Select **OK** to update the Denial of Service settings. Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.
7. Select the **Storm Control** tab. Select the **Activate Firewall Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.

**Wireless Firewall** ?

Activate Firewall Policy  ⓘ

**Denial of Service** **Storm Control** **Advanced Settings**

**Storm Control Settings**

Traffic Type	Interface Type	Interface Name	Packets per Second	
* ARP	* vLAN	* ge2	1	ⓘ

+ Add Row

**Storm Control Logging**

Traffic Type	Logging	
* Unicast	ⓘ <input checked="" type="checkbox"/> Warning	ⓘ

+ Add Row

OK Reset

**Figure 8-2** Wireless Firewall screen - Storm Control tab

The firewall maintains a facility to control packet storms. Storms are packet bombardments that exceed the high threshold configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the interface. Thresholds are configured in terms of packets per second.

8. Refer to the **Storm Control Settings** field to set the following:

<b>Traffic Type</b>	Use the drop-down menu to define the traffic type for which the Storm Control configuration applies. Options include <i>ARP</i> , <i>Broadcast</i> , <i>Multicast</i> and <i>Unicast</i> .
<b>Interface Type</b>	Use the drop-down menu to define the interface for which the Storm Control configuration is applied. Only the specified interface uses the defined filtering criteria. Options include <i>Ethernet</i> , <i>WLAN</i> and <i>Port Channel</i> .
<b>Interface Name</b>	Use the drop-down menu to refine the interface selection to a specific WLAN or physical port. This helps with threshold configuration for potentially impacted interfaces.
<b>Packets per Second</b>	Select the check box to activate the spinner control used to specify the packets per second threshold for activating the Storm Control mechanism.

9. Select **+ Add Row** as needed to add additional Storm Control configurations for other traffic types or interfaces. Select the **Delete** icon as required to remove selected rows.
10. Refer to the **Storm Control Logging** field to define how storm events are logged.

<b>Traffic Type</b>	Use the drop-down menu to define the traffic type for which the Storm Control logging configuration applies. Options include <i>ARP</i> , <i>Broadcast</i> , <i>Multicast</i> and <i>Unicast</i> .
<b>Logging</b>	Select the check box to activate the spinner control used to specify the standard log level used if a Storm Control attack is detected. The default log level is Warning.

11. Select **+ Add Row** as needed to add additional Storm Control log entries for other interfaces. Select the **Delete** icon as required to remove selected rows.
12. Select **OK** to update the Storm Control settings. Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.
13. Select the **Advanced Settings** tab.

Use the **Advanced Settings** tab to enable/disable the firewall, define application layer gateway settings, flow timeout configuration and TCP protocol checks.

**Wireless Firewall**

Activate Firewall Policy  ⓘ

**Denial of Service** **Storm Control** **Advanced Settings**

**Firewall Status**

ⓘ  Enabled  Disabled

**General**

Enable Proxy ARP ⓘ

DHCP Broadcast to Unicast ⓘ

L2 Stateful Packet Inspection ⓘ

IPMAC Conflict Enable ⓘ

IPMAC Conflict Logging ⓘ  Warning

IPMAC Conflict Action ⓘ Log and Drop

IPMAC Routing Conflict Enable ⓘ

IPMAC Routing Conflict Logging ⓘ  Warning

IPMAC Routing Conflict Action ⓘ Log and Drop

DNS Snoop Entry Timeout ⓘ 1800 (30 to 86,400 second)

IP TCP Adjust MSS ⓘ  472 (472 to 1,460 bytes)

TCP MSS Clamping ⓘ

Max Fragments/Datagram ⓘ 140 (2 to 8,129)

Max Defragmentations/Host ⓘ 8 (1 to 16,384)

Min Length Required ⓘ  8 (8 to 1,500 bytes)

IPv4 Virtual Defragmentation ⓘ

**Application Layer Gateway**

FTP ALG ⓘ

TFTP ALG ⓘ

SIP ALG ⓘ

SCCP ALG ⓘ

FaceTime ALG ⓘ

**Firewall Enhanced Logging**

Log Dropped ICMP Packets ⓘ None

Log Dropped Malformed Packets ⓘ None

Enable Verbose Logging ⓘ

**Stateful Flow Checks**

Enable Stateful DHCP Checks ⓘ

**Flow Timeout**

TCP Close Wait ⓘ 10 Seconds (1 to 32,400)

TCP Established ⓘ 90 Minutes (1 to 540)

TCP Reset ⓘ 10 Seconds (1 to 32,400)

TCP Setup ⓘ 10 Seconds (1 to 32,400)

Stateless TCP Flow ⓘ 90 Seconds (1 to 32,400)

Stateless FIN/RESET Flow ⓘ 10 Seconds (1 to 32,400)

ICMP ⓘ 30 Seconds (1 to 32,400)

UDP ⓘ 30 Seconds (15 to 32,400)

Any Other Flow ⓘ 30 Seconds (1 to 32,400)

**TCP Protocol Checks**

ⓘ  Check TCP states where a SYN packet tears down the flow

ⓘ  Check unnecessary resends of TCP packet

ⓘ  Check Sequence Number in ICMP Unreachable error packets

ⓘ  Check Acknowledgement Number in RST packets

ⓘ  Check Sequence Number in RST packets

OK Reset

**Figure 8-3** Wireless Firewall screen - Advanced Settings tab

14. Refer to the **Firewall Status** radio buttons to define the firewall as either *Enabled* or *Disabled*. The firewall is enabled by default.

If disabling the firewall, a confirmation prompt displays stating *NAT, wireless hotspot, proxy ARP, deny-static-wireless-client* and *deny-wireless-client* sending not permitted traffic excessively will be disabled.

15. Select **OK** to continue disabling the captive portal.

16. Refer to the **General** field to enable or disable the following firewall parameters:

<b>Enable Proxy ARP</b>	Select the radio button to allow the Firewall Policy to use Proxy ARP responses for this policy on behalf of another device. Proxy ARP allows the firewall to handle ARP routing requests for devices behind the firewall. This feature is enabled by default.
<b>DHCP Broadcast to Unicast</b>	Select the radio button to enable the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This feature is disabled by default.
<b>L2 Stateful Packet Inspection</b>	Select the radio button to enable stateful packet inspection for routed interfaces within the Layer 2 Firewall. This feature is enabled by default.
<b>IPMAC Conflict Enable</b>	Select this option to log and act upon detected IPMAC conflicts. These occur when removing a device from the network and attaching another using the same IP address.
<b>IPMAC Conflict Logging</b>	When enabled, use the drop-down menu to set the logging level ( <i>Error, Warning, Notification, Information</i> or <i>Debug</i> ) if an attack is detected. The default setting is <i>Warning</i> .
<b>IPMAC Conflict Action</b>	Use the drop-down menu to set the action taken when an attack is detected. Options include <i>Log Only, Drop Only</i> or <i>Log and Drop</i> . The default setting is <i>Log and Drop</i> .
<b>IPMAC Routing Conflict Enable</b>	Select this option to enable IPMAC Routing Conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct MAC address.
<b>IPMAC Routing Conflict Logging</b>	Select enable logging for IPMAC Routing Conflict detection. This feature is enabled by default and set to <i>Warning</i> .
<b>IPMAC Routing Conflict Action</b>	Use the drop-down menu to set the action taken when an attack is detected. Options include <i>Log Only, Drop Only</i> or <i>Log and Drop</i> . The default setting is <i>Log and Drop</i> .
<b>DNS Snoop Entry Timeout</b>	Select this option and set a timeout, in seconds, for DNS Snoop Entry. DNS Snoop Entry stores information such as Client to IP Address and Client to Default Gateway(s) and uses this information to detect if the client is sending routed packets to a wrong MAC address.
<b>IP TCP Adjust MSS</b>	Select this option and adjust the value for the <i>maximum segment size</i> (MSS) for TCP segments on the router. Set a value between 472 bytes and 1,460 bytes to adjust the MSS segment size. The default value is 472 bytes.
<b>TCP MSS Clamping</b>	Select this option to enable TCP MSS Clamping. TCP MSS Clamping allows configuration for the maximum segment size of packets at a global level.
<b>Max Fragments/ Datagram</b>	Set the maximum number of fragments (from 2 - 8,129) allowed in a datagram before it is dropped. The default value is 140 fragments.
<b>Max Defragmentations/ Host</b>	Set the maximum number of defragmentations, from 1 - 16,384 allowed per host before it is dropped. The default value is 8.
<b>Min Length Required</b>	Select this option and set a minimum length, from 8 bytes - 1,500 bytes, to enforce a minimum packet size before being subject to fragment based attack prevention.
<b>IPv4 Virtual Defragmentation</b>	Select this option to enable IPv4 Virtual Defragmentation, this helps prevent IPv4 fragments based attacks, such as tiny fragments or large number of ipv4 fragments.

17. The firewall policy allows traffic filtering at the application layer using the **Application Layer Gateway** feature. The Application Layer Gateway provides filters for the following common protocols:

<b>FTP ALG</b>	Select the <i>Enable</i> box to allow FTP traffic through the firewall using its default ports. This feature is enabled by default.
<b>TFTP ALG</b>	Select the <i>Enable</i> box to allow TFTP traffic through the firewall using its default ports. This feature is enabled by default.
<b>SIP ALG</b>	Select the <i>Enable</i> box to allow SIP traffic through the firewall using its default ports. This feature is enabled by default.
<b>SCCP ALG</b>	Select the check box to allow SCCP traffic through the firewall using its default ports. This feature is enabled by default. <i>Signalling Connection Control Part (SCCP)</i> is a network protocol that provides routing, flow control and error correction in telecommunication networks.
<b>FaceTime ALG</b>	Select the check box to allow Apple's FaceTime video calling traffic through the firewall using its default port. This feature is enabled by default.

18. Refer to the **Firewall Enhanced Logging** field to set the following parameters:

<b>Log Dropped ICMP Packets</b>	Use the drop-down menu to define how dropped ICMP packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include <i>Rate Limited, All or None</i> . The default setting is <i>None</i> .
<b>Log Dropped Malformed Packets</b>	Use the drop-down menu to define how dropped malformed packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include <i>Rate Limited, All or None</i> . The default setting is <i>None</i> .
<b>Enable Verbose Logging</b>	Select this option to enable verbose logging for dropped packets. This setting is disabled by default.

19. Select the **Enable Stateful DHCP Checks** radio button to enable the stateful checks of DHCP packet traffic through the firewall. The default setting is enabled. When enabled, all DHCP traffic flows are inspected.

20. Define **Flow Timeout** intervals for the following flow types impacting the firewall:

<b>TCP Close Wait</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds.
<b>TCP Established</b>	Define a flow timeout value in either <i>Seconds</i> (15 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 90 minutes.
<b>TCP Reset</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds.
<b>TCP Setup</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds.
<b>Stateless TCP Flow</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 90 seconds.
<b>Stateless FIN/RESET Flow</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds.

<b>ICMP</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 30 seconds.
<b>UDP</b>	Define a flow timeout value in either <i>Seconds</i> (15 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 30 seconds.
<b>Any Other Flow</b>	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 30 seconds.

21. Refer to the **TCP Protocol Checks** field to set the following parameters:

<b>Check TCP states where a SYN packet tears down the flow</b>	Select the check box to allow a SYN packet to delete an old flow in TCP_FIN_FIN_STATE and TCP_CLOSED_STATE and create a new flow. The default setting is enabled.
<b>Check unnecessary resends of TCP packets</b>	Select the check box to enable the checking of unnecessary resends of TCP packets. The default setting is enabled.
<b>Check Sequence Number in ICMP Unreachable error packets</b>	Select the check box to enable sequence number checks in ICMP unreachable error packets when an established TCP flow is aborted. The default setting is enabled.
<b>Check Acknowledgment Number in RST packets</b>	Select the check box to enable the checking of the acknowledgment number in RST packets which aborts a TCP flow in the SYN state. The default setting is enabled.
<b>Check Sequence Number in RST packets</b>	Select the check box to check the sequence number in RST packets which abort an established TCP flow. The default setting is enabled.

22. Select **OK** to update the Firewall Policy Advanced Settings. Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.

## 8.2 Configuring IP Firewall Rules

### ► Security Configuration

Access points use IP based firewalls like *Access Control Lists (ACLs)* to filter/mark packets based on the IP address from which they arrive, as opposed to filtering packets on Layer 2 ports.

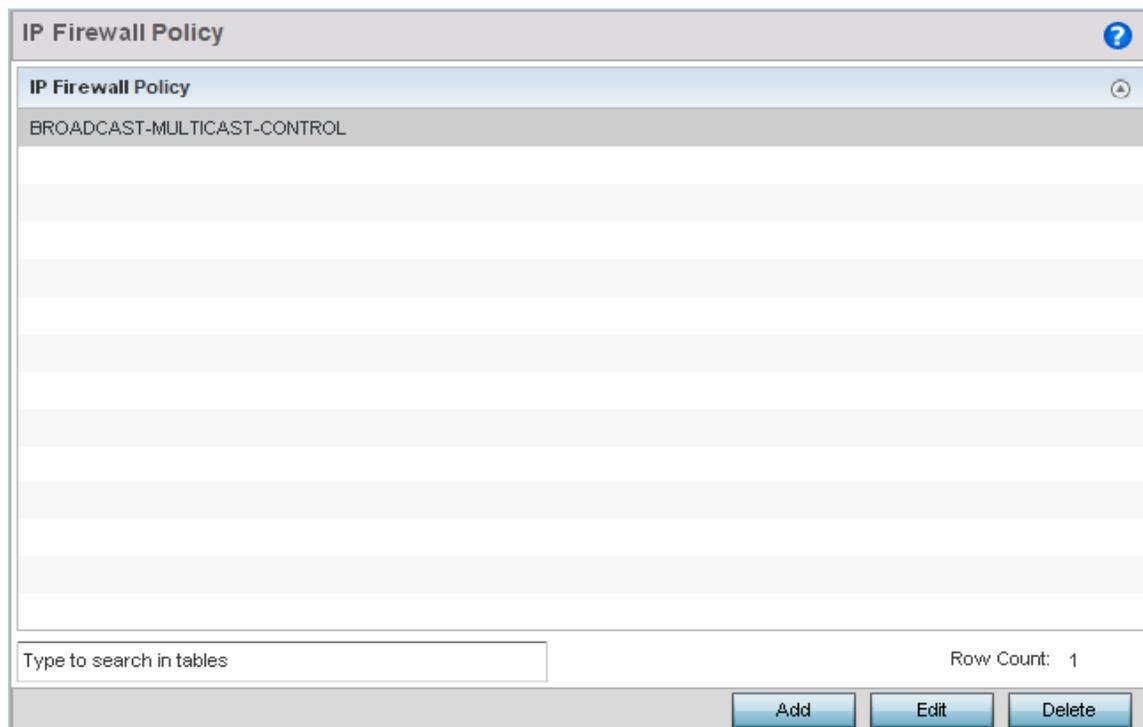
IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying an IP ACL. Firewall rules are processed by a firewall supported device from first to last. When a rule matches the network traffic an access point is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.



**NOTE:** Once defined, a set of IP firewall rules must be applied to an interface to be a functional filtering tool.

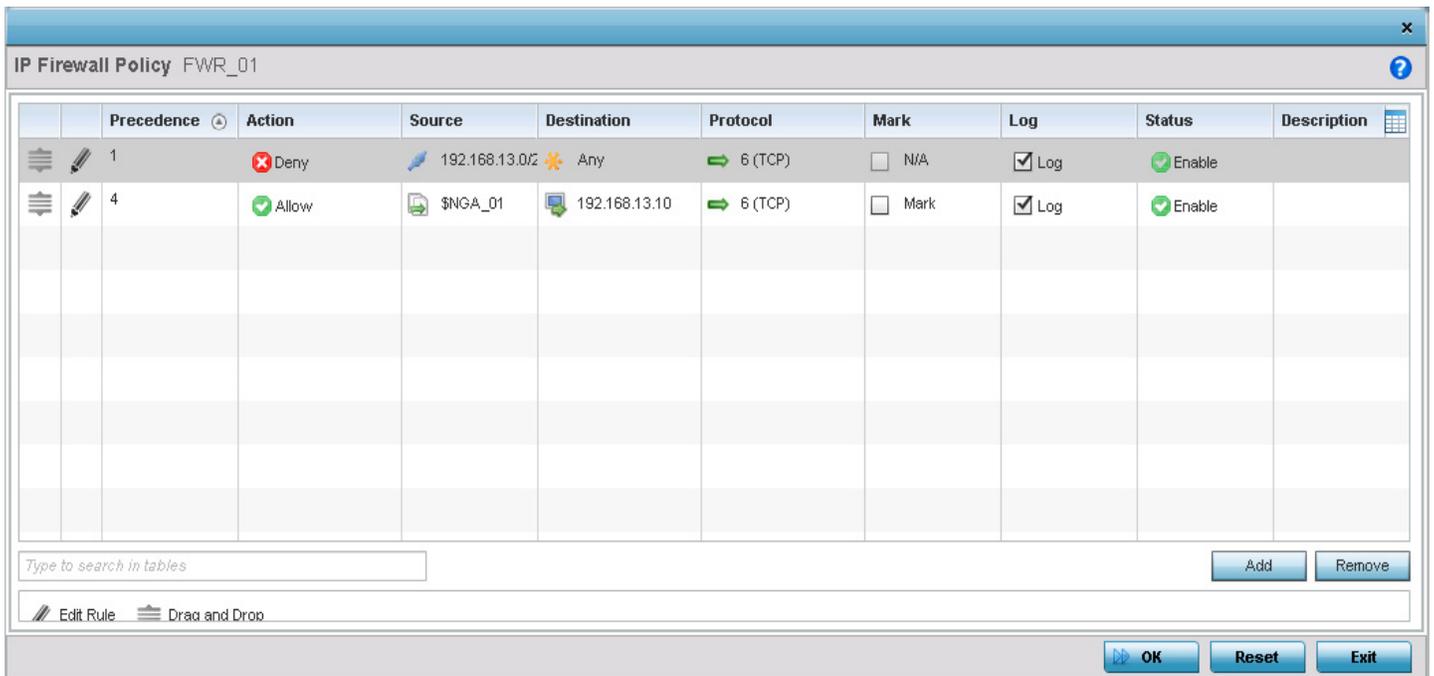
To add or edit an IP based Firewall Rule policy:

1. Select **Configuration** tab from the Web user interface.
2. Select **Security**.
3. Select **IP Firewall** to display existing IP firewall policies.



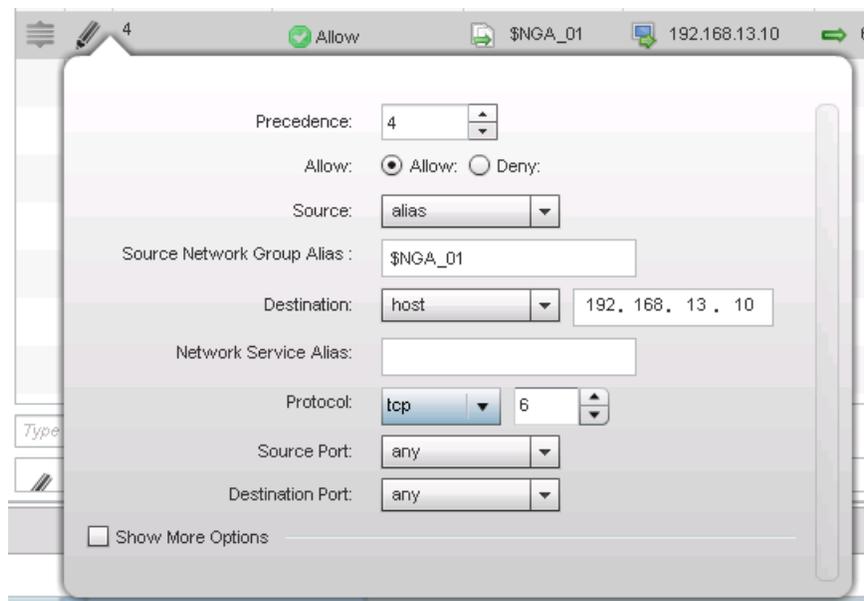
**Figure 8-4** IP Firewall Policy screen

4. Select **Add** to create a new IP Firewall Rule. Select an existing policy and select **Edit** to modify the attributes of the rule's configuration.
5. Select the added row to expand it into configurable parameters for defining a new rule.



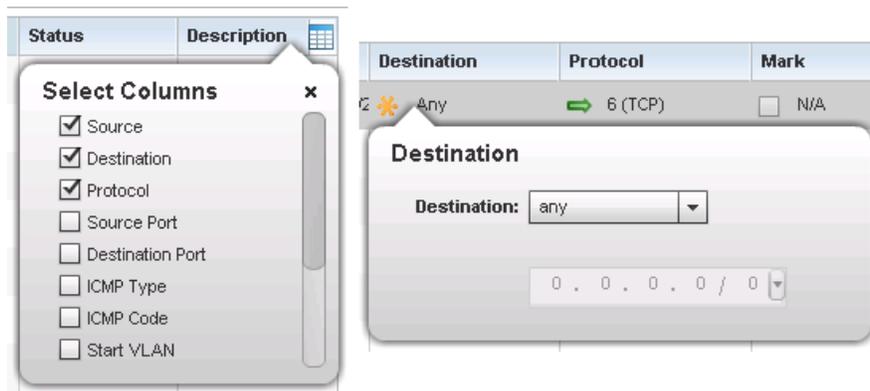
**Figure 8-5** IP Firewall Rules screen - Adding a new rule

6. If adding a new rule, enter a name up to 32 characters.
7. Select **Add** to add a new firewall rule.
8. IP firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.
  - a. Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.



**Figure 8-6** WLAN Security - IP Firewall Rules - Edit Rule screen

- b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.



**Figure 8-7** WLAN Security - IP Firewall Rules - IP Firewall Rules Add Criteria screen



**NOTE:** Only those selected IP ACL filter attributes display. Each value can have its current settings adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

9. Define the following parameters for the IP Firewall Rule:

<b>Precedence</b>	Specify or modify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
<b>Action</b>	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: <ul style="list-style-type: none"> <li>• <i>Deny</i> - Instructs the firewall to prohibit a packet from proceeding to its destination.</li> <li>• <i>Allow</i> - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
<b>Source</b>	Select the source for creating the ACL. <i>Source</i> options include: <ul style="list-style-type: none"> <li>• <i>Any</i> – Indicates any host device in any network.</li> <li>• <i>Network</i> – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.</li> <li>• <i>Host</i> – Indicates a single host with a specific IP address.</li> <li>• <i>Alias</i> – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.</li> </ul>
<b>Destination</b>	Select the destination for creating the ACL. <i>Destination</i> options include: <ul style="list-style-type: none"> <li>• <i>Any</i> – Indicates any host device in any network.</li> <li>• <i>Network</i> – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network.</li> <li>• <i>Host</i> – Indicates a single host with a specific IP address.</li> <li>• <i>Alias</i> – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.</li> </ul>

<b>Network Service Alias</b>	The service alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a \$ character and containing one special character) and include the protocol as relevant. Selecting either <i>tcp</i> or <i>udp</i> displays an additional set of specific TCP/UDP source and destinations port options.
<b>Source Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the source port for incoming IP ACL rule application is <i>any</i> , <i>equals</i> or an administrator defined <i>range</i> . If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting <i>equals</i> invokes a spinner control for setting a single numeric port. Selecting <i>range</i> displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings. A source port cannot be a destination port.
<b>Destination Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the destination port for incoming IP ACL rule application is <i>any</i> , <i>equals</i> or an administrator defined <i>range</i> . If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting <i>equals</i> invokes a spinner control for setting a single numeric port. Selecting <i>range</i> displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings.
<b>ICMP Type</b>	Selecting <i>ICMP</i> as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The <i>Internet Control Message Protocol</i> (ICMP) uses messages identified by numeric <i>type</i> . ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
<b>ICMP Code</b>	Selecting <i>ICMP</i> as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding <i>code</i> , helpful for troubleshooting network issues (0 - <i>Net Unreachable</i> , 1- <i>Host Unreachable</i> , 2 - <i>Protocol Unreachable</i> etc.).
<b>Start VLAN</b>	Select a Start VLAN icon within a table row to set (apply) a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
<b>End VLAN</b>	Select an End VLAN icon within a table row to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
<b>Protocol</b>	Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number.
<b>Mark</b>	Select this option to mark certain fields inside a packet before allowing them. Mark is only applicable for <i>Allow</i> rules. Mark sets the rule's 802.1p or <i>dscp</i> level (from 0 - 7).
<b>Log</b>	Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed.
<b>Status</b>	Select this option to enable or disable this particular IP Firewall rule in this rule set.
<b>Description</b>	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a <i>Select Columns</i> screen used to add or remove IP ACL criteria from the table.

10. Select **Add** as needed to add additional IP Firewall Rule configurations. Select the **Remove** icon as required to remove selected IP Firewall Rules.
  11. Select **OK** when completed to update the IP Firewall rules. Select **Reset** to revert back to the last saved configuration.
-

## 8.3 Device Fingerprinting

### ► Security Configuration

With the increase in popularity of *Bring Your Own Devices* (BYOD) for use in the corporate environment, there is an increase in the number of possible vectors of attacks on the network. BYOD devices are inherently unsafe as the organization does not have control on the level of security on these devices. The organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting feature enables administrators to control how BYOD devices access the network and control their access permissions.



**NOTE:** Ensure DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

To configure device fingerprinting:

1. Select **Configuration** tab from the Web user interface.
2. Select **Security**
3. Select **Device Fingerprinting** to display existing device fingerprinting configuration screens. The **Client Identity** screen displays:

Client Identity <span style="float: right;">?</span>	
Name	⌵
Android-2-1	
Android-2-2	
Android-2-3	
Android-2-3-x	
Android-3	
Android-4	
Android-4-1-X	
Android-4-2-X	
Galaxy-Note	
Galaxy-Tab	
iPhone-iPad	
Mac-OS-X	
Motorola-XOOM	
Ubuntu-11	
Windows-7	
Windows-8	
Windows-Phone-7-5	
Windows-XP	

Type to search in tables Row Count: 18

**Figure 8-8** Security - Device Fingerprinting - Client Identity screen



Name  Pre-defined **Android-4-2-X**  Custom

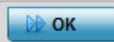
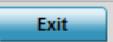
**DHCP Match Criteria**

Index	Message Type	Match Option	Match Type	Value Format	Option Value	
1	Request	55	Exact	Hex String	012103060f1c333a3b	
2	Request	60	Exact	ASCII	dhcpcd-5.5.6	

 Add Row

**Settings**

DHCP Match Message Type  **Request** ▼

**Figure 8-10** Security - Device Fingerprinting - New Client Identity - Pre-defined Identity screen

6. To create a custom client identity, select **Custom** and provide a name in the adjacent field and click the **OK** button at the bottom of the screen.
7. From the **DHCP Match Message Type** drop-down menu, select the message type to match. The available options are *request*, *discover*, *any* and *all*. Use this option to select the message type on which the fingerprint is matched.
  - *request* - Indicates the fingerprint is only checked with any DHCP request message received from any device.
  - *discover* - Indicates the fingerprint is only checked with any DHCP discover message received from any device.
  - *any* - Indicates the fingerprint is checked with either the DHCP request or the DHCP discover message.
  - *all* - Indicates the fingerprint is checked with both the DHCP request and DHCP discover message.
8. Click the **Add Row** to add a new signature to include in the client identity.

Name ClientIdentity\_MobileDevice

DHCP Match Criteria

Index	Message Type	Match Option	Match Type	Value Format	Option Value	
1	request	<input checked="" type="radio"/> Option-Codes	Exact	Hex String		

+ Add Row

Settings

OK Reset Exit

**Figure 8-11** Security - Device Fingerprinting - Client Signature screen

9. Provide the following information for each device signature:

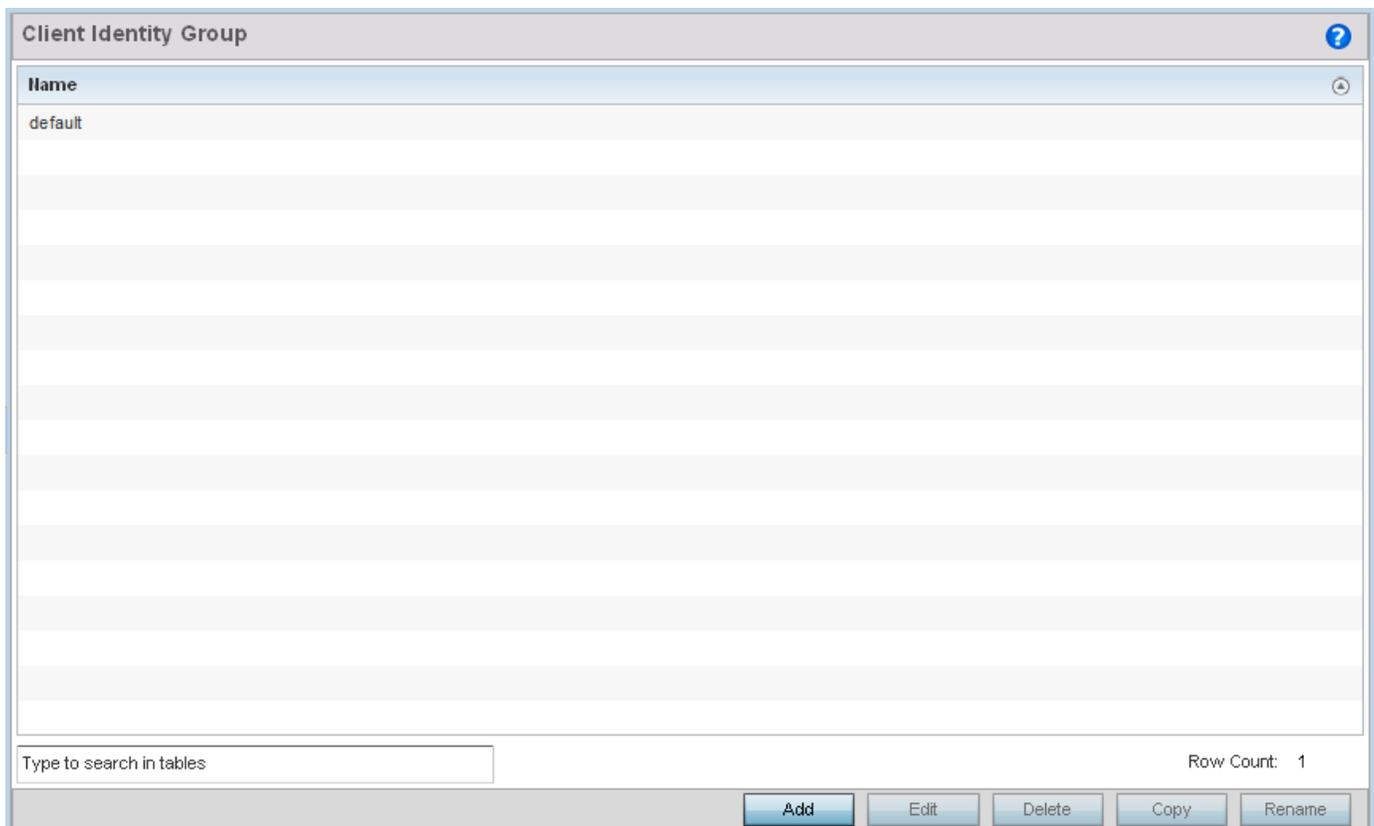
<b>Index</b>	Use the spinner control to assign an index for this signature. A maximum of 16 signatures can be created in each Client Identity.
<b>Message Type</b>	Use the drop-down menu to designate the DHCP message to look for the signatures. <ul style="list-style-type: none"> <li><i>request</i> – look for signature in the DHCP request messages.</li> <li><i>discover</i> – look for signature in the DHCP discover messages.</li> </ul>
<b>Match Option</b>	The <i>Match Option</i> field contains the following options: <ul style="list-style-type: none"> <li><i>Option Codes</i> – This indicates that the Option Codes passed in the DHCP request/discover message is used for matching. Options are passed in the DHCP discover/request messages as <i>Option Code</i>, <i>Option Type</i>, <i>Option Value</i> sets. When <i>Option Codes</i> is selected, all the Option Code passed in the DHCP discover/request are extracted and a fingerprint is derived. This derived fingerprint is used to identify the device.</li> <li><i>Option</i> – This indicates that a specific DHCP Option is used to identify the device. When this option is selected, a text box is enable to input the DHCP Option that is used for fingerprinting.</li> </ul>

<b>Match Type</b>	Use the drop-down menu to select how the signatures are matched. The available options are: <ul style="list-style-type: none"> <li>• <i>Exact</i> – The complete signature string completely matches the string specified in the <i>Option Value</i> field.</li> <li>• <i>starts-with</i> – The signature is checked if it starts with the string specified in the <i>Option Value</i> field.</li> <li>• <i>Contains</i> – The signature is checked if it contains a particular string specified in the <i>Option Value</i> field.</li> </ul>
<b>Value Format</b>	Use the drop-down menu to select the format of the value that is being checked. The value can be either <i>ASCII</i> or <i>Hexadecimal</i> .
<b>Option Value</b>	Use this text box to set the 64 character maximum DHCP option value to match.

10. Click **Ok** to save changes. Click **Reset** to revert all changes made to this screen.

Click **Exit** to close the *Client Identity* screen.

11. From the main menu on the left, select **Client Identity Group** item. The following screens displays:



**Figure 8-12** Security - Device Fingerprinting - Client Identity Group

*Client Identity Group* is a collection of *Client Identities*. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have

a different signature from Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

12. Select **Add** to create a new *Client Identity Group* policy. Client Identity Group policies configure the signatures used to identify clients and then use these signatures to classify and assign permissions to them.

Click **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

Name \* |

**DHCP Match Criteria**

Client Identity	Precedence	

+ Add Row

OK Reset Exit

**Figure 8-13** Security - Device Fingerprinting - Client Identity Group - New Client Identity Group

13. Provide a name in the **Name** field for the new client identity and click the **OK** button at the bottom of the screen.
14. Click the **Add Row** to add a new signature included in the client identity.

Name ClientIdentityGroup\_CIG

DHCP Match Criteria

Client Identity	Precedence	
ClientIdentity_MobileDevices	1	
* <input type="text"/>	<input type="text" value="1"/>	

+ Add Row

OK Reset Exit

**Figure 8-14** Security - Device Fingerprinting - Client Identity Group - New Client Identity Group

15. From the drop-down, select the *Client Identity Policy* to include in this group. Use the buttons next to the drop-down to manage and create new *Client Identity* policies.
16. Use the **Precedence** control to set the precedence for the Client Identity. This index sets the sequence the client identity in this Client Identity Group is checked or matched.
17. Click **Ok** to save changes. Click **Reset** to revert all changes made to this screen.  
Click **Exit** to close the *Client Identity Group* screen.

## 8.4 Configuring MAC Firewall Rules

### ► Security Configuration

Access points can use MAC based firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on Layer 2 ports.

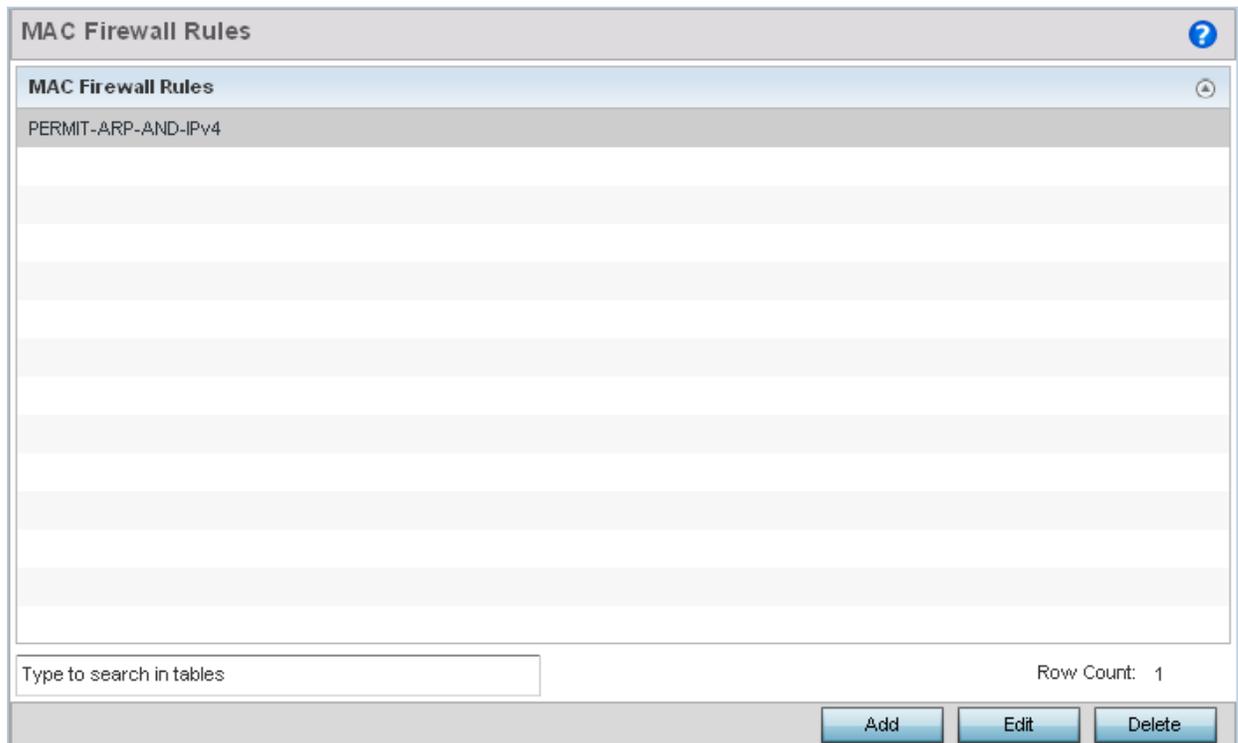
Optionally filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.



**NOTE:** Once defined, a set of MAC firewall rules must be applied to an interface to be a functional filtering tool.

To add or edit a MAC based Firewall Rule policy:

1. Select **Configuration** tab from the Web user interface.
2. Select **Security**.
3. Select **MAC Firewall Rules** to display existing MAC Firewall Rule policies.



**Figure 8-15** MAC Firewall Rules screen

4. Select **Add** to create a new MAC Firewall Rule. Select an existing policy and select **Edit** to modify the attributes of the rule's configuration.
5. Select the added row to expand it into configurable parameters for defining the MAC based firewall rule.

The screenshot shows the 'MAC Firewall Rules' configuration window. The title bar indicates the current rule is 'Rule2'. The main area contains a table with one rule entry:

Precedence	Rules
1	deny any any

Below the table, the configuration details for the selected rule are shown:

- Allow:** Deny
- Source MAC:** Any
- Destination MAC:** Any
- Action:** Log, Mark
- Ethertype:** other
- VLAN ID:** 1
- Match 802.1P:** 0
- Precedence:** 1
- Description:** (empty field)

At the bottom of the rule configuration area, there are 'Add Row' and 'Delete Row' buttons. A 'Total Rules:1' indicator is also present. The bottom of the window features 'OK', 'Reset', and 'Exit' buttons.

**Figure 8-16** MAC Firewall Rules screen - Adding a new rule

6. If adding a new **MAC Firewall Rule**, provide a name up to 32 characters in length.
7. Define the following parameters for the MAC Firewall Rule:

<b>Allow</b>	<p>Every MAC firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:</p> <ul style="list-style-type: none"> <li>• <i>Deny</i> - Instructs the firewall to not to allow a packet to proceed to its destination.</li> <li>• <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
<b>Source MAC / Destination MAC</b>	<p>Enter both <i>Source MAC</i> and <i>Destination MAC</i> addresses. Access points use the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.</p>
<b>Action</b>	<p>The following actions are supported:</p> <ul style="list-style-type: none"> <li>• <i>Log</i> - Events are logged for archive and analysis.</li> <li>• <i>Mark</i> - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. <ul style="list-style-type: none"> <li>• VLAN 802.1p priority.</li> <li>• DSCP bits in the IP header</li> </ul> </li> <li>• <i>Mark, Log</i> - Conducts both mark and log functions.</li> </ul>

<b>Precedence</b>	Use the spinner control to specify a precedence for this MAC firewall rule from 1 - 5000. Rules with lower precedence are always applied first to packets.
<b>VLAN ID</b>	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the RADIUS server). The VLAN ID can be from 1 - 4094.
<b>Match 802.1P</b>	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting from 0 - 7.
<b>Ethertype</b>	Use the drop-down menu to specify an Ethertype of either <i>other</i> , <i>ipv4</i> , <i>arp</i> , <i>rarp</i> , <i>appletalk</i> , <i>aarp</i> , <i>mint</i> , <i>wisp</i> , <i>ipx</i> , <i>802.1q</i> and <i>ipv6</i> . An Ethertype is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame.
<b>Description</b>	Provide a description (up to 64 characters) for the rule to help differentiate the it from others with similar configurations.

8. Select **+ Add Row** as needed to add additional MAC Firewall Rule configurations. Select the **- Delete Row** icon as required to remove selected MAC Firewall Rules.
9. Select **OK** when completed to update the MAC Firewall Rules. Select **Reset** to revert to the last saved configuration.

## 8.5 Wireless IPS (WIPS)

### ► Security Configuration

The access point supports *Wireless Intrusion Protection Systems* (WIPS) to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. An access point supports WIPS through the use of dedicated sensor devices designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

Unauthorized APs are untrusted and unsanctioned access points connected to a LAN that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install an unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the-middle attack or take control of wireless clients to launch denial-of-service attacks.



**NOTE:** WIPS is not supported natively by an AP6511 or AP6521 model access point and must be deployed using an external WIPS server resource.

---

---

A WIPS server can be deployed as a dedicated solution within a separate enclosure. When used with associated access point radios, a WIPS deployment provides the following enterprise class security management features:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the wireless network.
- *Rogue Detection and Segregation* - A WIPS supported network distinguishes itself by both identifying and categorizing nearby access points. WIPS identifies threatening versus non-threatening access points by segregating access points attached to the network (unauthorized APs) from those not attached to the network (neighboring access points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of thousands of neighboring access points.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues through the identification and removal of their connected access points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys.

To define an access point's WIPS configuration:

1. Select **Configuration** tab from the Web user interface.
2. Select **Security**
3. Select **Wireless IPS** to display existing Wireless Intrusion Protection policy.

The **Wireless IPS** screen displays the **Settings** tab by default.

---

**Figure 8-17** Wireless IPS screen - Settings tab

4. Select the **Activate Wireless IPS Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.
5. Within the **Wireless IPS Status** field, select either *Enabled* or *Disabled* to activate or de-activate WIPS. The default setting is enabled.
6. Enter an **Interval to Throttle Duplicates** in either *Seconds* (1 - 86,400), *Minutes* (1 - 1,400), *Hours* (1 - 24) or *Days* (1). This interval represents the duration event duplicates are *not* stored in history. The default setting is 120 seconds.
7. Refer to the **Rogue AP Detection** field to define the following detection settings for this WIPS policy:

<b>Enable Rogue AP Detection</b>	Select the check box to enable the detection of unsanctioned APs from this WIPS policy. The default setting is disabled.
<b>Wait Time to Determine AP Status</b>	Define a wait time in either <i>Seconds</i> (10 - 600) or <i>Minutes</i> (0 - 10) before a detected AP is interpreted as a rogue (unsanctioned) device, and potentially removed. The default interval is 1 minute.
<b>Ageout for AP Entries</b>	Set the interval the WIPS policy uses to ageout rogue devices. Set the policy in either <i>Seconds</i> (30 - 86,400), <i>Minutes</i> (0- 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). The default setting is 5 minutes.

8. Refer to the **Device Categorization** field to associate a Device Categorization Policy with this Wireless IPS policy. Select the **Add** icon to create a new Device Categorization policy, or select the **Edit** icon to modify an existing Device Categorization policy.

9. Select **OK** to update the settings. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.
10. Select the **WIPS Events** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters. This option need to remain selected to apply the WIPS configuration to the access point profile. The **Excessive** tab displays by default, with additional **MU Anomaly** and **AP Anomaly** tabs also available.

**Wireless IPS** ?

Activate Wireless IPS Policy  i

Settings
WIPS Events
WIPS Signatures

---

Excessive
MU Anomaly
AP Anomaly

**Excessive Actions Events**

Name	Enable	Filter Expiration	Client Threshold	Radio Threshold
802.11 Replay Check Failure	✗	0s	10	25
Aggressive Scanning	✗	0s	30	200
Authentication Server Failures	✗	0s	5	20
Decryption Failures	✗	0s	25	75
DoS Association or Authentication Flood	✗	0s	25	45
DoS EAPOL Start Storm	<input checked="" type="checkbox"/> Enabled <span style="float: right;">i</span>	0 <span style="float: right;">i</span>	Seconds <span style="float: right;">i</span> 10 <span style="float: right;">i</span>	20 <span style="float: right;">i</span>
DoS Unicast Deauthentication or Disassociatic	✗	0s	25	45
EAP Flood	✗	0s	15	40
EAP-NAK Flood	✗	0s	10	20
Frames from Unassociated Stations	✗	0s	2	0

OK
Reset

**Figure 8-18** Wireless IPS screen - WIPS Events - Excessive tab

The **Excessive** tab lists events with the potential of impacting network performance. An administrator can enable or disable event filtering and set the thresholds for the generation of the event notification and filtering action.

An *Excessive Action Event* is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the **Excessive Actions Events** table to select and configure the action taken when events are triggered.

11. Set the following **Excessive Action Event** configurations:

Name	
	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.

<b>Enable</b>	Displays whether tracking is enabled for each event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default.
<b>Filter Expiration</b>	Set the duration an event generating client is filtered. This creates a special ACL entry, and frames coming from the client are dropped. The default setting is 0 seconds.  This value is applicable across the RF Domain. If a station is detected performing an attack and is filtered by an access point, the information is passed to the domain controller. The domain controller then propagates this information to all the access points in the RF Domain.
<b>Client Threshold</b>	Set the client threshold after which the filter is triggered and an event generated.
<b>Radio Threshold</b>	Set the radio threshold after which an event is recorded to the event history.

- Select **OK** to save the updates to the to Excessive Actions configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.
- Select the **MU Anomaly** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

The screenshot shows the 'Wireless IPS' configuration window. At the top, there is a header 'Wireless IPS' with a help icon. Below it, a checkbox 'Activate Wireless IPS Policy' is checked. There are two rows of tabs: 'Settings', 'WIPS Events', and 'WIPS Signatures' in the first row; and 'Excessive', 'MU Anomaly', and 'AP Anomaly' in the second row. The 'MU Anomaly' tab is selected. Below the tabs is a section titled 'MU Anomaly Events' containing a table with the following data:

Name	Enable	Filter Expiration
Crackable WEP IV Key Used	X	0s
DoS Broadcast Deauthentication	X	0s
All Zero MAC Address Observed	X	0s
Invalid Frame Type Detected	X	0s
Invalid Management Frame	X	0s
Invalid Sequence Number	Enabled	0
Identical Source/Destination Address	X	0s
Invalid 802.1X Frame Detected	X	0s
Netstumbler (v3.2.0, 3.2.3, 3.3.0)	X	0s
Non-Changing WEP IV	X	0s
Non-Conforming-Data	X	0s
TKIP MIC Counter Measures by Station	X	0s

At the bottom of the window, there are 'OK' and 'Reset' buttons.

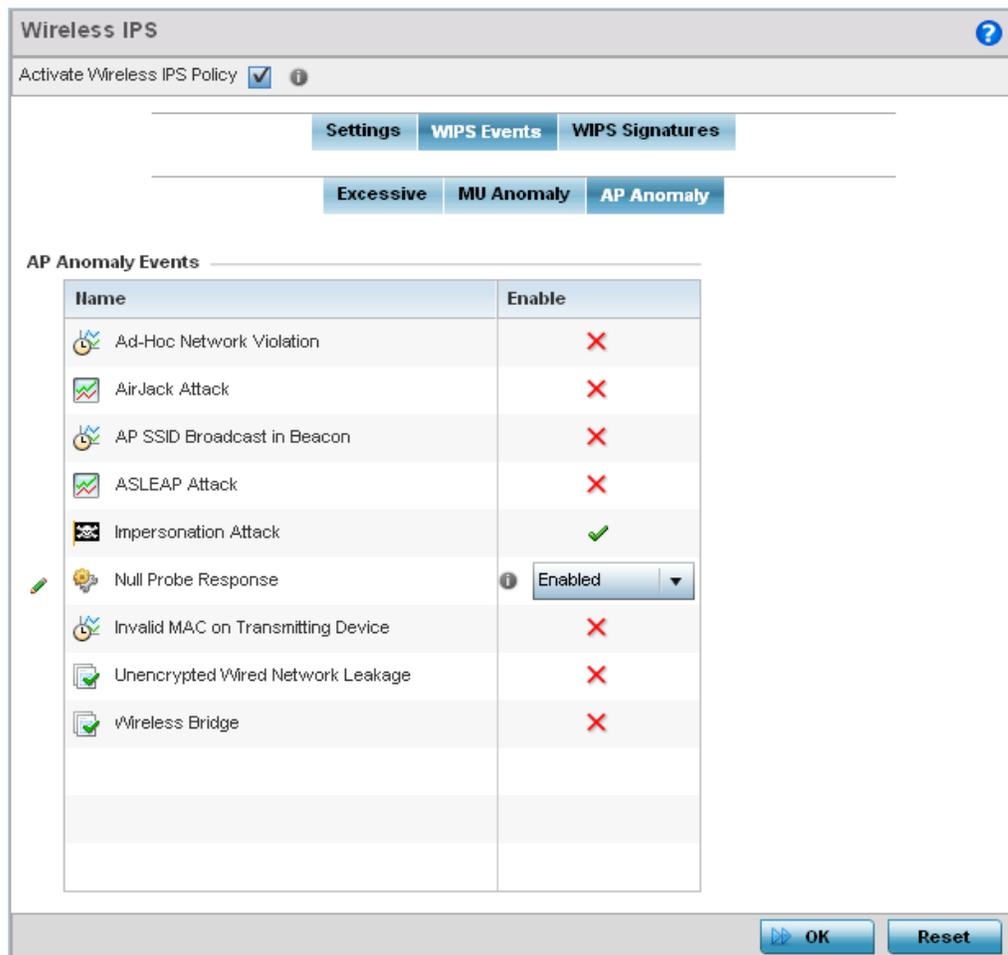
**Figure 8-19** Wireless IPS screen - WIPS Events - MU Anomaly tab

*MU Anomaly* events are suspicious events by wireless clients that can compromise the security and stability of the network. Use the MU Anomaly screen to set the intervals clients can be filtered upon the generation of each event.

14. Set the following **MU Anomaly Event** configurations:

<b>Name</b>	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
<b>Enable</b>	Displays whether tracking is enabled for each MU Anomaly event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold. A red "X" defines the event as disabled, and not tracked by the WIPS policy. Each event is disabled by default.
<b>Filter Expiration</b>	Set the duration a client is filtered. This creates a special ACL entry, and frames coming from the client are silently dropped. The default setting is 0 seconds. For each violation, define a time to filter value (in seconds) which determines how long received packets are ignored from an attacking device once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.

15. Select **OK** to save the updates to the MU Anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.
16. Select the **AP Anomaly** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.



**Figure 8-20** Wireless IPS screen - WIPS Events - AP Anomaly tab

AP Anomaly events are suspicious frames sent by neighboring APs. Use the **AP Anomaly** tab to enable or disable an event.

17. Enable or disable the following **AP Anomaly Events**:

<b>Name</b>	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
<b>Enable</b>	Displays whether tracking is enabled for each AP Anomaly event. Use the drop-down menu to enable/disable events as required. A green check mark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default.

18. Select **OK** to save the updates to the AP Anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.
19. Select the **WIPS Signatures** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

A WIPS signature is the set or parameters, or pattern, used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them.



**Signature**

Name

**Settings**

Enable Signature

BSSID MAC

Source MAC

Destination MAC

Frame Type to Match

Match on SSID

SSID Length  (0 to 32)

**Thresholds**

Wireless Client Threshold   (1 to 65,535)

Radio Threshold   (1 to 65,535)

**Filter Expiration**

Filter Expiration   (1 to 86,400 seconds)

**Payload**

Index	Pattern	Offset	

**Figure 8-22** WIPS Signature Configuration screen

22. If adding a new WIPS signature, define a **Name** to distinguish it from others with similar configurations. The name cannot exceed 64 characters.
23. Set the following network address information for a new or modified WIPS Signature:

<b>Enable Signature</b>	Select the radio button to enable the WIPS signature for use with the profile. The default signature is enabled.
<b>BSSID MAC</b>	Define a BSS ID MAC address used for matching and filtering with the signature.
<b>Source MAC</b>	Define a source MAC address for the packet examined for matching, filtering and potential device exclusion using the signature.
<b>Destination MAC</b>	Set a destination MAC address for a packet examined for matching, filtering and potential device exclusion using the signature.
<b>Frame Type to Match</b>	Use the drop-down menu to select a frame type for matching with the WIPS signature.
<b>Match on SSID</b>	Sets the SSID used for matching. Ensure it's specified properly or the SSID won't be properly filtered.
<b>SSID Length</b>	Set the character length of the SSID used for matching purposes. The maximum length is 32 characters.

24. Refer to **Thresholds** field to set the thresholds used as filtering criteria.

<b>Wireless Client Threshold</b>	Specify the threshold limit per client that, when exceeded, signals the event. The configurable range is from 1 - 65,535.
<b>Radio Threshold</b>	Specify the threshold limit per radio that, when exceeded, signals the event. The configurable range is from 1 - 65,535.

25. Set a **Filter Expiration** from 1 - 86,400 seconds that specifies the duration a client is excluded from radio association when responsible for triggering a WIPS event.

26. Refer to the **Payload** table to set a numerical index and offset for the WIPS signature.

27. Select **OK** to save the updates to the WIPS Signature configuration. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked and applied to the access point profile by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.





## 8.7 Security Deployment Considerations

### ► *Security Configuration*

Before defining a firewall supported configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Firewalls implement access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value.
- It's important to recognize the firewall's configuration is a mechanism for enforcing a network access policy.
- A role based firewall requires an advanced security license to apply inbound and outbound firewall policies to users and devices. Role based firewalls are not supported on AP6511 and AP6521 model access points.
- Firewalls cannot protect against tunneling over application protocols to poorly secured wireless clients.
- Firewalls should be deployed on WLANs implementing weak encryption to minimize access to trusted networks and hosts in the event the WLAN is compromised.
- Firewalls should be enabled when providing Captive Portal guest access. Firewalls should be applied to Captive Portal enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.

Before configuring WIPS support, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WIPS is best utilized when deployed in conjunction with a corporate or enterprise wireless security policy. Since an organization's security goals vary, the security policy should document site specific concerns. The WIPS system can then be modified to support and enforce these additional security policies
- WIPS reporting tools can minimize dedicated administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be investigated and minimize the need for network monitoring.
- It is important to keep your WIPS system firmware and software up to date. A quarterly system audit can ensure firmware and software versions are current.
- Only a trained wireless network administrator can determine the criteria used to authorize or ignore devices. You may want to consider your organization's overall security policy and your tolerance for risk versus users' need for network access. Some questions that may be useful in deciding how to classify a device are:
  - Does the device conform to any vendor requirements you have?
  - What is the signal strength of the device? Is it likely the device is outside your physical radio coverage area?
  - Is the detected access point properly configured according to your organization's security policies?
- Motorola Solutions recommends trusted and known access points be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.



# CHAPTER 9

# SECURITY CONFIGURATION

Motorola Solutions WING software supports services providing captive portal access, leased DHCP IP address assignments to requesting clients and local RADIUS client authentication.

For more information, refer to the following:

- [\*Configuring Captive Portal Policies\*](#)
- [\*Setting the DNS Whitelist Configuration\*](#)
- [\*Setting the DHCP Server Configuration\*](#)
- [\*Setting the Bonjour Gateway Configuration\*](#)
- [\*Setting the RADIUS Configuration\*](#)

Refer to [\*Services Deployment Considerations on page 9-51\*](#) for tips on how to optimize the access point's configuration.

---

## 9.1 Configuring Captive Portal Policies

### ► Security Configuration

A *captive portal* is an access policy that provides temporary and restrictive access to the access point managed wireless network.

A captive portal policy provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access the wireless network. Once logged into the captive portal, additional *Terms and Conditions*, *Welcome* and *Fail* pages provide the administrator with a number of options on screen flow and appearance.

Captive portal authentication is used primarily for guest or visitor access to the network, but is increasingly used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Each supported access point model can support up to 32 captive portal policies, with the exception of AP6511 and AP6521 models, which can only support 16 captive portal policies.

### 9.1.1 Configuring a Captive Portal Policy

#### ► Configuring Captive Portal Policies

To configure a captive portal policy:

1. Select **Configuration** tab from the Web user interface.
2. Select **Services**.

The upper, left-hand, side of the user interface displays an area where *Captive Portal*, *DNS Whitelist* and *DHCP Server Policy* configuration options can be selected.

3. Select **Captive Portals**.

The **Captive Portal** screen displays the configurations of existing policies. New captive portal access policies can be created, existing policies can be modified or existing policies deleted.



<b>AAA Policy</b>	Lists each AAA policy used to authorize client guest access requests. The security provisions provide a way to configure advanced AAA policies that can be applied to captive portal policies supporting authentication. When a captive portal policy is created or modified, a AAA policy must be defined and applied to authorize, authenticate and account user requests.
-------------------	--

5. Select **Add** to create a new captive portal policy, **Edit** to modify an existing policy or **Delete** to remove an existing captive portal policy.

The **Basic Configuration** tab displays by default. Define the policy's security, access and whitelist basic configuration before defining HTML pages for guest user access.

---

**Captive Portal Policy** test
?

Basic Configuration
Web Page

**Settings**

Captive Portal Server Mode i  Internal (Self)  Centralized  Centralized Controller

Hosting VLAN Interface i  (0 to 4,096)

Captive Portal Server Host i  Hostname

Connection Mode i  HTTP  HTTPS

Simultaneous Users i  (1 to 8,192)

**Security**

AAA Policy i <none> + gears

**Access**

Access Type i  No authentication required  
 Generate Logging Record and Allow Access  
 Custom User Information for RADIUS Authentication  
 RADIUS Authentication i ⚠ Email option is part of experimental feature  
 email

RADIUS Lookup Information i

Terms and Conditions page i

**Client Settings**

Radius VLAN Assignment i

Post Authentication VLAN i  (1 to 4,096)

Client Access Time i  (10 to 10,080 minutes)

Inactivity Timeout i  Minutes ( 5 to 1,440 )

**DNS Whitelist**

DNS Whitelist i  + gears

**Accounting**

Enable RADIUS Accounting i

Enable Syslog Accounting i

Syslog Host i  Hostname

Syslog Port i

**Data Limit**

Limit i  (1 to 102,400 MegaBytes)

Action i Log Only

**Logout FQDN**

Logout FQDN i  (e.g., logout.guestaccess.com)

**Redirection Ports**

Destination Ports for Redirection i  (e.g., 1080,8001,8080-8090)

OK
Reset
Exit

**Figure 9-2** Captive Portal Policy screen - Basic Configuration tab

6. Define the following **Settings** for the captive portal policy:

<b>Captive Portal Policy</b>	If creating a new policy, assign a name representative of its access permissions, location or intended wireless client user base. If editing an existing captive portal policy, the policy name cannot be modified. The name cannot exceed 32 characters.
<b>Captive Portal Server Mode</b>	Set the mode as <i>Internal (Self)</i> , <i>Centralized</i> or <i>Centralized Controller</i> . Select <i>Internal (Self)</i> to maintain the captive portal configuration (Web pages) internally on the access point. Select <i>External (Centralized)</i> if the captive portal is supported on an external server. Select <i>Centralized Controller</i> for the captive portal to reside on the access point's connected Virtual Controller AP. The default value is <i>Internal (Self)</i> .
<b>Hosting VLAN Interface</b>	When <i>Centralized Server</i> is selected as the <i>Captive Portal Server Mode</i> , use the spinner control to set the VLAN where the client can reach the controller. 0 is the default value.
<b>Captive Portal Server Host</b>	Set a numeric IP address (non DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is only available if hosting the captive portal on an <i>External (Centralized)</i> server resource.
<b>Connection Mode</b>	Select either <i>HTTP</i> or <i>HTTPS</i> to define the connection medium. Motorola Solutions recommends the use of <i>HTTPS</i> , as it offers additional data protection <i>HTTP</i> cannot provide. The default value however is <i>HTTP</i> .
<b>Simultaneous Users</b>	Select the check box and use the spinner control to set from 1 - 8192 users (client MAC addresses) allowed to simultaneously access and use the access point's captive portal.

7. Use the **AAA Policy** drop-down menu to select the *Authentication*, *Authorization* and *Accounting* (AAA) policy used to validate user credentials and provide captive portal guest access to the network.

If no AAA policies exist, one must be created by selecting the **Create** icon, or an existing AAA policy can be selected and modified by selecting the **Edit** icon. For information on creating a AAA policy, see [AAA Policy on page 7-12](#).

8. Set the following **Access** parameters to define captive portal access, RADIUS lookup information and whether the login pages contain terms that must be accepted before access is granted:

<b>Access Type</b>	<p>Select the radio button for the authentication scheme applied to wireless clients using the captive portal for guest access. Options include:</p> <ul style="list-style-type: none"> <li>• <i>No authentication required</i> - Clients can freely access the captive portal Web pages without authentication.</li> <li>• <i>Generate Logging Record and Allow Access</i> - Access is provided without authentication, but a record of the accessing client is logged.</li> <li>• <i>Custom User Information for RADIUS Authentication</i> - When selected, accessing clients are required to provide a 1-32 character data string to authenticate the client.</li> <li>• <i>RADIUS Authentication</i> - An accessing client's user credentials require authentication with an external RADIUS resource before access is granted. This is the default setting, as not all supported access points have an onboard RADIUS server.</li> <li>• <i>email</i> - When selected, accessing clients are required to provide an email address to authenticate the client.</li> </ul>
<b>RADIUS Lookup Information</b>	When <i>Custom User Information for RADIUS Authentication</i> is selected as the access type, provide a 1 - 32 character lookup information string used as a customized authentication mechanism.

<b>Terms and Conditions page</b>	Select this option (with any access type) to include terms that must be adhered to for captive portal access. These terms are included in the Terms and Conditions page when No authentication required is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled.
----------------------------------	--

9. Set the following **Client Settings** to define the duration clients are allowed captive portal access and when they're timed out due to inactivity:

<b>RADIUS VLAN Assignment</b>	Select this option to enable the RADIUS server to assign a VLAN post authentication. Once a captive portal user is authenticated, the user is assigned the VLAN as configured in the <i>Post Authentication VLAN</i> field.
<b>Post Authentication VLAN</b>	Use the spinner control to define the VLAN that a captive portal user is assigned once authenticated by a RADIUS server.
<b>Client Access Time</b>	Use the spinner control to define the duration wireless clients are allowed access to the network using the captive portal policy. Set an interval from 30 - 10,800 minutes. The default interval is 1,440 minutes.
<b>Inactivity Timeout</b>	Use the drop-down menu to specify an interval in either <i>Minutes</i> (5 - 30) or <i>Seconds</i> (300 - 1,800) that, when exceeded, times out clients that have not transmitted a packet within the captive portal.

10. Use the **DNS White List** drop-down menu to use a set of allowed destination IP addresses for the captive portal. These allowed DNS destination IP addresses are called a *Whitelist*. If no whitelist entry exists with the correct set of IP addresses, select the **Create** icon (to the right of the drop-down menu) and define a new whitelist. For more information, see [Setting the DNS Whitelist Configuration on page 9-14](#).

Each supported access point model can support up to 32 whitelists, with the exception of AP6511 and AP6521 models which can only support up to 16 whitelists.

To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist.

Refer to the drop-down menu of existing **DNS White List** entries to select a policy to be applied to this captive portal policy.

- a. If creating a new whitelist, assign it a name up to 32 characters. Use the **+ Add Row** button to populate the whitelist table with Host and IP Index parameters that must be defined for each whitelist entry.

The screenshot shows a web-based configuration interface for a Captive Portal DNS Whitelist. At the top, there is a text field labeled 'Name' containing the value 'whitelist1'. Below this is a section titled 'DNS Entries' which contains a table. The table has three columns: 'DNS Entry', 'Match Suffix', and a delete icon. The first row of the table contains the text 'lancelot' in the 'DNS Entry' column, 'Hostname' in the 'Match Suffix' column, and a delete icon. Below the table is a button labeled '+ Add Row'. At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 9-3** Captive Portal DNS Whitelist screen

- b. Provide a numerical IP address or Hostname within the **DNS Entry** parameter for each destination IP address or host in the whitelist.
  - c. Use the **Match Suffix** parameter to match any hostname or domain name as a suffix. The default setting is disabled.
  - d. If necessary, select the radio button of an existing whitelist entry and select the **- Delete** icon to remove the entry from the whitelist.
11. Set the following **Accounting** parameters to define how accounting is conducted for clients entering and exiting the captive portal. Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data (such as captive portal start and stop times), executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track captive portal services users are consuming.

<b>Enable RADIUS Accounting</b>	Select this option to use an external RADIUS resource for AAA accounting for the captive portal. When the radio button is selected, a AAA Policy field displays. This setting is disabled by default.
<b>Enable Syslog Accounting</b>	Select this option to log information about the use of remote access services by users using an external syslog resource. This information is of great assistance in partitioning local versus remote users. Remote user information can be archived to an external location for periodic network and user administration. This feature is disabled by default.

<b>Syslog Host</b>	When syslog accounting is enabled, use the drop-down menu to determine whether an <i>IP address</i> or a <i>host name</i> is used as a syslog host. The IP address or hostname of an external server resource is required to route captive portal syslog events to that destination.
<b>Syslog Port</b>	When syslog accounting is enabled, define the numerical syslog port to route traffic with the external syslog server. The default port is 514.

12. Set the following **Data Limit** parameters:

<b>Limit</b>	Select the option to enable limiting usage. Use the spinner to set a maximum usage limit in megabytes.
<b>Action</b>	Use the drop-down to configure the action to be taken once the data limit is reached. Choose from one of: <ul style="list-style-type: none"> <li>• <i>Log only</i> – Logs the event</li> <li>• <i>log-and-disconnect</i> – Logs the event and disconnects the user.</li> </ul>

13. Set the following **Logout FQDN** parameters:

<b>Logout FQDN</b>	Configure the <i>fully qualified domain name</i> (FQDN) of the domain where the user will be redirected after logging out of the captive portal.
--------------------	--

14. Refer to the **Destination Ports for Redirection** item, and enter destination ports (separated by commas, or using a dash for a range) for consideration when re-directing client connections. Standard ports 80 and 443 are always considered for client connections regardless of what is entered by the administrator.
15. Select **OK** to save the changes made within the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.
16. Select the **Web Page** tab to create HTML pages requesting wireless clients use to login and navigate within the captive portal.

The **Login** page displays by default.

**Captive Portal Policy** policy1

**Basic Configuration** **Web Page**

Web Page Source  Internal  Advanced  Externally Hosted

**Login** **Terms and Conditions** **Welcome** **Fail** **No Service**

Organization's Name

Title Text

Header Text

Login Message

Footer Text

Main Logo URL

Small Logo URL

Signature

A simple auto-generated set of web pages are created based on the provided fields.  
Three separate web pages are provided for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

OK Reset **Exit**

**Figure 9-4** Captive Portal Policy screen - Web Page tab

The *Login* screen prompts for a username and password to access the captive portal and proceed to either the Terms and Conditions page (if used) or the Welcome page. The *Terms and Conditions* page provides conditions that must be agreed to before wireless client guest access is provided for the captive portal policy. The *Welcome* page asserts a user has logged in successfully and can access the captive portal. The *Fail* page asserts the authentication attempt has failed, and the user is not allowed access (using this captive portal policy) and must provide the correct login information again to access the Internet. The *No Service* page asserts that the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically re-connected to the portal.

17. Provide the following required information when creating **Login**, **Terms and Conditions**, **Welcome** and **Fail** pages maintained internally:

<b>Organization's Name</b>	If the captive portal is defined on behalf of an organization, that name can be associated as sponsoring the captive portal.
----------------------------	--

<b>Title Text</b>	Set the title text displayed on the <i>Login, Terms and Conditions, Welcome</i> and <i>Fail</i> pages when wireless clients access each page. The text should be in the form of a page title describing the respective function of each page and should be unique to each login, terms, welcome and fail function.
<b>Header Text</b>	Provide header text unique to the function of each page.
<b>Login Message</b>	Specify a message containing unique instructions or information for the users accessing each specific page. In the case of the Terms and Conditions page, the message can be the conditions requiring agreement before guest access is permitted.
<b>Footer Text</b>	Provide a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of captive portal Web pages.
<b>Main Logo URL</b>	The Main Logo URL is the URL for the main logo image displayed on the Login, Terms and Conditions, Welcome and Fail pages. Use the <i>Browse</i> button to navigate to the location of the target file.
<b>Small Logo URL</b>	The Small Logo URL is the URL for a small logo image displayed on the Login, Terms and Conditions, Welcome and Fail pages. Use the <i>Browse</i> button to navigate to the location of the target file.
<b>Signature</b>	Specify a signature message. This is primarily used to display copyright messages. This field is only displayed on the Login page.

18. Select **OK** to save the changes made within the Internal Pages screen. Selecting **Reset** reverts the settings back to the last saved configuration.
19. If hosting the captive portal on an external system, select the **Externally Hosted** radio button.

Captive Portal Policy policy1 ?

**Basic Configuration** **Web Page**

Web Page Source   Internal  Advanced  Externally Hosted

Login URL

Agreement URL

Welcome URL

Fail URL

Acknowledgement URL

No Service

A set of pre-existing web pages outside of the Controller are specified by the provided URLs. Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

**OK** **Reset** **Exit**

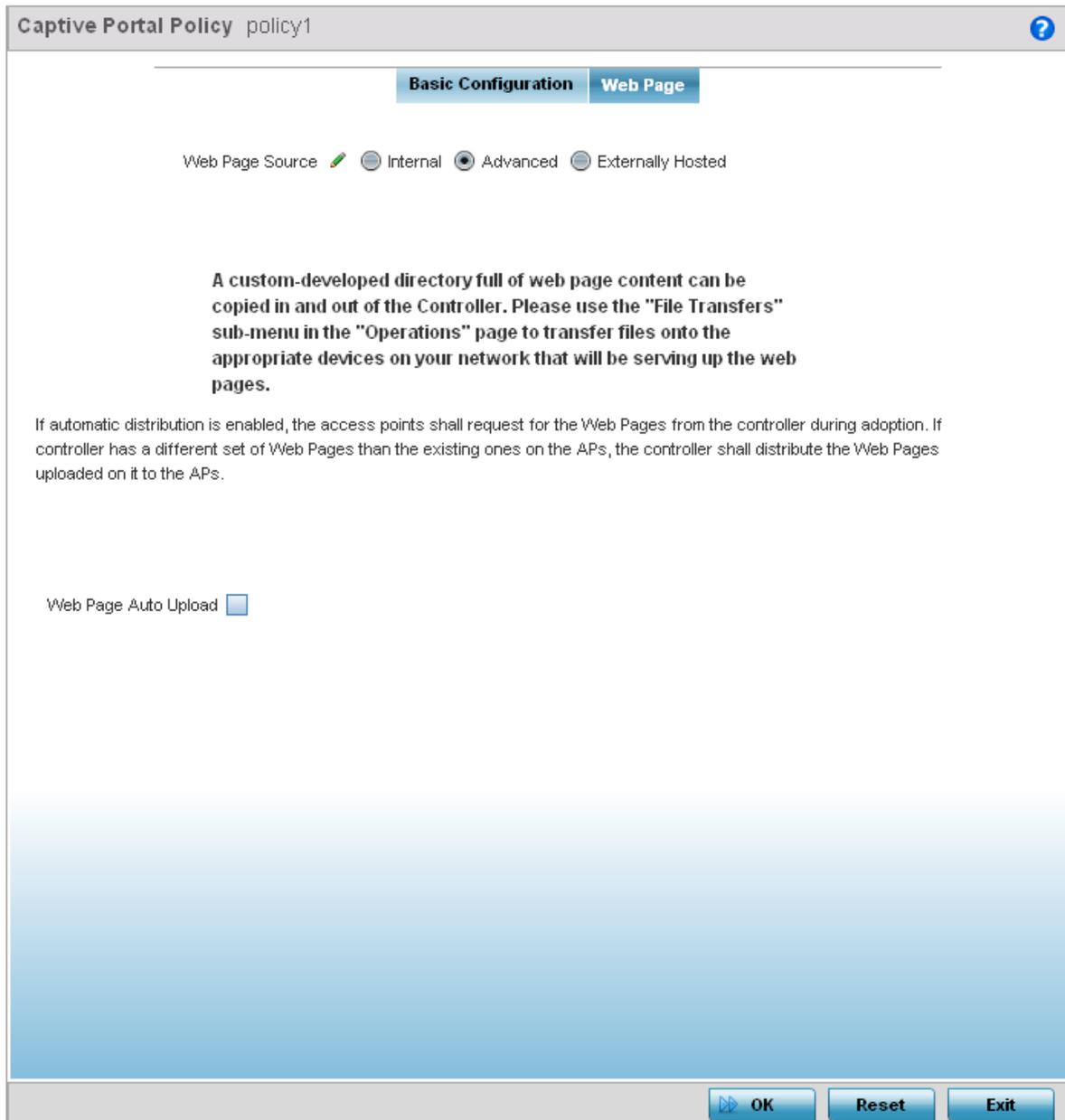
**Figure 9-5** Captive Portal Policy screen - Web Page tab - Externally Hosted Web Page screen

20. Set the following URL destinations for externally hosted captive portal pages:

<b>Login URL</b>	Define the complete URL for the location of the Login page. The Login screen prompts the user for a username and password to access the Terms and Conditions or Welcome page.
<b>Agreement URL</b>	Define the complete URL for the location of the Terms and Conditions page. The Terms and Conditions page provides conditions that must be agreed to before wireless client access is provided.
<b>Welcome URL</b>	Define the complete URL for the location of the Welcome page. The Welcome page asserts the user has logged in successfully and can access resources via the captive portal.
<b>Fail URL</b>	Define the complete URL for the location of the Fail page. The Fail page asserts authentication attempt has failed, and the client cannot access the captive portal and the client needs to provide correct login information to regain access.
<b>Acknowledgement URL</b>	Define the complete URL to the location of the Acknowledgement page. The Acknowledgement URL is needed by returning users whose MAC addresses has been validated previously, but must accept the conditions of the captive portal again.
<b>No Service</b>	Define the complete URL to the location of the No Service page. The No Service URL is needed by users encountering difficulties connecting to the external resource used to host the captive portal pages.

21. Select **OK** when completed to update the captive portal policy settings. Select **Reset** to revert the screen back to its last saved configuration.

22. Select **Advanced** to use a custom directory of Web pages copied to and from the access point for captive portal support.



**Figure 9-6** Captive Portal Policy screen - Web Page tab - Advanced Web Page screen

23. The access point maintains its own set of Advanced Web pages for custom captive portal creation. Refer to **Operations > Devices > File Transfers** and use the *Source* and *Target* fields to move captive portal pages as needed to managed devices that may be displaying and hosting captive portal connections.

Select the **Web Page Auto Upload** check box to enable automatic upload of captive portal Web pages.

For more information, refer to [File Management on page 12-23](#)



## 9.3 Setting the DHCP Server Configuration

### ► [Security Configuration](#)

*Dynamic Host Configuration Protocol* (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The DHCP server ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address management is conducted by the DHCP server, not an administrator.

AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points have an internal DHCP server resource. However, AP6511 and AP6521 models do not have an onboard DHCP server resource and an external resource must be used.

The DHCP server groups wireless clients based on defined user-class option values. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnet. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Numerous DHCP network address credentials can have an *alias* applied. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements. An alias name always starts with a dollar sign (\$) and should not exceed 32 characters. An alias that's applied to a DHCP configuration can be either a *Global*, *Profile*, *RF Domain* or *Device* alias. For more information on aliases and their application, see [Alias on page 7-34](#).

A single DHCP server configuration is supported by the access point, no separate DHCP policies can be defined and maintained. For more information, refer to the following:

- [Defining DHCP Pools](#)
- [Defining DHCP Server Global Settings](#)
- [DHCP Class Policy Configuration](#)

### 9.3.1 Defining DHCP Pools

#### ► [Setting the DHCP Server Configuration](#)

A pool (or range) of IP network addresses and DHCP options can be created for each IP interface configured. This range of addresses can be made available to DHCP enabled wireless devices within the network on either a permanent or leased basis. DHCP options are provided to each DHCP client with a DHCP response and provide DHCP clients information required to access network resources such as a default gateway, domain name, DNS server and WINS server configuration. An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string specified by the DHCP client's vendor.

To define the parameters of a DHCP pool:

1. Select **Configuration** tab from the web user interface.
2. Select **Services**.

3. Select **DHCP Server**. The DHCP Pool tab displays by default.

The screenshot shows the DHCP Server Policy configuration interface. At the top, there is a header 'DHCP Server' with a help icon. Below it, the 'Activate DHCP Server Policy' checkbox is checked. The main area has three tabs: 'DHCP Pool' (selected), 'Global Settings', and 'Class Policy'. A table displays the DHCP pool configuration with the following data:

DHCP Pool	Subnet	Domain Name	Boot File	Lease Time
pool12	157.235.221.0/24	lancelot		1d 0h 0m 0s

At the bottom of the table, there is a search input field labeled 'Type to search in tables' and a 'Row Count: 1' indicator. Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

**Figure 9-8** DHCP Server Policy screen - DHCP Pool tab

4. Select the **Activate DHCP Server Policy** option to optimally display the screen and enable the ability Add or Edit a new policy. This option must remain selected to apply the DHCP pool configuration to the access point profile.
5. Review the following DHCP pool configurations to determine if an existing pool can be used as is, a new one requires creation or edit or a pool requires deletion:

<b>DHCP Pool</b>	Displays the name assigned to the network pool when created. The DHCP pool name represents a group of IP addresses used to assign to DHCP clients upon request. The name assigned cannot be modified as part of the edit process. If a network pool configuration is obsolete it can be deleted.
<b>Subnet</b>	Displays the network address and mask used by clients requesting DHCP resources.
<b>Domain Name</b>	Displays the domain name used with this network pool. Hostnames are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A <i>fully qualified domain name</i> (FQDN) consists of a hostname plus a domain name. For example, <i>computername.domain.com</i> .
<b>Boot File</b>	Boot files ( <i>Boot Protocol</i> ) are used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed.

**Lease Time**

If a lease time has been defined for a listed network pool, it displays as an interval between 1 - 9,999,999 seconds. DHCP leases provide addresses for defined times to various clients. If a client does not use a leased address for the defined time, that IP address can be re-assigned to another DHCP supported client.

6. Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool or **Delete** to remove a pool.

The screenshot shows the 'DHCP Pools' configuration window with the 'Basic Settings' tab selected. It features two 'General' sections. The left section is for subnet configuration, with 'Subnet' set to IP 172.16.10.0/24, and 'Domain Name' and 'DNS Servers' fields. The right section is for lease and router configuration, with 'Lease Time' set to 86400 seconds and 'Default Routers' fields. Below these is an 'IP Address Ranges' table with columns for IP Start, IP End, and Class Policy. At the bottom are 'OK', 'Reset', and 'Exit' buttons.

**Figure 9-9** DHCP Pools screen - Basic Settings tab

If adding or editing a DHCP pool, the DHCP Pool screen displays the **Basic Settings** tab by default. Define the required parameters for the *Basic Settings*, *Static Bindings* and *Advanced* tabs to complete the creation of a DHCP pool.

7. Set the following **General** parameters. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

<b>DHCP Pool</b>	If adding a new pool, a name is required. The pool is the range of IP addresses defined for DHCP assignment or lease. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted. The name cannot exceed 32 characters.
<b>Subnet</b>	Define the IP address and Subnet Mask used for DHCP discovery and requests between the DHCP Server and DHCP clients. The IP address and subnet mask of the pool are required to match the addresses of the layer 3 interface for the addresses to be supported through that interface. Select <i>Alias</i> to use a network alias with the subnet configuration. For more information see <a href="#">Alias on page 7-34</a> . A numeric IP address is the default setting, not an alias.

<b>Domain Name</b>	Provide the domain name used with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. An FQDN consists of a hostname plus a domain name. For example, computername.domain.com. Select <i>Alias</i> to use a string alias with the domain name configuration. If setting a domain name alias, ensure it begins with a dollar sign (\$) and does not exceed 32 characters. For more information see <a href="#">Alias on page 7-34</a> . An actual domain name is the default setting, not an alias.
<b>DNS Servers</b>	Define one or a group of <i>Domain Name Servers</i> (DNS) to translate domain names to IP addresses. Select <i>Clear</i> to remove any single IP address as needed. Up to 8 IP addresses can be supported. Select <i>Alias</i> to use a host alias with the DNS servers configuration. If setting a DNS Server alias, ensure it begins with a dollar sign (\$) and does not exceed 32 characters. For more information see <a href="#">Alias on page 7-34</a> . An actual DNS IP address is the default setting, not an alias.
<b>Lease Time</b>	DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another DHCP supported client. Select this option to assign a lease time in either <i>Seconds</i> (1 - 31, 622, 399), <i>Minutes</i> (1 - 527,040), <i>Hours</i> (1 - 8,784) or <i>Days</i> (1 - 366). The default setting is enabled, with a lease time of 1 day.
<b>Default Routers</b>	After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address of one or a group of routers used to map hostnames into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported. Select <i>Alias</i> to use a host alias with the default routers configuration. For more information see <a href="#">Alias on page 7-34</a> . An actual router IP address is the default setting, not an alias.

- Use the **IP Address Ranges** and **Excluded IP Address Ranges** fields to define the range of included (starting and ending) IP addresses and excluded (starting and ending) IP addresses for this particular pool.

Refer to the IP Address Ranges field and select the **+ Add Row** button at the bottom of the field to add a new range. At any time you can select the radio button of an existing IP address range and select the **Delete** icon to remove it from the list of those available.

Enter a viable range of IP addresses in the **IP Start** and **IP End** columns. This is the range of addresses available for assignment to DHCP supported wireless clients within the network.

Select the **Create** icon or **Edit** icon within the **Class Policy** column to display the *DHCP Server Policy* screen if a class policy is not available from the drop-down menu.

Refer to the **Excluded IP Address Range** field and select the **+Add Row** button. Add ranges of IP address to exclude from lease to requesting DHCP clients. Having ranges of unavailable addresses is a good practice to ensure IP address resources are in reserve. Select the **Delete** icon as needed to remove an excluded address range.

- Select **OK** to save the updates to the **DHCP Pool Basic Settings** tab. Select **Reset** to revert to the last saved configuration.
- Select the **Static Bindings** tab from within the DHCP Pools screen.

A binding is a collection of configuration parameters, including an IP address, associated with, or *bound to*, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings provide the assignment of IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.



**Figure 9-11** Static Bindings Add screen

13. Define the following **General** parameters required to complete the creation of the static binding configuration. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

<b>Client Identifier Type</b>	Use the drop-down menu whether the DHCP client is using a <i>Hardware Address</i> or <i>Client Identifier</i> as its identifier type with a DHCP server.
<b>Value</b>	Provide a hardware address or client identifier value to help differentiate the client from other client identifiers.
<b>IP Address</b>	Set the IP address of the client using this host pool. Select <i>Alias</i> to use a network alias with the IP address configuration. For more information see <a href="#">Alias on page 7-34</a> .
<b>Domain Name</b>	Provide a domain name of the current interface. Domain names aren't case sensitive and can contain alphabetic or numeric letters or a hyphen. A <i>fully qualified domain name</i> (FQDN) consists of a hostname plus a domain name. For example, <i>computername.domain.com</i> . The Domain Name option is selected by default. Select <i>Alias</i> to use a string alias with the domain name configuration. For more information see <a href="#">Alias on page 7-34</a> .

<b>Boot File</b>	Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed. The IP option is selected by default. Optionally select <i>Alias</i> to provide a boot file IP alias beginning with a dollar sign (\$) and not exceeding 32 characters. For more information see <a href="#">Alias on page 7-34</a> .
<b>BOOTP Next Server</b>	Provide the numerical IP address of the server providing BOOTP resources. Select <i>Alias</i> to use a network alias with the BOOTP Next Server configuration. The IP option is selected by default. Optionally select <i>Alias</i> to provide a next BOOTP server IP alias beginning with a dollar sign (\$) and not exceeding 32 characters. For more information see <a href="#">Alias on page 7-34</a> .
<b>Client Name</b>	Provide the name of the client requesting DHCP Server support.
<b>Enable Unicast</b>	Unicast packets are sent from one location to another location (there is just one sender, and one receiver). Select this option to forward unicast messages to just a single device within this network pool. This setting is disabled by default.

14. Define the following **NetBIOS** parameters required to complete the creation of the static binding configuration:

<b>NetBIOS Node Type</b>	Set the NetBIOS Node Type used with this particular pool. The node can have one of the following types: <ul style="list-style-type: none"> <li>• <i>Broadcast</i> - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.</li> <li>• <i>Peer-to-Peer</i> - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.</li> <li>• <i>Mixed</i> - A mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address.</li> <li>• <i>Hybrid</i> - A combination of two or more nodes.</li> <li>• <i>Undefined</i> - No node type is applied.</li> </ul>
<b>NetBIOS Servers</b>	Specify a numerical IP address of a single or group of NetBIOS WINS servers available to DHCP supported wireless clients. A maximum of 8 server IP addresses can be assigned. Select <i>Alias</i> to use a network alias with the NetBIOS server configuration. Alias begins with a dollar sign (\$) and does not exceed 32 characters. For more information see <a href="#">Alias on page 7-34</a> .

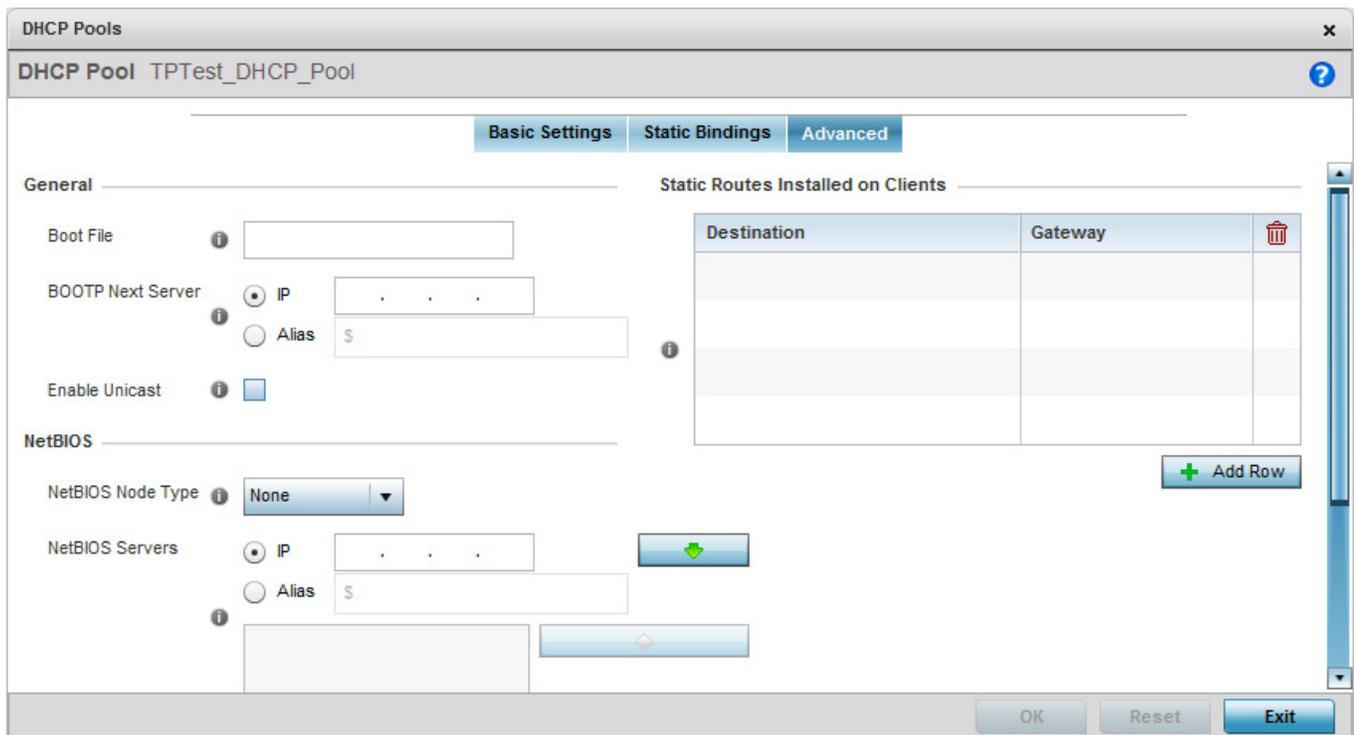
15. Refer to the **Static Routes Installed on Clients** field to set **Destination** IP and **Gateway** addresses enabling assignment of static IP addresses without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the space required in NVRAM to maintain address pools. Select the **+ Add Row** button to add individual destinations. Select the **Delete** icon to remove it from the list of those available.
16. Scroll down to the **DHCP Option Values** table to set Global DHCP options. A set of global DHCP options applies to all clients, whereas a set of subnet options applies only to the clients on a specified subnet. If you configure the same option in more than one set of options, the precedence of the option type decides which the DHCP server supports a client.
17. Select the **+ Add Row** button to add individual options. Assign each a **Global DHCP Option Name** to help differentiate it from others with similar configurations. At any time you can select the radio button of an existing option and select the **- Delete** button to remove it from the list of those available.
18. Assign a **Value** to each option with codes in the range of 1 through 254. A vendor specific option definition only applies to the vendor class for which it is defined.

19. Within the **Network** field, define one or group of **DNS Servers** to translate domain names to IP addresses. Up to 8 IP addresses can be provided and translated. Select **Alias** to use a network alias with the DNS server configuration. For more information see [Alias on page 7-34](#).

Within the **Network** field, define one or more **Default Routers** to resolve routes to other parts of the network. Up to 8 IP addresses can be provided for Default Routers. Select **Alias** to use a network alias with the default routers configuration. For more information see [Alias on page 7-34](#).

20. Select **OK** when completed to update the static bindings configuration. Select **Reset** to revert to the last saved configuration.

21. Select the **Advanced** tab to define additional NetBIOS and Dynamic DNS parameters.



**Figure 9-12** DHCP Pools screen - Advanced tab

22. The addition or edit of the network pool's advanced settings requires the following **General** parameters be set:

<b>Boot File</b>	Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each pool can use a different file as needed.
<b>BOOTP Next Server</b>	Provide the numerical IP address of the server providing BOOTP resources. The IP option is selected by default. Optionally select <i>Alias</i> to provide a next BOOTP server IP alias beginning with a dollar sign (\$) and not exceeding 32 characters. For more information see <a href="#">Alias on page 7-34</a> .
<b>Enable Unicast</b>	Unicast packets are sent from one location to another location (there's just one sender, and one receiver). Select this option to forward unicast messages to just a single device within the network pool. This setting is disabled by default.

23. Set the following **NetBIOS** parameters for the network pool:

<b>NetBIOS Node Type</b>	<p>Set the NetBIOS Node Type used with this pool. The following types are available:</p> <p>Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.</p> <ul style="list-style-type: none"> <li>• <i>Peer-to-Peer</i> - Uses directed calls to communicate with a known NetBIOS name server, such as a WINS server, for the IP address of a NetBIOS machine.</li> <li>• <i>Mixed</i> - Is a mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address.</li> <li>• <i>Hybrid</i> - Is a combination of two or more nodes.</li> <li>• <i>Undefined</i> - No NetBIOS Node Type is used.</li> </ul>
<b>NetBIOS Servers</b>	<p>Specify a numerical IP address of a single or group of NetBIOS WINS servers available to DHCP supported wireless clients. Select <i>Alias</i> to use a network alias with the NetBIOS server configuration. Alias begins with a dollar sign (\$) and does not exceed 32 characters. For more information see <a href="#">Alias on page 7-34</a>.</p>

24. Refer to the **DHCP Option Values** table to set global DHCP options applicable to all clients, whereas a set of subnet options applies to just the clients on a specified subnet.

Select the **+ Add Row** button to add individual options. Assign each a **Global DHCP Option Name** to help differentiate it from others with similar configurations. At any time you can select the radio button of an existing option and select the **Delete** icon to remove it from the list of those available.

Assign a **Value** to each option with codes in the range 1 through 254. A vendor-specific option definition only applies to the vendor class for which it's defined.

25. Refer to the **Static Routes Installed on Clients** table to set fixed routes for client destination and gateways.

26. Select the **+ Add Row** button to add individual options for **Destination** and **Gateway** addresses.

27. Select **OK** to save the updates to the DHCP pool's Advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

### 9.3.2 Defining DHCP Server Global Settings

#### ▶ [Setting the DHCP Server Configuration](#)

Setting a DHCP server global configuration entails defining whether BOOTP requests are ignored and setting DHCP global server options.

To define DHCP server global settings:

1. Select the **Global Settings** tab and ensure the **Activate DHCP Server Policy** button remains selected. This option must remain selected to implement the configuration as part of the access point profile.

**DHCP Server** ?

Activate DHCP Server Policy  i

**DHCP Pool** **Global Settings** **Class Policy**

**Configuration**

Ignore BOOTP Requests i

Ping Timeout i  seconds ( 1 to 10 )

**Activation Criteria**

Criteria i  v

VRRP Group i  ( 1 to 255 )

**Global DHCP Server Options**

Name	Type	Code	

+ Add Row

OK Reset

**Figure 9-13** DHCP Server Policy screen - Global Settings tab

2. Set the following parameters within the **Configuration** field:

<b>Ignore BOOTP Requests</b>	Select the check box to ignore BOOTP requests. BOOTP requests boot remote systems within the network. BOOTP messages are encapsulated inside UDP messages and are forwarded. This feature is disabled by default, so unless selected, BOOTP requests are forwarded.
<b>Ping Timeout</b>	Set an interval (from 1 -10 seconds) for the DHCP server ping timeout. The timeout is used to intermittently ping and discover whether a client requested IP address is already used.

3. Set the following **Activation Criteria** for the DHCP server policy:

<b>Criteria</b>	Select the <i>Criteria</i> option to invoke a drop-down menu to determine when the DHCP daemon is invoked. Options include <i>vrrp-master</i> , <i>cluster-master</i> , and <i>rf-domain-manager</i> . A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router.
<b>VRRP Group</b>	Set the VRRP group ID from 1-255. VRRP Group is only enabled when the criteria is set to <i>vrrp-master</i> . The default setting is group 1.

4. Refer to the **Global DHCP Server Options** field.

Use the **+ Add Row** button at the bottom of the field to add a new global DHCP server option. At any time you can select the radio button of an existing global DHCP server option and select the **Delete** icon to remove it from the list of those available.

Use the **Type** drop-down menu to specify whether the DHCP option is being defined as a numerical IP address or ASCII string or Hex string. Highlight an entry from within the Global Options screen and click the Remove button to delete the name and value.

5. Select **OK** to save the updates to the DHCP server global settings. Select **Reset** to revert to the last saved configuration.

### 9.3.3 DHCP Class Policy Configuration

#### ▶ *Setting the DHCP Server Configuration*

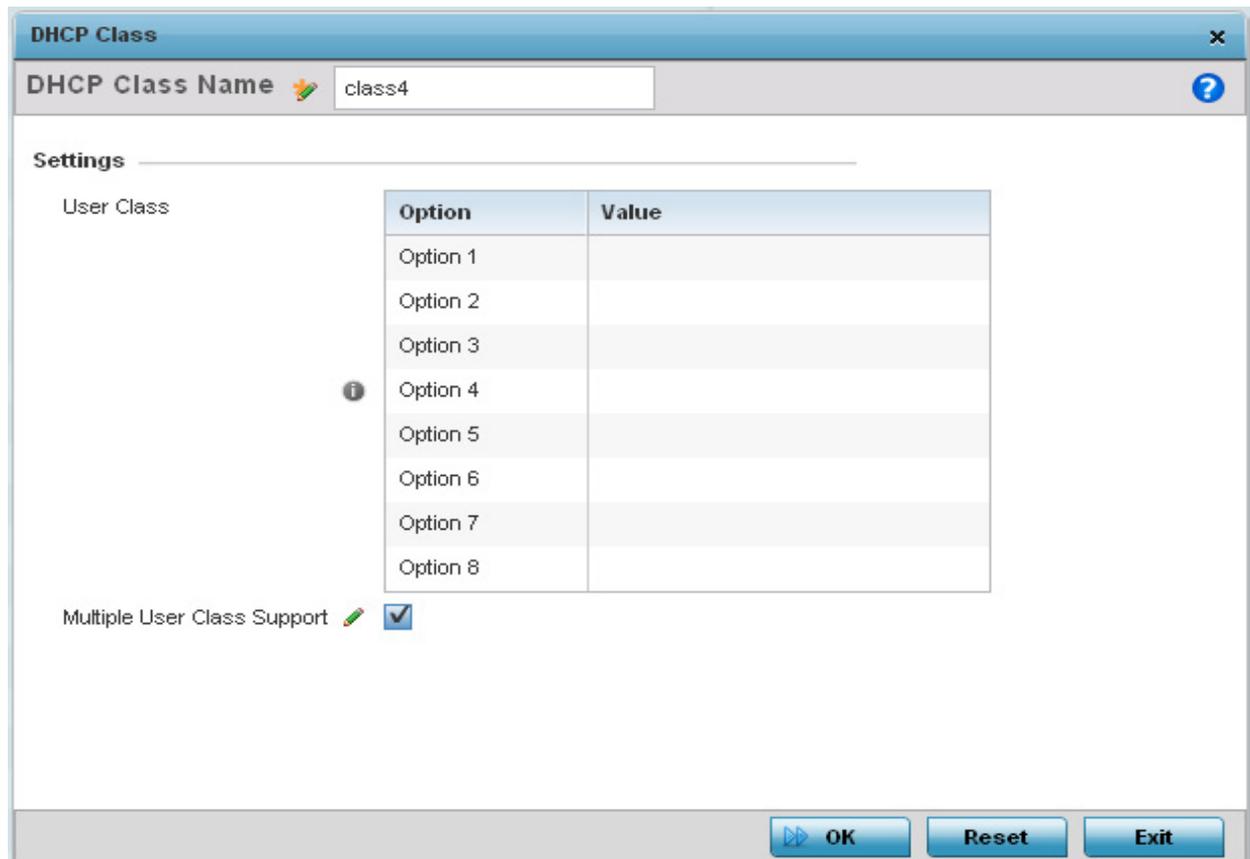
The DHCP server assigns IP addresses to DHCP enabled wireless clients based on user class option names. Clients with a defined set of user class option names are identified by their user class name. The DHCP server can assign IP addresses from as many IP address ranges as defined by the administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

Refer to the **DHCP Class Policy** screen to review existing DHCP class names and their current multiple user class designations. Multiple user class options enable a user class to transmit multiple option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

To review DHCP class policies:

1. Select the **Class Policy** tab and ensure the **Activate DHCP Server Policy** button remains selected. This option must remain selected to implement the configuration as part of the access point profile.





**Figure 9-15** DHCP Class - Name Add screen

3. If adding a new **DHCP Class Name**, assign a name representative of the device class supported. The DHCP user class name should not exceed 32 characters.
4. Select a row within the **Value** column to enter a 32 character maximum value string.
5. Select the **Multiple User Class** radio button to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.
6. Select **OK** to save the updates to this DHCP class policy. Select **Reset** to revert to the last saved configuration.

## 9.4 Setting the Bonjour Gateway Configuration

### ► *Security Configuration*

Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a local area network (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.



**NOTE:** Upto eight (8) Bonjour Discovery Policies can be configured.

---

---

The following options can be configured:

- [Configuring the Bonjour Discovery Policy](#)
- [Configuring the Bonjour Forwarding Policy](#)

### 9.4.1 Configuring the Bonjour Discovery Policy

#### ► *Setting the Bonjour Gateway Configuration*

The Bonjour Discovery Policy configures how Bonjour services can be located. It configures the VLANs on which these services can be found.

To display Bonjour Discovery Policy information:

1. Select **Configuration**.
2. Select **Services**.
3. Select **Bonjour Gateway** to expand its submenu.
4. Select **Discovery Policy**. The following screen displays:

The screenshot shows a window titled "Discovery Policy" with a search bar and a table. The table has one row with the name "Test". Below the table is a search input field and a "Row Count: 1" indicator. At the bottom are buttons for "Add", "Edit", "Delete", "Copy", and "Rename".

Name
Test

**Figure 9-16** Bonjour - Discovery Policy screen

This screen displays the name of the configured Bonjour discovery policies.

5. Select an existing policy and click **Edit** to edit it. To add a new policy, select **Add**.

The screenshot shows a window titled "Name Test" with a "Rules" section. It contains a table with three columns: "Service Name", "VLAN Type", and "Service VLANs". The first row is pre-filled with "Predefined", a dropdown menu, "Alias", a text field with "\$", a dropdown menu with an asterisk, and a text field with "(\$2a xz,4,7-12,...)". There are "Add Row", "OK", "Reset", and "Exit" buttons at the bottom.

Service Name	VLAN Type	Service VLANs
<input checked="" type="radio"/> Predefined <input type="radio"/> Alias \$	*	(\$2a xz,4,7-12,...)

**Figure 9-17** Bonjour - Discovery Policy - Add/Edit Policy screen

6. Select the **+ Add Row** button to add a rule to the Bonjour Discovery Policy. These are the services which can be discovered by the Bonjour Gateway.

Refer to the following for more information on the discovery rules.

<b>Service Name</b>	Configures the service that can be discovered by the Bonjour Gateway. <ul style="list-style-type: none"> <li>• <i>Predefined</i> – Use the drop-down menu to select from a list of predefined Apple services.</li> <li>• <i>Alias</i> – Use an existing alias to define a service that is not available in the predefined list.</li> </ul>
<b>VLAN Type</b>	Use the drop-down menu to select the VLAN type. <ul style="list-style-type: none"> <li>• <i>local</i> – Indicates that the VLAN(s) defined in <i>Service VLAN</i> field is local in nature.</li> <li>• <i>tunneled</i> – Indicates that the VLAN(s) defined in <i>Service VLAN</i> field are tunneled.</li> </ul>
<b>Service VLANs</b>	Provide a VLAN or a list of VLANs on which the selected service is discoverable.

7. Select **OK** to save the updates to this Bonjour Discovery Policy. Select **Reset** to revert to the last saved configuration.

## 9.4.2 Configuring the Bonjour Forwarding Policy

### ▶ *Setting the Bonjour Gateway Configuration*

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.



**NOTE:** Only one (1) Bonjour Forwarding Policy can be configured.



**NOTE:** There must be Layer 2 connectivity between the devices for forwarding to work.

To display Bonjour Discovery Policy information:

1. Select **Configuration**.
2. Select **Services**.
3. Select **Bonjour Gateway** to expand its submenu.
4. Select **Forwarding Policy**. The following screen displays:

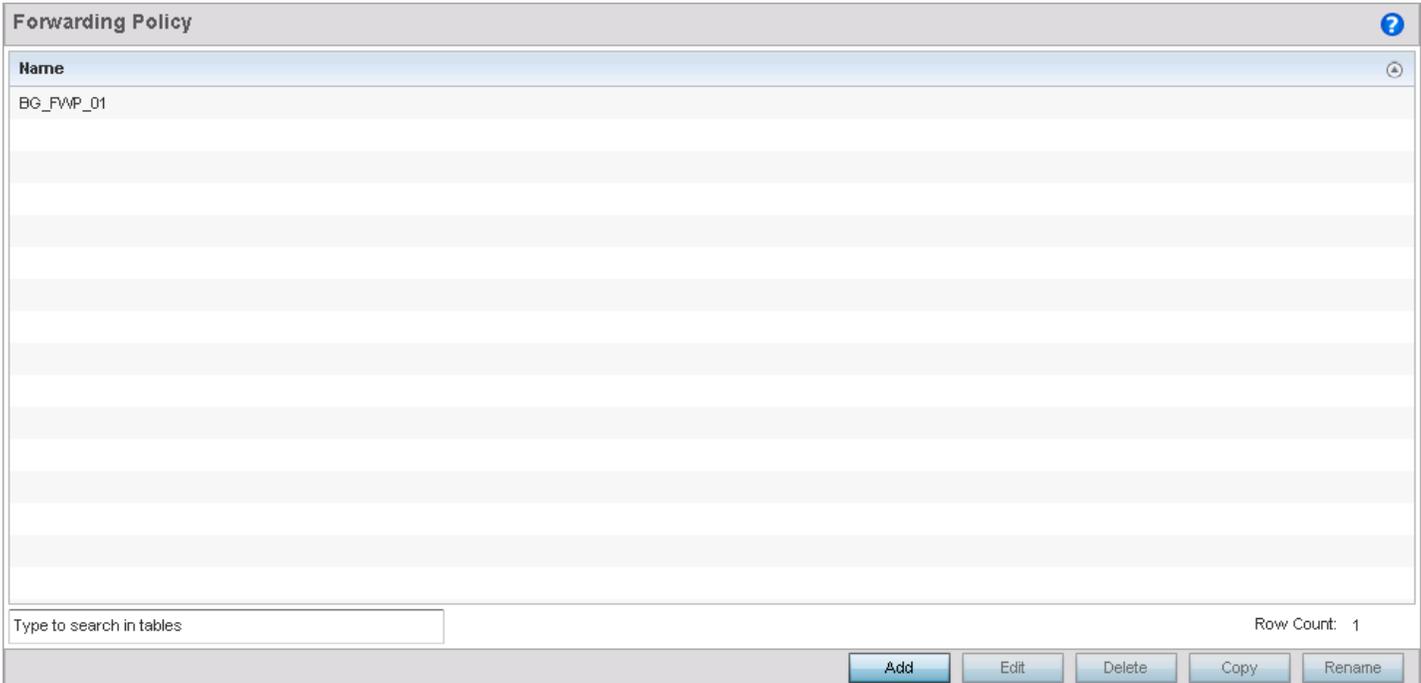


Figure 9-18 Bonjour Gateway - Forwarding Policy screen

This screen displays the name of the configured Bonjour forwarding policies.

- 5. Select an existing policy and click **Edit** to edit it. To add a new policy, select **Add**.

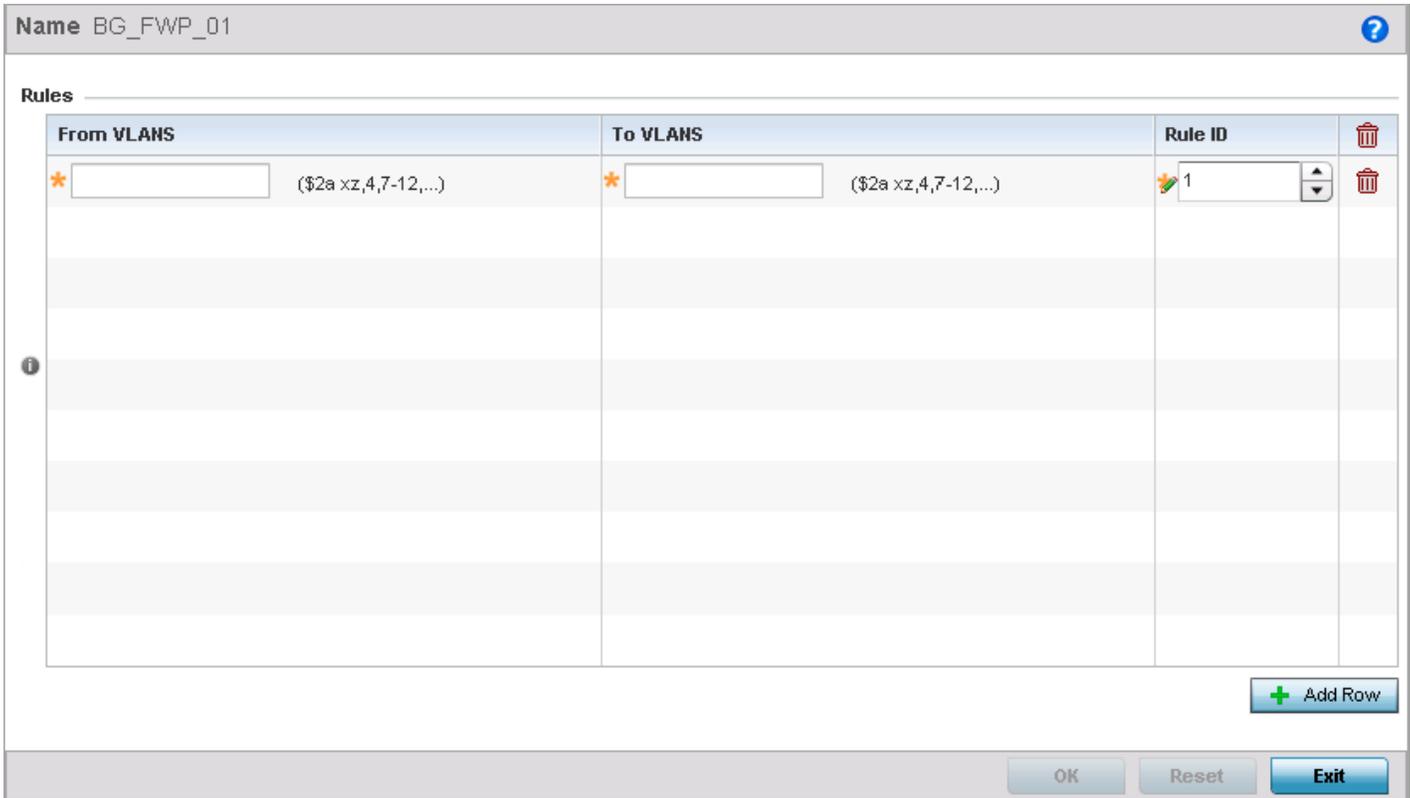


Figure 9-19 Bonjour Gateway - Forwarding Policy - Add screen

6. Select the **+ Add Row** button to add a forwarding rule to the Bonjour Forwarding Policy. Advertisements from VLANs that contain services are forwarded to VLANs containing clients.

<b>From VLANs</b>	<i>From VLANs</i> are VLANs where the Apple services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
<b>To VLANs</b>	<i>To VLANs</i> are VLANs where clients for the services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
<b>Rule ID</b>	Use the spinner to set a unique rule ID for this rule.

7. Select **OK** to save the updates to this DHCP class policy. Select **Reset** to revert to the last saved configuration.
-

## 9.5 Setting the RADIUS Configuration

### ► [Security Configuration](#)

*Remote Authentication Dial-In User Service* (RADIUS) is a client/server protocol and software enabling remote access servers to authenticate users and authorize their access to the access point managed network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the access point's RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to a RADIUS supported access point, the access point sends the authentication request to the RADIUS server. The authentication and encryption of communications between the access point and server takes place through the use of a shared secret password (not transmitted over the network).

The access point's local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assign policies for the group authorization.

AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX model access points have an internal RADIUS server resource. However, AP6511 and AP6521 models do not have an onboard RADIUS server resource and an external resource must be used.

The access point allows the enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. The access point uses a default trustpoint. A certificate is required for EAP TTLS, PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

To view RADIUS configurations:

1. Select **Configuration** tab from the web user interface.
2. Select **Services**.
3. Select the **RADIUS** option. The RADIUS Group screen displays (by default).

For information on creating the groups, user pools and server policies needed to validate user credentials against a server policy configuration, refer to the following:

- [Creating RADIUS Groups](#)
- [Defining User Pools](#)
- [Configuring the RADIUS Server](#)

### 9.5.1 Creating RADIUS Groups

#### ► [Setting the RADIUS Configuration](#)

The access point's RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the access point's local database. The user ID in the received access request is mapped to the associated wireless group for authentication. Group configurations allow the enforcement of the following policies controlling user access:

- *The assignment of a VLAN to the user upon successful authentication*
- *The creation of a start and end of time in (HH:MM) when a user is allowed to authenticate*
- *The creation of a list of SSIDs to which a user belonging to this group is allowed to associate*
- *The ability to set the days of the week a user is allowed to login*



<b>Role</b>	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: <ul style="list-style-type: none"> <li>• <i>monitor</i> - Read-only access</li> <li>• <i>helpdesk</i> - Helpdesk/support access</li> <li>• <i>network-admin</i> - Wired and wireless access</li> <li>• <i>security-admin</i> - Grants full read/write access</li> <li>• <i>system-admin</i> - System administrator access</li> </ul>
<b>VLAN</b>	Displays the VLAN ID used by the group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the access point managed network (once authenticated by the local RADIUS server).
<b>Time Start</b>	Specifies the time users within each listed group can access local RADIUS resources.
<b>Time Stop</b>	Specifies the time users within each listed group lose access to local RADIUS resources.

5. Select **Add** to create a new group. To modify the settings of an existing group, select the group and click the **Edit** button. To delete an obsolete group, select the group and click the **Delete** button.

### 9.5.1.1 Creating RADIUS Groups

#### ► Creating RADIUS Groups

To create a RADIUS group:

1. Select **Configuration** tab from the web user interface.
2. Select **Services**.
3. Select and expand the **RADIUS** menu. Select **Groups** if the RADIUS Group screen is not already displayed by default.
4. Select **Add** to create a new RADIUS group, **Edit** to modify the configuration of an existing group or **Delete** to permanently remove a selected group.

**Figure 9-21** RADIUS Group Policy Add screen

5. Define the following **Settings** to define the user group configuration:

<b>RADIUS Group Policy</b>	If creating a new RADIUS group, assign it a name to help differentiate it from others with similar configurations. The name cannot exceed 32 characters or be modified as part of a RADIUS group edit process.
<b>Guest User Group</b>	Select this option to assign only guest access and temporary permissions to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions. This setting is disabled by default.

<b>VLAN</b>	Select this option (and use the slider) to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (Single VLAN) is enabled for the WLAN for the VLAN to work properly. For more information, see <a href="#">Basic WLAN Configuration on page 6-5</a> .
<b>WLAN SSID</b>	Assign a list of SSIDs (users) the RADIUS group are allowed to associate to. An SSID cannot exceed 32 characters. Assign WLAN SSIDs representative of users a guest user will need to access. The parameter is not available if this RADIUS group has been defined as a management group.
<b>Rate Limit from Air</b>	Select the check box to set an uplink rate limit for managed clients within this RADIUS group. Use the spinner to set value from 100 - 1,000,000 kbps. Setting a value of 0 disables rate limiting.
<b>Rate Limit to Air</b>	Select the check box to set a downlink rate limit from clients within this RADIUS group. Use the spinner to set value from 100 - 1,000,000 kbps. Setting a value of 0 disables rate limiting.
<b>Management Group</b>	Select this option to designate the RADIUS group as a management group. If set as management group, assign a role to the members of the group using the Access drop-down menu, allowing varying levels of administrative rights. This feature is disabled by default.
<b>Access</b>	If a group is listed as a management group, assign how the devices can be accessed. Available access types are: <ul style="list-style-type: none"> <li>• <i>Web</i> - Web access through browser is permitted</li> <li>• <i>SSH</i> - SSH access through command line is permitted</li> <li>• <i>Telnet</i> - Telnet access through command line is permitted</li> <li>• <i>Console</i> - Console access to the device is permitted</li> </ul>
<b>Role</b>	If a group is listed as a management group, assign a unique role. Available roles include: <ul style="list-style-type: none"> <li>• <i>monitor</i> - Read-only access</li> <li>• <i>helpdesk</i> - Helpdesk/support access</li> <li>• <i>network-admin</i> - Wired and wireless access</li> <li>• <i>security-admin</i> - Grants full read/write access</li> <li>• <i>system-admin</i> - System administrator access</li> </ul>

6. Set the **Schedule** to configure access times and dates. Select **Restrict Access By Time** control to enable time based access.

<b>Time Start</b>	Use the spinner control to set the time (in HH:MM format) RADIUS group members are allowed to login and access RADIUS server resources (for example, 14:45 = 2:45). Select either the <i>AM</i> or <i>PM</i> radio button to set the time as morning or evening.
<b>Time Stop</b>	Use the spinner control to set the time (in HH:MM format) RADIUS group members are denied access to RADIUS server resources (for example, 15:45 = 3:45). Select either the <i>AM</i> or <i>PM</i> radio button to set the time as morning or evening. If already logged in, the RADIUS group user is deauthenticated from the WLAN.

7. Select **Restrict Access By Day Of Week** control to enable access based on the day of the week.

<b>Days</b>	Select the day(s) of the week RADIUS group members can access RADIUS resources.
-------------	---

- Click the **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

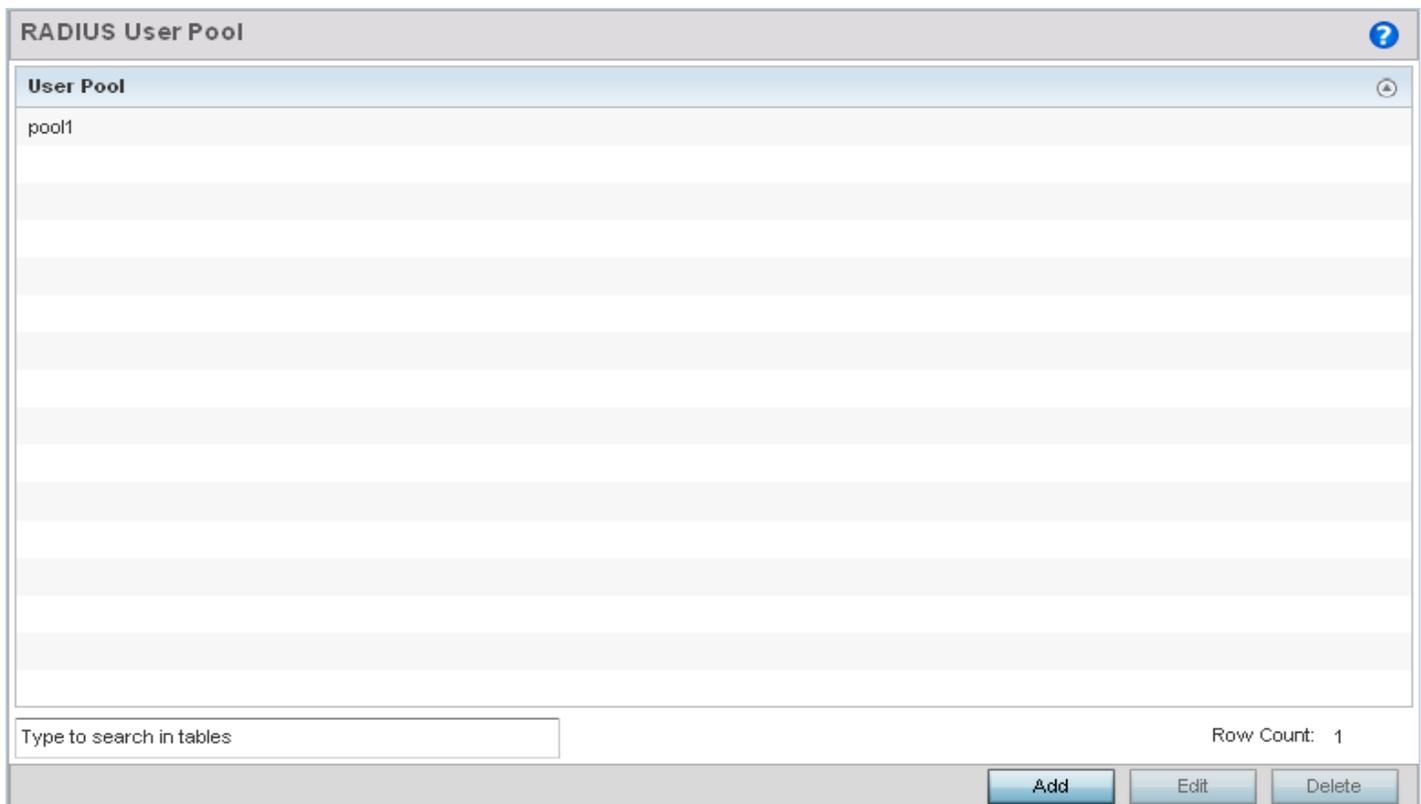
## 9.5.2 Defining User Pools

### ▶ *Setting the RADIUS Configuration*

A user pool defines policies for individual user access to the access point's internal RADIUS resources. User or pools provide a convenient means of providing user access to RADIUS resources based on the pool's unique permissions (either temporary or permanent). A pool can contain a single user or group of users.

To configure a RADIUS user pool and unique user IDs:

- Select **Configuration** tab from the web user interface.
- Select **Services**.
- Expand the **RADIUS** menu option and select **User Pools**.



**Figure 9-22** RADIUS User Pool screen

- Select **Add** to create a new user pool, **Edit** to modify the configuration of an existing pool or **Delete** to remove a selected pool.
- If creating a new pool, assign it a name up to 32 characters and select **Continue**.  
The name should be representative of the users comprising the pool and/or the temporary or permanent access privileges assigned.



<b>Expiry Time</b>	Lists the time the listed user Id losses access internal RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.
--------------------	--

7. Select the **Add** button to add a new RADIUS user, **Edit** to modify the configuration of an existing user or **Delete** to remove an existing user Id.

**Figure 9-24** RADIUS - Add User screen

8. Set the following to create a new RADIUS user with unique access privileges:

<b>User Id</b>	Assign a unique alphanumeric string identifying this user. The ID cannot exceed 64 characters.
<b>Password</b>	Provide a password unique to this user. The password cannot exceed 32 characters. Select the Show check box to expose the password's actual character string. Leaving the option unselected displays the password as a string of asterisks (*).
<b>Guest User</b>	Select the check box to designate this user as a guest with temporary access. The guest user must be assigned unique access times to restrict their access.
<b>Group</b>	If the user has been defined as a guest, use the Group drop-down menu to assign the user a group with temporary access privileges. If the user is defined as a permanent user, select a group from the group list. If there's no groups listed relevant to the user's intended access, select the Create icon and create a new group configuration suitable for the user membership. For more information, see <a href="#">Creating RADIUS Groups on page 9-36</a> .
<b>Email Id</b>	Set the E-mail ID for this user.

<b>Telephone</b>	Configure the telephone number for this user.
------------------	---

9. Set the following **Time** settings for the new user:

<b>Start Date</b>	Configure the <i>month, day</i> and <i>year</i> the listed user can access the access point's internal RADIUS server resources.
<b>Start Time</b>	Configure the time the listed user can access the internal RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.
<b>Expiry Date</b>	Configure the month, day and year the listed user can no longer access the internal RADIUS server.
<b>Expiry Time</b>	Configure the time the listed user losses access internal RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.

10. Select **OK** to save the user group membership configuration. Select **Reset** to revert to the last saved configuration.

### 9.5.3 Configuring the RADIUS Server

#### ▶ *Setting the RADIUS Configuration*

A RADIUS server policy is a unique authentication and authorization configuration for receiving user connection requests, authenticating users and returning the configuration information necessary for the RADIUS client to deliver service to the user. An access point's requesting client is the entity with authentication information requiring validation. The access point's local RADIUS server has access to a database of authentication information used to validate client authentication requests.

The RADIUS server ensures the information is correct using authentication schemes like PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information. The access point's RADIUS server policy can also be configured to refer to an external LDAP resource to verify the user's credentials. The creation and utilization of a single RADIUS server policy is supported.

To manage the access point's RADIUS server policy:

1. Select **Configuration** tab from the web user interface.
2. Select **Services**.
3. Expand the **RADIUS** menu option and select **RADIUS Server**.

**RADIUS Server** ?

Activate RADIUS Server Policy  i

Server Policy
Client
Proxy
LDAP

**Settings**

RADIUS User Pools
 


i
Create

LDAP Server Dead Period i


( 0 to 10 )

LDAP Groups
 

+
⚙️
↓

i

↑

LDAP Group Verification i

LDAP Chase Referral i

Local Realm
 

↓

i

↑

**Authentication**

Default Source i
 Local  LDAP

Default Fallback i

Source	FallBack	SSID	Precedence	
				🗑️

Sources i
+ Add Row

Authentication Type i

Enable CRL Validation i

**LDAP Agent**

Username	Password	Retry Timeout	Redundancy	Domain Name	
					🗑️

**Session Resumption / Fast Reauthentication**

Enable Session Resumption i

Cached Entry Lifetime i



(1 to 24 hours)

Maximum Cache Entries i



(10 to 1,024)

▶ OK
Reset

**Figure 9-25** RADIUS Server Policy screen - Server Policy tab

The **RADIUS Server Policy** screen displays with the **Server Policy** tab displayed by default.

4. Select the **Activate RADIUS Server Policy** button to enable the parameters within the screen for configuration. Ensure this option remains selected, or this RADIUS server configuration is not applied to the access point profile.

5. Define the following **Settings** required in the creation or modification of the server policy:

<b>RADIUS User Pools</b>	Select the user pools to apply to this server policy. Up to 32 can be applied. If a pool requires creation, select the Create link. For more information, see <a href="#">Defining User Pools on page 9-38</a> .
<b>LDAP Server Dead Period</b>	Set an interval in either <i>Seconds</i> (0 - 600) or <i>Minutes</i> (0- 10) during which the access point will not contact its LDAP server resource. A dead period is only implemented when additional LDAP servers are configured and available.
<b>LDAP Groups</b>	Use the drop-down menu to select LDAP groups to apply the server policy configuration. Select the <i>Create</i> or <i>Edit</i> icons as needed to either create a new group or modify an existing group. Use the arrow icons to add and remove groups as required.
<b>LDAP Group Verification</b>	Select the check box to set the LDAP group search configuration. This setting is enabled by default.
<b>LDAP Chase Referral</b>	Select the check box to set the LDAP referral chase feature. This settings is enabled by default. When enabled, if the LDAP server does not contain the requested information, it indicates to the LDAP client that it does not have the requested information and provides the client with another LDAP server that could have the requested information. It is up to the client to contact the other LDAP server for its information.
<b>Local Realm</b>	Define the LDAP Realm performing authentication using information from an LDAP server. User information includes <i>user name</i> , <i>password</i> , and the <i>groups</i> to which the user belongs.

6. Set the following **Authentication** parameters to define server policy authorization settings.

<b>Default Source</b>	Select the RADIUS resource for user authentication with this server policy. Options include Local for the local user database or LDAP for a remote LDAP resource. The default setting is Local
<b>Default FallBack</b>	Select this option to indicate that fall back from RADIUS to local is enabled incase RADIUS authentication is not available for any reason. This option is only enabled when <i>LDAP</i> is selected as the <i>Default Source</i> . Use the <i>Add Row</i> button to add fallback sources into the <i>Sources</i> table. Provide the following information: <ul style="list-style-type: none"> <li>• <i>Source</i> – Select the type of fallback. Select from <i>LDAP</i> or <i>Local</i></li> <li>• <i>Fallback</i> – Select to enable fallback on this record.</li> <li>• <i>SSID</i> – Enter the SSID to fall back on.</li> <li>• <i>Precedence</i> – Use the spinner to select the precedence for selection of fallback.</li> </ul>

<b>Authentication Type</b>	<p>Use the drop-down menu to select the EAP authentication scheme for local and LDAP authentication. The following EAP authentication types are supported:</p> <ul style="list-style-type: none"> <li>• <i>All</i> – Enables all authentication schemes.</li> <li>• <i>TLS</i> - Uses TLS as the EAP type</li> <li>• <i>TTLS and MD5</i> - The EAP type is TTLS, with default authentication using MD5.</li> <li>• <i>TTLS and PAP</i> - The EAP type is TTLS, with default authentication using PAP.</li> <li>• <i>TTLS and MSCHAPv2</i> - The EAP type is TTLS, with default authentication using MSCHAPv2.</li> <li>• <i>PEAP and GTC</i> - The EAP type is PEAP, with default authentication using GTC.</li> <li>• <i>PEAP and MSCHAPv2</i> - The EAP type is PEAP with default authentication using MSCHAPv2. However, when user credentials are stored on an LDAP server, the RADIUS server cannot conduct PEAP-MSCHAPv2 authentication on its own, as it is not aware of the password. Use LDAP agent settings to locally authenticate the user. Additionally, an authentication utility (such as Samba) must be used to authenticate the user. Samba is an open source software used to share services between Windows and Linux machine.</li> </ul>
<b>Do Not Verify Username</b>	Only enabled when <i>TLS</i> is selected in <i>Authentication Type</i> . When selected, user name is not matched but the certificate expiry is checked.
<b>Enable CRL Validation</b>	Select this option to enable a <i>Certificate Revocation List</i> (CRL) check. Certificates can be checked and revoked for a number of reasons, including the failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. This option is disabled by default.

7. If using LDAP as the default authentication source, select **+ Add Row** to set LDAP Agent settings.

When a user's credentials are stored on an external LDAP server, the controller or service platform's local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource using credentials maintained locally.

<b>Username</b>	Enter a 128 character maximum username for the LDAP server's domain administrator. This is the username defined on the LDAP server for RADIUS authentication requests.
<b>Password</b>	Enter and confirm the 32 character maximum password (for the username provided above). The successful verification of the password maintained on the controller or service platform enables PEAP-MSCHAPv2 authentication using the remote LDAP server resource.
<b>Retry Timeout</b>	Set the number of <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) to wait between LDAP server access requests when attempting to join the remote LDAP server's domain. The default settings is one minute.
<b>Redundancy</b>	Define the <i>Primary</i> or <i>Secondary</i> LDAP agent configuration used to connect to the LDAP server domain.
<b>Domain Name</b>	Enter the name of the domain (from 1 - 127 characters) to which the LDAP server resource belongs.

8. Set the following **Session Resumption/Fast Reauthentication** settings to define how server policy sessions are re-established once terminated and require cached data to resume:

<b>Enable Session Resumption</b>	Select the check box to control volume and the duration cached data is maintained by the server policy upon the termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption. This setting is disabled by default.
<b>Cached Entry Lifetime</b>	Use the spinner control to set the lifetime (1 - 24 hours) cached data is maintained by the RADIUS server policy. The default setting is 1 hour.
<b>Maximum Cache Entries</b>	Use the spinner control to define the maximum number of entries maintained in cache for this RADIUS server policy. The default setting is 128 entries.

9. Select **OK** to save the settings to the server policy configuration. Select **Reset** to revert to the last saved configuration.
10. Select the **Client** tab and ensure the **Activate RADIUS Server Policy** button remains selected.

The access point uses a RADIUS client as a mechanism to communicate with a central server to authenticate users and authorize access.

The client and server share a *secret* (a password). That shared secret followed by the request authenticator is put through a MD5 hash to create a 16 octet value used with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS *access request* packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified *access accept* packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified *access reject* message, the username and password are considered incorrect, and the user is not authenticated.

**RADIUS Server** ?

Activate RADIUS Server Policy  i

Server Policy
Client
Proxy
LDAP

**RADIUS Clients**

IP Address	Shared Secret	
* 157. 235. 112. 11 / 25	* ***** <input type="checkbox"/> Show	<input type="button" value="🗑️"/> <input type="button" value="🗑️"/>

**Figure 9-26** RADIUS Server Policy screen - Client tab

11. Select the **+ Add Row** button to add a table entry for a new client's IP address, mask and shared secret. To delete a client entry, select the **Delete** icon on the right-hand side of the table entry.
12. Specify the **IP Address** and mask of the RADIUS client authenticating with the RADIUS server.
13. Specify a **Shared Secret** for authenticating the RADIUS client.
14. Shared secrets verify RADIUS messages with a RADIUS enabled device configured with the same shared secret. Select the **Show** check box to expose the shared secret's actual character string. Leave the option unselected to display the shared secret as a string of asterisks (\*).
15. Select **OK** to save the server policy's client configuration. Select the **Reset** button to revert to the last saved configuration.
16. Select the **Proxy** tab and ensure the **Activate RADIUS Server Policy** button remains selected.

A user's access request is sent to a proxy server if it cannot be authenticated by local RADIUS resources. The proxy server checks the information in the user access request, and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to the NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the access point's RADIUS server receives a request for a user name containing a realm, the server references a table of configured realms. If the realm is known, the server proxies the request to the RADIUS server. The behavior of the proxying server is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove or rewrite requests when they are proxied.

**RADIUS Server** ?

Activate RADIUS Server Policy  i

Server Policy
Client
Proxy
LDAP

**Proxy Retries**

Proxy Retry Delay i  seconds ( 5 to 10 )

Proxy Retry Count i  (3 to 6)

**Realms**

Realm Name	IP Address	Port Number	Shared Secret	
* <input style="width: 100%;" type="text" value="percival"/>	* <input style="width: 100%;" type="text" value="157. 235. 111. 22"/>	<span style="font-size: small;">i</span> <input style="width: 60px;" type="text" value="1812"/>	* <input style="width: 100%;" type="text" value="*****"/> <input type="checkbox"/> Show <span style="float: right;">i</span>	

+ Add Row

OK
Reset

**Figure 9-27** RADIUS Server Policy screen - Proxy tab

17. Enter the **Proxy Retry Delay** as a value in seconds (from 5 - 10 seconds). This is the interval the RADIUS server waits before making an additional connection attempt. The default delay interval is 5 seconds.
18. Enter the **Proxy Retry Count** field as a value from 3 - 6. This is the number of retries sent to the proxy server before giving up the request. The default retry count is 3 attempts.
19. Select the **+ Add Row** button to add a RADIUS server proxy realm name and network address. To delete a proxy server entry, select the **Delete** icon on the right-hand side of the table.
20. Enter a 50 character maximum **Realm Name**. When the access point's RADIUS server receives a request for a user name, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.
21. Enter the Proxy server's **IP Address**. This is the address of server checking the information in the user access request. The proxy server either accepts or rejects the request on behalf of the RADIUS server.
22. Enter the TCP/IP **Port Number** for the server that acts as a data source for the proxy server. Use the spinner to select a value from 1024 - 65535. The default port is 1812.
23. Enter the RADIUS client's **Shared Secret** for authenticating the RADIUS proxy.
24. Select the **Show** check box to expose the shared secret's actual character string. Leave the option unselected to display the shared secret as a string of asterisks (\*).
25. Select the **OK** button to save the changes. Select the **Reset** button to revert to the last saved configuration.
26. Select the **LDAP** and ensure the **Activate RADIUS Server Policy** button remains selected.

Administrators have the option of using the access point's RADIUS server to authenticate users against an external LDAP server resource. An external LDAP user database allows the centralization of user information and reduces administrative user management overhead. Thus, making the RADIUS authorization process more secure and efficient.

RADIUS is not just a database. It's a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location. It's the access point's RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. There's no way to perform such complex authorization checks from a LDAP user database alone.



**Figure 9-29** LDAP Server Add screen

29. Set the following **Network** address information required for the connection to the external LDAP server resource:

<b>Redundancy</b>	Define whether this LDAP server is a primary or secondary server resource. Primary servers are always queried for the first connection attempt. However, designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server were to become unavailable.
<b>IP Address</b>	Set the IP address of the external LDAP server acting as the data source for the RADIUS server.
<b>Login</b>	Define a unique login name used for accessing the remote LDAP server resource. Consider using a unique login name for each LDAP server to increase the security of the connection between the access point and remote LDAP resource.
<b>Port</b>	Use the spinner control to set the physical port used by the RADIUS server to secure a connection with the remote LDAP server resource. The default port is 389.
<b>Timeout</b>	Set an interval between 1 - 10 seconds the RADIUS server uses as a wait period for a response from the target primary or secondary LDAP server resource. The default setting is 10 seconds.

30. Set the following **Network** information for the connection to the external LDAP server resource:

<b>Bind DN</b>	Specify the <i>distinguished name</i> to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas.
----------------	--

<b>Base DN</b>	Specify a <i>distinguished name</i> (DN) that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with the most specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the <i>Relative Distinguished Name</i> (RDN). The RDN identifies an entry distinctly from any other entries that have the same parent.
<b>Bind Password</b>	Enter a valid password for the LDAP server. Select the <i>Show</i> check box to expose the password's actual character string. Leave the option unselected to display the password as a string of asterisks (*). The password cannot 32 characters.
<b>Password Attribute</b>	Enter the LDAP server password attribute. The password cannot exceed 64 characters.

31. Set the following **Attributes** for LDAP groups to optimally refine group queries:

<b>Group Attribute</b>	LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group, an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.
<b>Group Filter</b>	Specify the group filters used by the LDAP server. The group filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
<b>Group Membership Attribute</b>	Specify the group member attribute sent to the LDAP server when authenticating users.

32. Select the **OK** button to save the changes to the LDAP server configuration. Select **Reset** to revert to the last saved configuration.

## 9.6 Services Deployment Considerations

### ► *Security Configuration*

Before defining the access point's configuration using the Services menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends each RADIUS client use a different shared secret password. If a shared secret is compromised, only the one client poses a risk as opposed all the additional clients that potentially share that secret password.
  - Consider using an LDAP server as a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location.
  - Designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server were to become unavailable.
-



# CHAPTER 10

## SECURITY CONFIGURATION

The access point uses mechanisms to allow/deny access to the network for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for unique policies. Management Access is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Motorola Solutions recommends disabling unused and insecure management interfaces as required within different access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources too.



**NOTE:** The access point utilizes a single Management Access policy, so ensure all the intended administrative roles, access control permissions, authentication settings and SNMP settings are correctly set. If the access point is a Virtual Controller AP, these are the management settings used by adopted access points.

---

---

To set Management Access administrative rights, access control permissions, authentication refer to the following:

- [Creating Administrators and Roles](#)
- [Setting the Access Control Configuration](#)
- [Setting the Authentication Configuration](#)
- [Setting the SNMP Configuration](#)
- [SNMP Trap Configuration](#)

Refer to [Management Access Deployment Considerations on page 10-13](#) for tips on how to optimize the access point's management access configuration.



**Figure 10-2** Administrators screen

- If adding a new administrator, enter the name in the **User Name** field. This is a mandatory field, and cannot exceed 32 characters. Optimally assign a name representative of the user's intended access type and role.
- Provide a strong administrator password. Once provided, **Reconfirm** the password to ensure its accuracy. This is also a mandatory field.
- Define protocol **Access** for the user's unique permissions. If required, all four options can be selected and invoked simultaneously.

<b>Web UI</b>	Select this option to enable access to the access point's Web UI.
<b>Telnet</b>	Select this option to enable access to the access point using TELNET.
<b>SSH</b>	Select this option to enable access to the access point using SSH.
<b>Console</b>	Select this option to enable access to the access point's console.

- Select an **Administrator Role**. Only one role can be assigned.

<b>Superuser</b>	Select this option to assign complete administrative rights to this user. This entails all the roles listed.
<b>System</b>	Select this option to allow the administrator to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
<b>Network</b>	Select this option to allow the user to configure all wired and wireless parameters (IP configuration, VLANs, L2/L3 security, WLANs, radios etc).

<b>Security</b>	Select this option to set the administrative rights for a security administrator allowing the configuration of all security parameters.
<b>Monitor</b>	Select this option to assign permissions without administrative rights. The Monitor option provides read-only permissions.
<b>Help Desk</b>	Assign this option to someone who typically troubleshoots and debugs reported problems. The Help Desk manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the access point.
<b>Web User</b>	Select this option to assign privileges to add users for captive portal authentication. For more information on captive portal access rights and configuration requirements, see <a href="#">Configuring Captive Portal Policies on page 9-2</a> .

9. Select **OK** to save the administrator configuration. Select **Reset** to revert to the last saved configuration.

## 10.2 Setting the Access Control Configuration

### ► Security Configuration

Refer to the **Access Control** screen to allow/deny management access to the network using selected protocols (*HTTP, HTTPS, Telnet, SSH* or *SNMP*). Access options can be either enabled or disabled as required. Motorola Solutions recommends disabling unused interfaces to reduce security holes. The Access Control tab is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

The following table demonstrates some interfaces provide better security than others and are more desirable:

<b>Access Type</b>	<b>Encrypted</b>	<b>Authenticated</b>	<b>Default State</b>
Telnet	No	Yes	Disabled
HTTP	No	Yes	Disabled
HTTPS	Yes	Yes	Disabled
SSHv2	Yes	Yes	Disabled

To set user access control configurations:

1. Select **Configuration**.
2. Select **Management**.
3. Select **Access Control** from the list of Management Policy options in the upper, left-hand, side of the UI.

**Access Control**

Management Activated ⓘ

**Telnet**

Enable Telnet

Telnet Port ⓘ 23 (1 to 65,535)

**SSH**

Enable SSHv2 ⓘ

SSHv2 Port ⓘ 22

**HTTP/HTTPS**

Enable HTTP ⓘ

Enable HTTPS ⓘ

**FTP**

Enable FTP ⓘ

FTP Username ⓘ ftpuser

FTP Password ⓘ \*\*\*\*\*

**Access Restrictions**

Filter Type ⓘ None

IP Access List ⓘ <none>

Source Hosts

IP Address	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Source Subnets ⓘ . . . / ⓘ

Logging Policy ⓘ None

OK Reset

**Figure 10-3** Management Policy - Access Control screen

4. Set the following parameters required for **Telnet** access:

<b>Enable Telnet</b>	Select the check box to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.
<b>Telnet Port</b>	Set the port on which Telnet connections are made (1 - 65,535). The default port is 23. Change this value using the spinner control or by entering the port number in the field.

5. Set the following parameters required for **SSH** access:

<b>Enable SSHv2</b>	Select the check box to enable SSH device access. SSH ( <i>Secure Shell</i> ) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.
<b>SSHv2 Port</b>	Set the port on which SSH connections are made. The default port is 22. Change this value using the spinner control or by entering the port number in the field.

6. Set the following **HTTP/HTTPS** parameters:

<b>Enable HTTP</b>	Select the check box to enable HTTP device access. HTTP provides limited authentication and no encryption.
<b>Enable HTTPS</b>	Select the check box to enable HTTPS device access. HTTPS ( <i>Hypertext Transfer Protocol Secure</i> ) is more secure than plain HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication



**NOTE:** If an AP6511 or AP6521's external RADIUS server is not reachable, HTTPS or SSH management access to the access point may be denied. Those models (unlike AP6522, AP6522M, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX) do not have an onboard RADIUS resource and are reliant on an external RADIUS resource for authentication.

7. Set the following **FTP** parameters:

<b>Enable FTP</b>	Select the check box to enable FTP device access. FTP ( <i>File Transfer Protocol</i> ) is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally on the controller. FTP access is disabled by default.
<b>FTP Username</b>	Specify a username required when logging in to the FTP server. The username cannot exceed 32 characters.
<b>FTP Password</b>	Specify a password required when logging in to the FTP server. Reconfirm the password in the field provided to ensure it has been entered correctly. The password cannot exceed 63 characters.
<b>FTP Root Directory</b>	Provide the complete path to the root directory in the space provided. The default setting has the root directory set to flash:/

8. Set the following **General** parameters:

<b>Idle Session Timeout</b>	Specify an inactivity timeout for management connects (in seconds) between 1 - 4,320. The default setting is 12.0
<b>Message of the Day</b>	Enter message of the day text (no longer than 255 characters) displayed at login for clients connecting via Telnet or SSH.

9. Set the following **Access Restrictions**:

<b>Filter Type</b>	Select a filter type for access restriction. Options include <i>IP Access List</i> , <i>Source Address</i> or <i>None</i> . To restrict management access to specific hosts, select <i>Source Address</i> as the filter type and provide the allowed addresses within the <i>Source Hosts</i> field.
<b>IP Access List</b>	If the selected filter type is <i>IP Access List</i> , select an access list from the drop-down menu or select the <i>Create</i> button to define a new one. IP based firewalls function like <i>Access Control Lists (ACLs)</i> to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you do not have an idea of what kind of access to allow or deny, a firewall is of little value, and could provide a false sense of network security.
<b>Source Hosts</b>	If the selected filter type is <i>Source Address</i> , enter an IP Address or IP Addresses for the source hosts. To restrict management access to specific hosts, select <i>Source Address</i> as the filter type and provide the allowed addresses within the <i>Source Hosts</i> field.
<b>Source Subnets</b>	If the selected filter type is <i>Source Address</i> , enter a source subnet or subnets for the source hosts. To restrict management access to specific subnets, select <i>Source Address</i> as the filter type and provide the allowed addresses within the <i>Source Subnets</i> field.
<b>Logging Policy</b>	If the selected filter is <i>Source Address</i> , enter a logging policy for administrative access. Options includes <i>None</i> , <i>Denied Requests</i> or <i>All</i> .

10. Select **OK** to save the Access Control configuration. Select **Reset** to revert to the last saved configuration.

## 10.3 Setting the Authentication Configuration

### ► Security Configuration

As part of the access point's Management Policy, define how client authentication requests are validated using either an *external* or *internal* authentication resource:

To configure an authentication resource:

1. Select **Configuration**.
2. Select **Management**.
3. Select **Authentication** from the list of Management Policy options in the upper, left-hand, side of the UI.

**Authentication** ?

Management Activated ⓘ

**Authentication**

Local  Enabled  Disabled

RADIUS  External ⓘ  Fallback

AAA Policy

TACACS ⓘ  Authentication ⓘ  Fallback

          ⓘ  Accounting ⓘ  Authorization

AAA TACACS Policy ⓘ

**Note:** TACACS Authorization and Auditing will not work for GUI access.

OK Reset

**Figure 10-4** Management Policy - Authentication screen

4. Set the following to authenticate access requests to the access point managed network:

<b>Local</b>	Define whether the access point's internal RADIUS resource (if supported) is used to validate authentication requests. The default setting is Enabled. When enabled, network address information is not required for an external RADIUS resource. AP6511 and AP6521 models have no local resource however and must use an external RADIUS server.
<b>RADIUS</b>	If local is disabled, an external RADIUS resource is used as the authentication service. <i>External</i> and <i>Fallback</i> are not available if the access point's local RADIUS resource is enabled.

5. Use the drop-down menu to specify to select the **AAA Policy** to use with an external RADIUS resource.

An AP6511 or AP6521 model access point (or a model that's not using its local RADIUS resource) will need to interoperate with a RADIUS and LDAP Server (AAA Servers) to provide user database information and user authentication data.

If there is no AAA policy suiting your RADIUS authentication requirements, either select the **Create** icon to define a new AAA policy or select an existing policy from the drop-down menu and select the **Edit** icon to update its configuration. For more information on defining the configuration of a AAA policy, see [AAA Policy on page 7-12](#).

- Set the following AAA TACACS configuration parameters

<b>Authentication</b>	Select to enable TACACS authentication on login.
<b>Accounting</b>	Select to enable TACACS accounting on login.
<b>Fallback</b>	Select to enable fallback to use local authentication if TACACS authentication fails.
<b>Authorization</b>	Select to enable TACACS authorization on login.

- Configure the **AAA TACACS Policy** to use with this authentication policy. Use the drop-down to select a configured AAA TACACS policy.
- Select **OK** to update the configuration. Select **Reset** to revert to the last saved configuration.

## 10.4 Setting the SNMP Configuration

### ► Security Configuration

The access point can use *Simple Network Management Protocol* (SNMP) to interact with wireless devices. SNMP is an application layer protocol that facilitates the exchange of management information. SNMP enabled devices listen on port 162 (by default) for SNMP packets from their management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistical data and configuration parameters from a supported wireless device. The read-write community string is used by a management server to *set* device parameters. SNMP is generally used to monitor a system's performance and other parameters.

<b>SNMP Version</b>	<b>Encrypted</b>	<b>Authenticated</b>	<b>Default State</b>
SNMPv2	No	No	Enabled
SNMPv3	Yes	Yes	Enabled

To define SNMP management values:

1. Select **Configuration > Management**.
2. Select **SNMP** from the list of Management Policy options in the upper, left-hand, side of the UI.

**SNMP** Management Activated ⓘ

**SNMP**

Enable SNMPv1

Enable SNMPv2

Enable SNMPv3 ⓘ

**SNMP v1/v2c Community String**

Community	Access Control	
private	Read-Write	
public	Read Only	

**SNMPv3 Users**

User Name	Authentication	Encryption	Password	
snmpmanager	MD5	DES	*****	
snmptrap	MD5	DES	*****	

Figure 10-5 Management Policy screen - SNMP tab

3. Enable or disable SNMPv2 and SNMPv3.

<b>Enable SNMPv1</b>	Select the check box to enable SNMPv1 support. SNMPv1 provides device management using a hierarchical set of variables. SNMPv1 uses <i>Get</i> , <i>GetNext</i> , and <i>Set</i> operations for data management. SNMPv1 is enabled by default.
<b>Enable SNMPv2</b>	Select the check box to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses <i>Get</i> , <i>GetNext</i> , and <i>Set</i> operations for data management. SNMPv2 is enabled by default.
<b>Enable SNMPv3</b>	Select the check box to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the <i>User-based Security Model</i> (USM) for message security and the <i>View-based Access Control Model</i> (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

4. Set the **SNMP v1/v2 Community String** configuration. Use the **+ Add Row** function as needed to add additional SNMP v1/2 community strings, or select an existing community string's radio button and select the **Delete** icon to remove it.

<b>Community</b>	Define a <i>public</i> or <i>private community</i> designation. By default, SNMPv2 community strings on most devices are set to public for the read-only community string and private for the read-write community string.
<b>Access Control</b>	Set the access permission for each community string used by devices to retrieve or modify information. The available options include: <ul style="list-style-type: none"> <li>• <i>Read Only</i> - Allows a remote device to retrieve information</li> <li>• <i>Read-Write</i> - Allows a remote device to modify settings</li> </ul>

5. Set the **SNMPv3 Users** configuration. Use the **+ Add Row** function as needed to add additional SNMP v3 user configurations, or select a SNMP user's radio button and select the **Delete** icon to remove the user.

<b>User Name</b>	Use the drop-down menu to define a user name of either snmpmanager, snmpoperator or snmpttrap.
<b>Authentication</b>	Displays the authentication scheme used with the listed SNMPv3 user. The listed authentication scheme ensures only trusted and authorized users and devices are permitted access.
<b>Encryption</b>	Displays the encryption scheme used with the listed SNMPv3 user. The listed encryption scheme ensures data is protected when forwarded over insecure interfaces like HTTP.
<b>Password</b>	Provide the user's password in the field provided. Select the <i>Show</i> radio button to display the actual character string used in the password. Leaving the radio button unselected protects the password and displays each character as "*" .

6. Select **OK** to update the SNMP configuration. Select **Reset** to revert to the last saved configuration.

## 10.5 SNMP Trap Configuration

### ► Security Configuration

An access point can use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices, and are therefore an important fault management tool.

A SNMP trap receiver is the SNMP message destination. A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc.

SNMP trap notifications exist for most operations, but not all are necessary for day-to-day operation.

To define a SNMP trap configuration for receiving events at a remote destination:

1. Select **Configuration > Management**.
2. Select **SNMP Traps** from the list of Management Policy options in the upper, left-hand, side of the UI.

The screenshot shows the 'SNMP Traps' configuration window. At the top, it says 'Management Activated'. Under 'Trap Generation', the 'Enable Trap Generation' checkbox is checked. The 'Trap Receivers' section contains a table with the following data:

IP Address	Port	Version	
172.16.10.20	162	SNMPv2c	[Delete Icon]

At the bottom right of the table area, there is an '+ Add Row' button. At the very bottom of the window, there are 'OK' and 'Reset' buttons.

**Figure 10-6** Management Policy screen - SNMP Traps tab

3. Select the **Enable Trap Generation** check box to enable trap creation using the trap receiver configuration defined in the lower portion of the screen. This feature is disabled by default.
4. Refer to the **Trap Receiver** table to set the configuration of the external resource receiving trap information. Select **Add Row +** as required to add additional trap receivers. Select the **Delete** icon to permanently remove a trap receiver.

<b>IP Address</b>	Set the IP address of the external server resource receiving SNMP traps on behalf of the access point.
<b>Port</b>	Set the server port dedicated to receiving traps. The default port is 162.
<b>Version</b>	Set the SNMP version for sending SNMP traps. SNMPv2c is the default.

5. Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

## 10.6 Management Access Deployment Considerations

Before defining an access control configuration as part of a Management Access policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Unused management protocols should be disabled to reduce a potential attack.
  - Use management interfaces providing encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide both data privacy and authentication.
  - By default, SNMPv2 community strings on most devices are set to *public* for the read-only community string and *private* for the read-write community string. Legacy Motorola Solutions devices may use other community strings by default.
  - Motorola Solutions recommends SNMPv3 be used for device management, as it provides both encryption, and authentication.
  - Enabling SNMP traps can provide alerts for isolated attacks at both small radio deployments or distributed attacks occurring across multiple sites.
-



# CHAPTER 11

## DIAGNOSTICS

An access point's resident diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting network performance. Performance and diagnostic information is collected and measured for anomalies causing a key processes to potentially fail.

Numerous tools are available within the Diagnostics menu. Some allow event filtering, some enable log views and some allow you to manage files generated when hardware or software issues are detected.

Diagnostic capabilities include:

- *Fault Management*
  - *Crash Files*
  - *Advanced*
-

## 11.1 Fault Management

### ► Diagnostics

Fault management enables users administering multiple sites to assess device performance and issues effecting the network. Use the Fault Management screens to view and administrate errors generated by an access point or a connected wireless client.

To conduct Fault Management on an access point:

1. Select **Diagnostics**.
2. Select **Fault Management**.

The *Filter Events* screen displays by default. Use this screen to configure how events are tracked and managed. By default, all events are enabled, and an administrator has to turn off events if they don't require tracking.

**Filter Events** ?

**Customize Event Filters**

Severity: All Severities ▼

Module: All Modules ▼

Source: 00 - 00 - 00 - 00 - 00 - 00

Message Substring:

Add to Active Filters

**Active Event Filters**

Severity	Module	Source	Message Substring	Remove Filter
Critical	nsm	0a-11-26-71-00-bd		Click to Remove

Enable All Events   Disable All Events   Activate Defined Filter(s)

**Figure 11-1** Fault Management - Filter Events screen

Use the *Filter Events* screen to create filters for managing events. Events can be filtered based on severity, module received, source MAC of the event, device MAC of the event and MAC address of the wireless client.

3. Define the following **Customize Event Filters**:

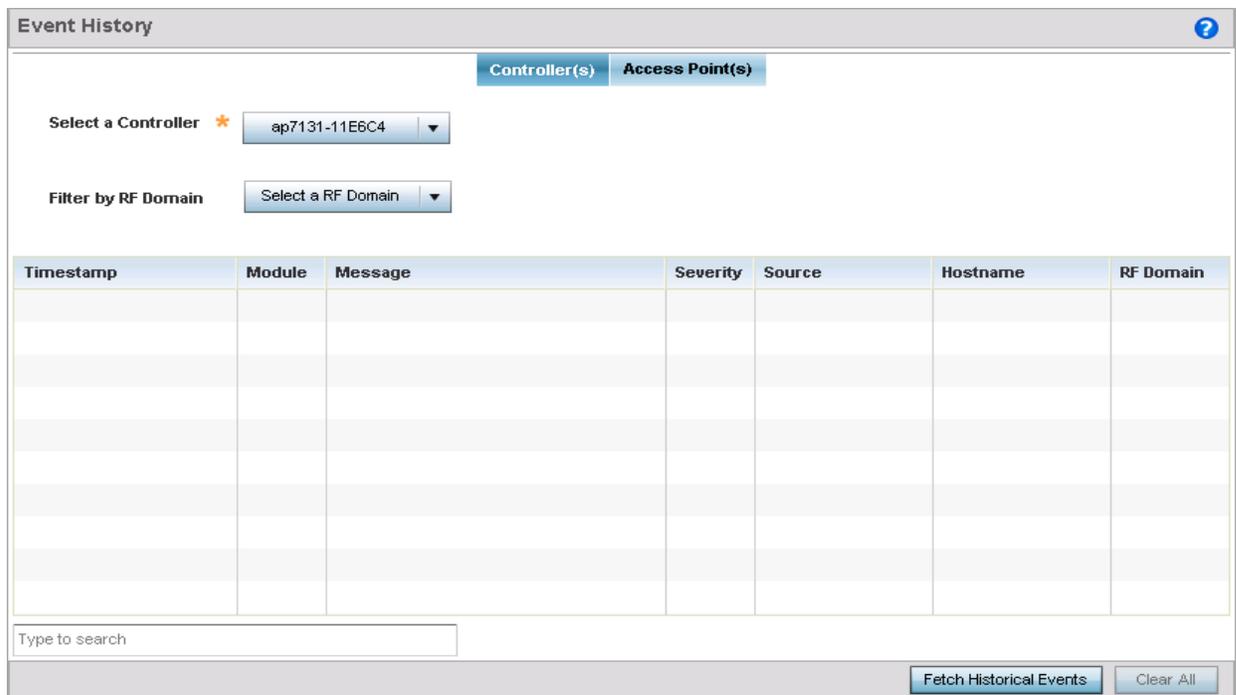
<b>Severity</b>	<p>Set the severity of the event being filtered. Select from the following:</p> <ul style="list-style-type: none"> <li>• <i>All Severities</i> – All events are displayed irrespective of their severity</li> <li>• <i>Critical</i> – Only critical events are displayed</li> <li>• <i>Error</i> – Only errors are displayed</li> <li>• <i>Warning</i> – Only warnings are displayed</li> <li>• <i>Informational</i> – Only informational events are displayed</li> </ul>
-----------------	---



<b>Module</b>	Displays the module used to track the event. Events detected by other modules are not tracked.
<b>Message</b>	Displays error or status messages for each event listed.
<b>Severity</b>	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: <ul style="list-style-type: none"> <li>• <i>All Severities</i> – All events are displayed regardless of their severity</li> <li>• <i>Critical</i> – Only critical events are displayed</li> <li>• <i>Error</i> – Only errors are displayed</li> <li>• <i>Warning</i> – Only warnings are displayed</li> <li>• <i>Informational</i> – Only informational events are displayed</li> </ul>
<b>Source</b>	Displays the MAC address of the source device tracked by the selected module.
<b>Hostname</b>	Displays the Hostname/IP address of the source device tracked by the selected module.

8. Select **Clear All** to clear the events displayed on this screen and begin a new event data collection.
9. Select **Event History** from the upper, left-hand, side of the Fault Management browser.

The *Event History* screen displays events for both wireless controllers and access points. The *Controller(s)* tab displays by default. Information on this tab can be filtered by controllers and then further by the RF Domains on the selected controller. Similarly, the *Access Point(s)* tab displays information for each RF Domain on the access point and this information can be further filtered on the devices adopted by this access point.



**Figure 11-3** Fault Management - Event History screen

10. In the *Controller(s)* tab, select the controller from the **Select a Controller** field to filter events to display. To filter messages further, select a RF Domain from the **Filter by RF Domain** field.
11. In the *Access Point(s)* tab, select the RF Domain from the **Select a RF Domain** field to filter events to display. To filter messages further, select a device from the **Filter by Device** field.,

12. Select **Fetch Historical Events** from the lower, right-hand, side of the UI to populate the table with either device or RF Domain events. The following event data is fetched and displayed:

<b>Timestamp</b>	Displays the timestamp (time zone specific) each listed event occurred.
<b>Module</b>	Displays the module tracking the listed event. Events detected by other modules are not tracked.
<b>Message</b>	Displays error or status message for each event.
<b>Severity</b>	Displays event severity as defined for tracking from the Configuration screen. Severity options include: <ul style="list-style-type: none"> <li>• <i>All Severities</i> – All events are displayed regardless of severity</li> <li>• <i>Critical</i> – Only critical events are display</li> <li>• <i>Error</i> – Only errors display</li> <li>• <i>Warning</i> – Only warnings display</li> <li>• <i>Informational</i> – Only informational events display, no critical events, errors or warnings.</li> </ul>
<b>Source</b>	Displays the MAC address of the device tracked by the selected module.
<b>Hostname</b>	Displays the Hostname/IP address of the device tracked by the selected module.
<b>RF Domain</b>	Displays the RF Domain where the selected access point MAC address resides.

13. Select **Clear Events** to clear the event table and begin a new data collection for the specified device.



## 11.3 Advanced

### ► Diagnostics

Use Advanced diagnostics to review and troubleshoot potential issues with the access point's *User Interface* (UI). The UI Diagnostics screen contains tools to effectively identify and correct access point UI issues. Diagnostics can also be performed at the device level for connected clients.

The following options are available under the Advanced menu:

- [UI Debugging](#)
- [View UI Logs](#)
- [View Sessions](#)

### 11.3.1 UI Debugging

#### ► Advanced

Use the **UI Debugging** screen to view debugging information for a selected device.

To review device debugging information:

1. Select **Diagnostics**.
2. Select **Advanced** to display the UI Debugging menu options. By default, **NETCONF Viewer** is selected.

Once a target ID is selected, its debugging information displays within the **NETCONF Viewer** screen.

**UI Debugging**

NETCONF Viewer

Schema Browser

**Real-Time NETCONF Messages**

ID	Type	Operation	Time (ms)
51	rpc	get-config	
51	rpc-reply	data	1312
52	rpc	cancel_pending_request	
52	rpc-reply	status	2391
53	rpc	cancel_pending_request	
53	rpc-reply	status	1531
49	rpc-reply	ok	301515
51	rpc	get_notifications	

```

*****
<rpc message-id="52">
  <cancel_pending_request/>
</rpc>

```

Find:   Size: 10

**Figure 11-5** UI Debugging screen - NETCONF Viewer

3. Use **NETCONF Viewer** to review NETCONF information. NETCONF is a tag-based configuration protocol. Messages are exchanged using XML tags.

The **Real Time NETCONF Messages** area lists an XML representation of any message generated by the system. The main display area of the screen is updated in real time.

Refer to the **Request Response** and **Time Taken** fields on the bottom of the screen to assess the time taken to receive and respond to requests. The time is displayed in microseconds.

Use the **Clear** button to clear the contents of the Real Time NETCONF Messages area. Use the **Find** parameter and the **Next** button to search for message variables in the Real Time NETCONF Messages area.

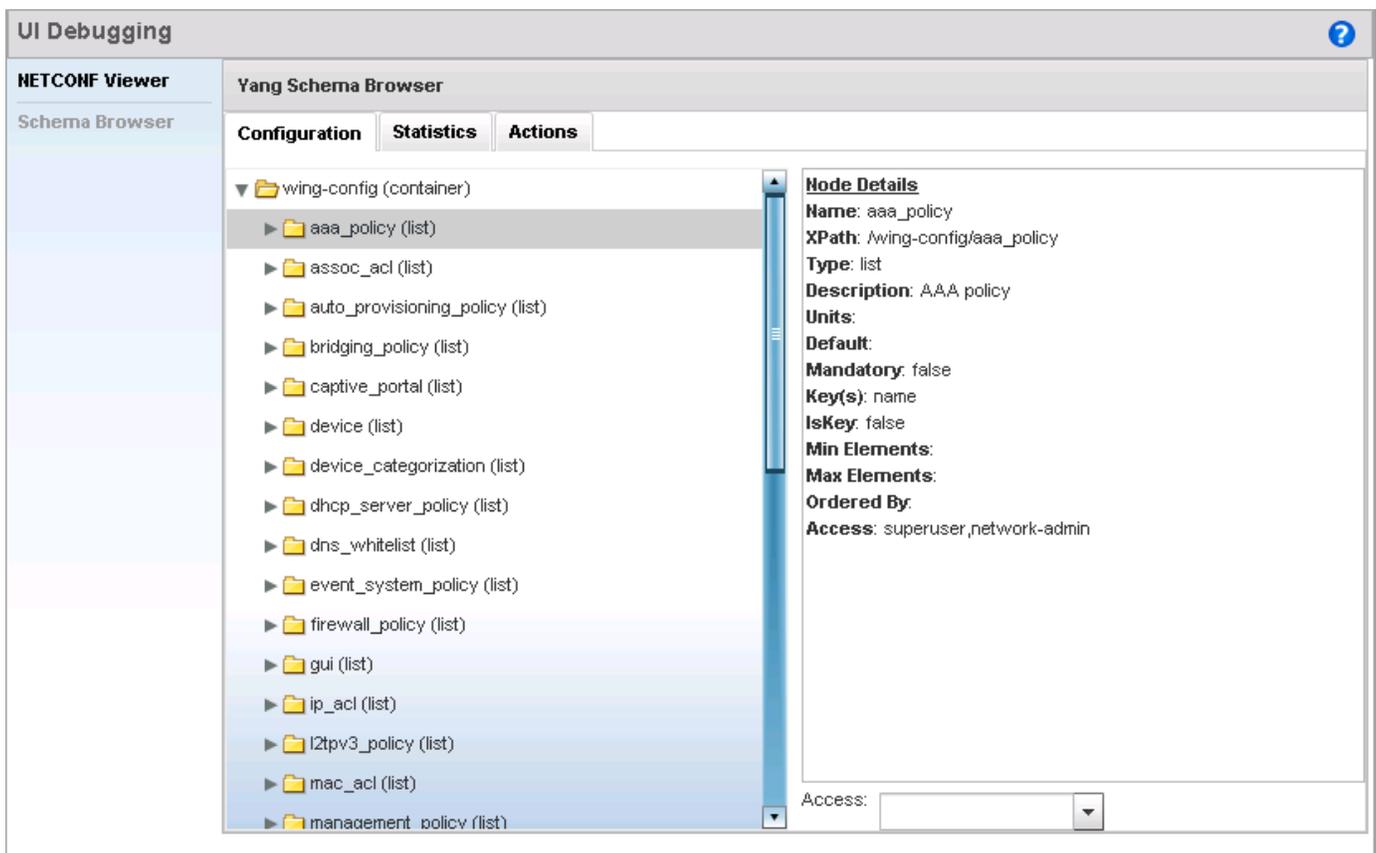
### 11.3.1.1 Schema Browser

#### ► *Advanced*

Use the schema browser to navigate through the WiNG schema.

To review device debugging information:

1. Select **Diagnostics**.
2. Select **Advanced** to display the UI Debugging menu options.
3. Select **Schema Browser** from the navigation pane on the left. The following screen displays:



**Figure 11-6** UI Debugging screen - Schema Browser

The **Schema Browser** displays the **Configuration** tab by default. The Schema Browser displays two fields (regardless of the *Configuration*, *Statistics* or *Actions* tab selected). Use the left field to navigate the schema by expanding and collapsing directories. Selecting a node on the left displays node details on the right. The Schema Browser does not display information in real time. It only displays the data on the device when last updated.

4. Expand a configuration parameter to review its settings. The Configuration tab provides an ideal place to verify if the last saved configuration differs from default settings, or has been erroneously changed in respect to the access point's intended configuration.

5. Select the **Statistics** tab to assess performance data and statistics for a target device.

Use Statistics data to assess whether the device is optimally configured in respect to its intended deployment objective. Often the roles of radio supported devices and wireless clients change as additional devices and radios are added to the access point managed network.

6. Select the **Actions** tab to display schema for any action that can be configured.

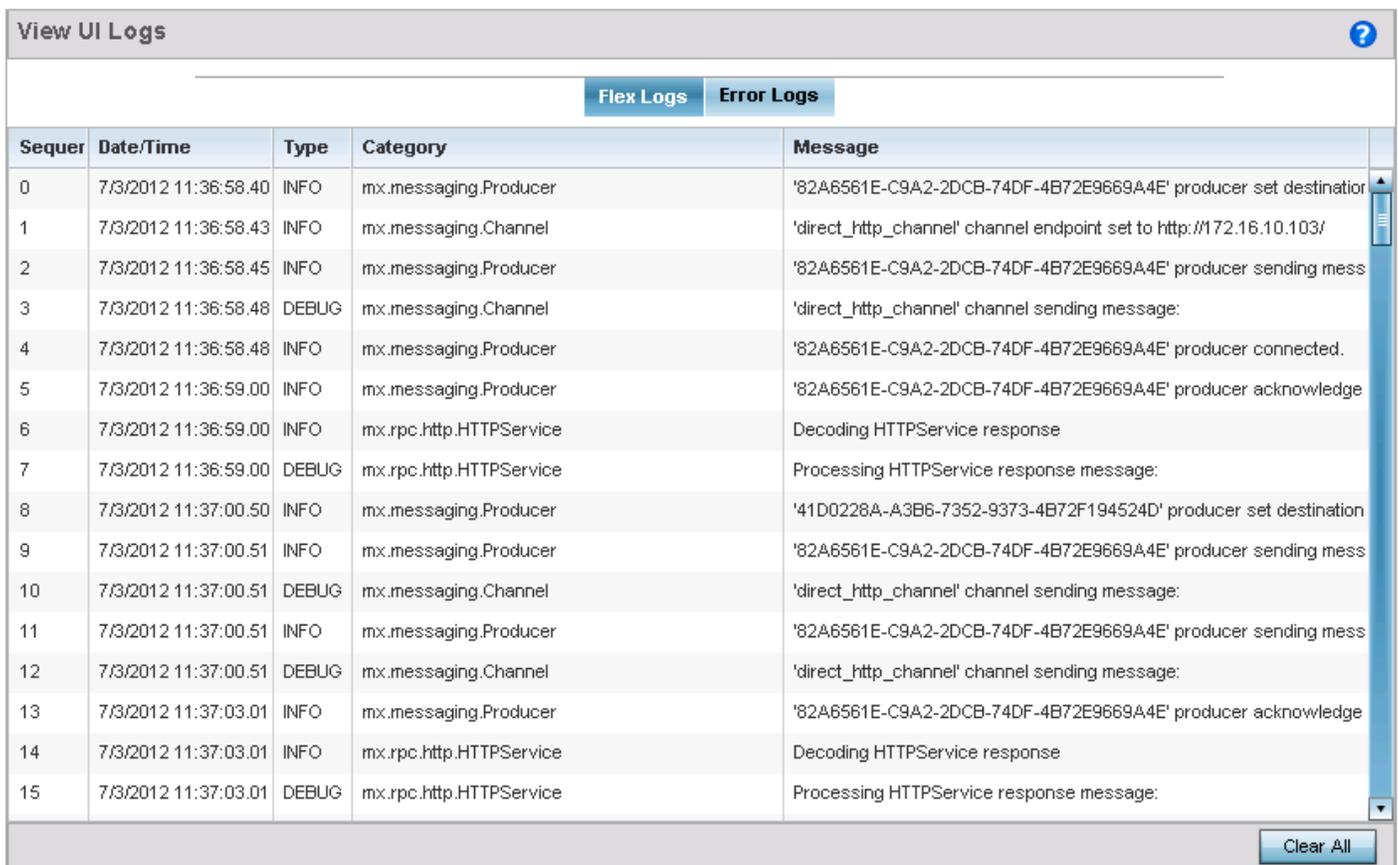
### 11.3.2 View UI Logs

#### ► Advanced

Use the **View UI Logs** screen to view the log messages generated by the device. Logs are classified as *Flex Logs* and *Error Logs*. These logs provide a real-time look into the state of the device and provide useful information for debugging and trouble shooting issues.

To display the logs:

1. Select **Diagnostics**.
2. Select **Advanced** to display the UI Debugging menu options.
3. Select the **View UI Logs** menu item to display the logs. By default, the *Flex Logs* screen displays.



Sequencer	Date/Time	Type	Category	Message
0	7/3/2012 11:36:58.40	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer set destination
1	7/3/2012 11:36:58.43	INFO	mx.messaging.Channel	'direct_http_channel' channel endpoint set to http://172.16.10.103/
2	7/3/2012 11:36:58.45	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer sending mess
3	7/3/2012 11:36:58.48	DEBUG	mx.messaging.Channel	'direct_http_channel' channel sending message:
4	7/3/2012 11:36:58.48	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer connected.
5	7/3/2012 11:36:59.00	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer acknowledge
6	7/3/2012 11:36:59.00	INFO	mx.rpc.http.HTTPService	Decoding HTTPService response
7	7/3/2012 11:36:59.00	DEBUG	mx.rpc.http.HTTPService	Processing HTTPService response message:
8	7/3/2012 11:37:00.50	INFO	mx.messaging.Producer	'41D0228A-A3B6-7352-9373-4B72F194524D' producer set destination
9	7/3/2012 11:37:00.51	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer sending mess
10	7/3/2012 11:37:00.51	DEBUG	mx.messaging.Channel	'direct_http_channel' channel sending message:
11	7/3/2012 11:37:00.51	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer sending mess
12	7/3/2012 11:37:00.51	DEBUG	mx.messaging.Channel	'direct_http_channel' channel sending message:
13	7/3/2012 11:37:03.01	INFO	mx.messaging.Producer	'82A6561E-C9A2-2DCB-74DF-4B72E9669A4E' producer acknowledge
14	7/3/2012 11:37:03.01	INFO	mx.rpc.http.HTTPService	Decoding HTTPService response
15	7/3/2012 11:37:03.01	DEBUG	mx.rpc.http.HTTPService	Processing HTTPService response message:

**Figure 11-7** View UI Logs - Flex Logs tab

The *Sequence* (order of occurrence), *Date/Time*, *Type*, *Category* and *Message* items display for each log option selected.

Use the **Clear All** button to clear all logs shown in this screen.

4. Select the **Error Logs** tab to display the error logs for this device. The following screen displays:







# CHAPTER 12

## SECURITY CONFIGURATION

The functions supported within the **Operations** menu allow the administration of firmware, configuration files and certificates for managed devices.

A certificate links identity information with a public key enclosed in the certificate. Device certificates can be imported and exported to a secure remote location for archive and retrieval as they are required for application to other managed devices.

*Self Monitoring At Run Time RF Management* (Smart RF) is a Motorola Solutions innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements. The Smart RF functionality scans the RF network to determine the best channel and transmit power for each managed access point radio.

For more information, refer to the following:

- [Devices](#)
- [Certificates](#)
- [Smart RF](#)

Refer to [Operations Deployment Considerations on page 12-55](#) for tips on how to optimize the access point's configuration

---

## 12.1 Devices

### ► Security Configuration

Motorola Solutions periodically releases updated device firmware and configuration files to the Motorola Solutions Support Web site. If an access point's (or its associated device's) firmware is older than the version on the Web site, Motorola Solutions recommends updating to the latest firmware version for full functionality and utilization. Additionally, selected devices can either have a primary or secondary firmware image applied or fallback to a selected firmware image if an error were to occur in the update process.

Device update activities include:

- [Managing Firmware and Configuration Files](#)
- [Rebooting the Device](#)
- [Locating a Device](#)
- [Upgrading Device Firmware](#)
- [Viewing Device Summary Information](#)
- [Adopted Device Upgrades](#)
- [File Management](#)
- [Adopted Device Restart](#)
- [Captive Portal Pages](#)
- [Re-elect Controller](#)



**NOTE:** AP upgrades can only be performed by access points in Virtual Controller AP mode, and cannot be initiated by Standalone APs. Additionally, upgrades can only be performed on access points of the same model as the Virtual Controller AP.

---

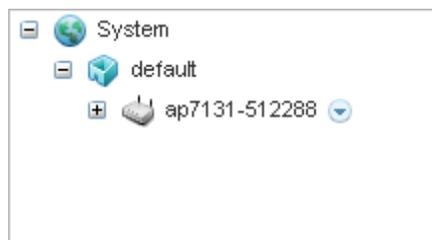
---

These tasks can be performed on individual access points and wireless clients.

### 12.1.1 Managing Firmware and Configuration Files

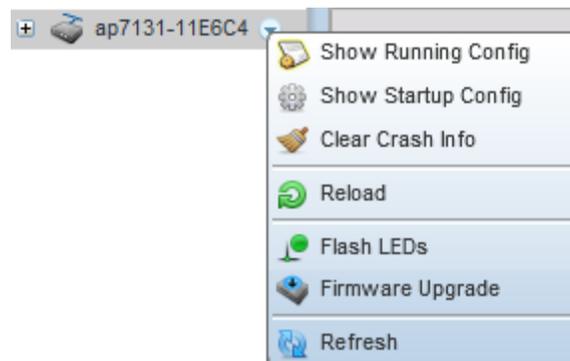
#### ► Devices

Firmware and configuration files are viewed and managed from the device browser.



**Figure 12-1** Device Browser

Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-2** Device Browser - Options for an AP7131

Refer to the drop-down menu on the lower, left-hand side, of the UI. The following tasks and displays are available in respect to device firmware for the selected device:

<b>Show Running Config</b>	Select this option to display the running configuration of the selected device. The running configuration is displayed in a separate window. Select <i>Execute</i> to perform the function. For more information on viewing and managing the running configuration, see <a href="#">Managing Running Configuration on page 12-3</a> .
<b>Show Startup Config</b>	Select this option to display the startup configuration of the selected device. The startup configuration is displayed in a separate window. Select <i>Execute</i> to perform the function. For more information on viewing and managing the startup configuration, see <a href="#">Managing Startup Configuration on page 12-6</a> .
<b>Clear Crash Info</b>	Select this option to clear the crash dump files stored on the selected device. A screen displays listing the crash dump files stored on the selected device. From the screen, a crash dump file can be deleted or copied elsewhere. For more information on managing the crash dump files, see <a href="#">Managing Crash Dump Files on page 12-9</a> .
<b>Reload</b>	Select this option to reload the selected device. Clicking this option reboots the selected device.
<b>Flash LEDs</b>	Select this option to flash the selected device's LEDs. Use this option when it is required to identify the physical location of the device. For more information, see <a href="#">Locating a Device on page 12-11</a> .
<b>Firmware Upgrade</b>	Select this option to upgrade the selected device's firmware. For information on conducting a device firmware upgrade, see <a href="#">Upgrading Device Firmware on page 12-12</a> .

For information on conducting a device firmware upgrade, see [Upgrading Device Firmware on page 12-12](#). For information on file transfers, see [File Management on page 12-23](#).

### 12.1.1.1 Managing Running Configuration

#### ► [Managing Firmware and Configuration Files](#)

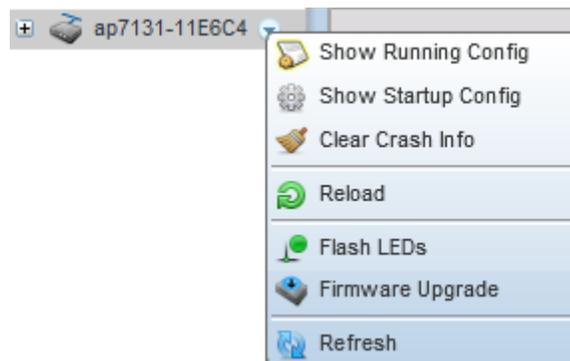
Running configuration is the current configuration of the selected device. To view and manage the running configuration:

1. Select a target device from the left-hand side of the UI.



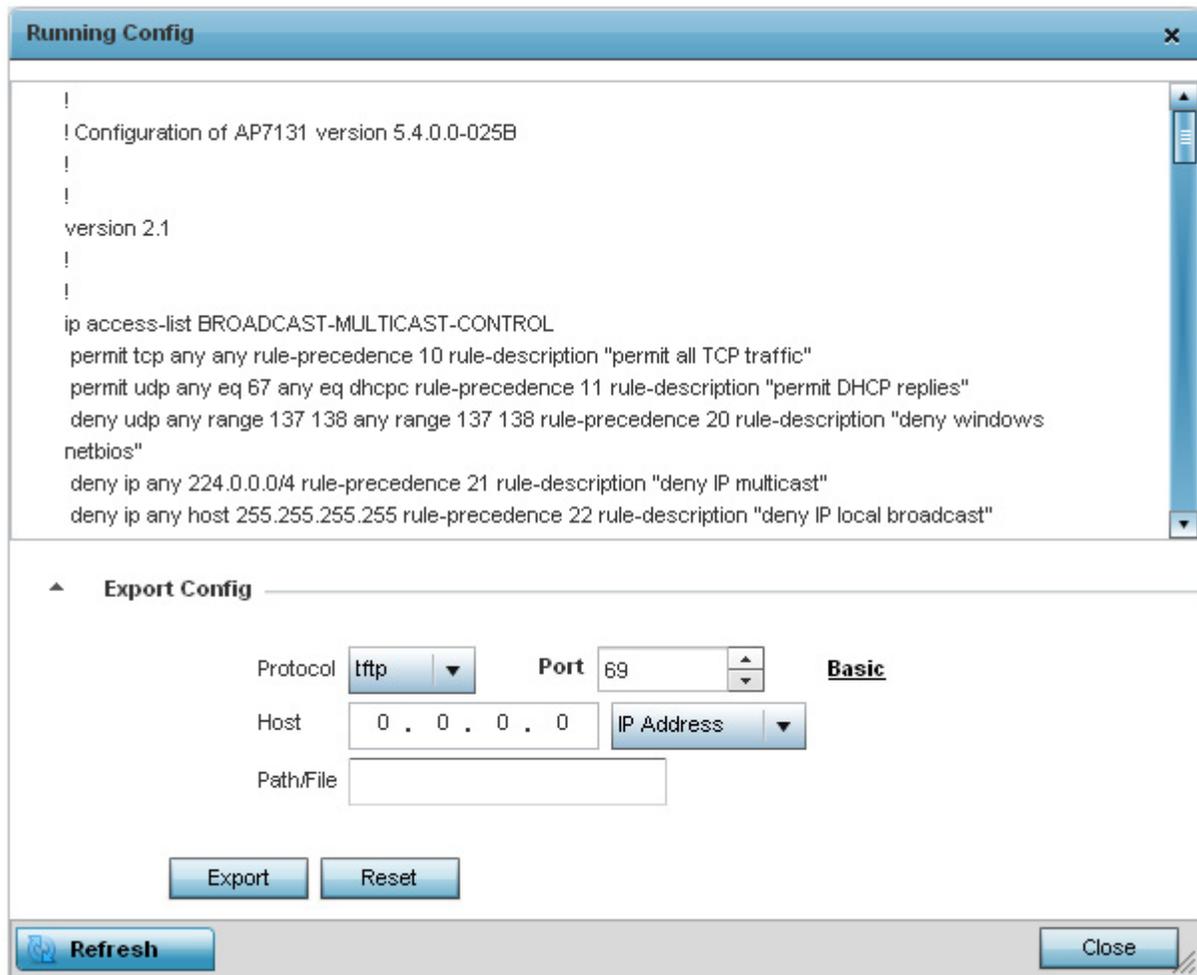
**Figure 12-3** Device Browser

2. Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-4** Device Browser - Options for a device

3. Select **Show Running Config** to display the *Running Configuration* window.



**Figure 12-5** Operations - Manage Running Configuration

- Use the **Export Config** field to configure the parameters required to export the running configuration to an external server. Refer to the following to configure the export parameters:

<b>Protocol</b>	Select the protocol used for exporting the running configuration. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	Use the spinner control or manually enter the value to define the port used by the protocol for exporting the running configuration. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .

<b>Host</b>	Enter IP address or the hostname of the server used to export the running configuration to. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Path/File</b>	Specify the path to the folder to export the running configuration to. Enter the complete relative path to the file on the server.
<b>User Name</b>	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Password</b>	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .

5. Select **Export** button to export the running configuration using the settings configured in the **Export Config** field.



**NOTE:** Another way to export the running configuration to the device used to view the configuration is to click in the area that displays the running configuration and use the **[ctrl]+a** keyboard combination to select all the contents of the text area into the OS's clipboard memory. Open a text editor, paste the copied content and save the file.

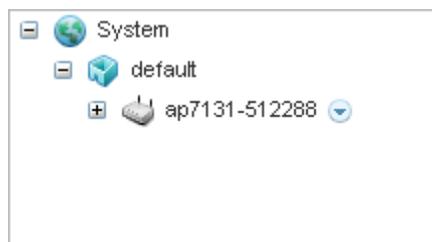
6. To update the screen with the latest changes made to the running configuration, select the **Refresh** button located to the bottom right of the screen.

### 12.1.1.2 Managing Startup Configuration

#### ► *Managing Firmware and Configuration Files*

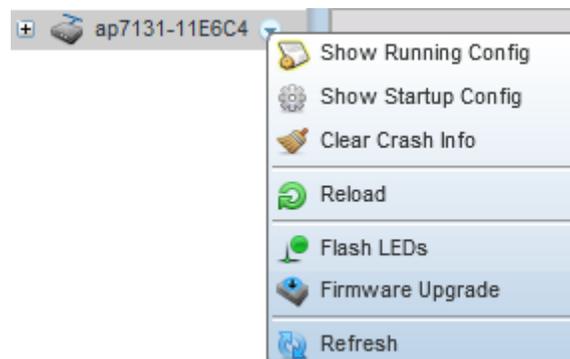
Startup configuration is the configuration that will be loaded the next time the device is booted. To view and manage the startup configuration:

1. Select a target device from the left-hand side of the UI.



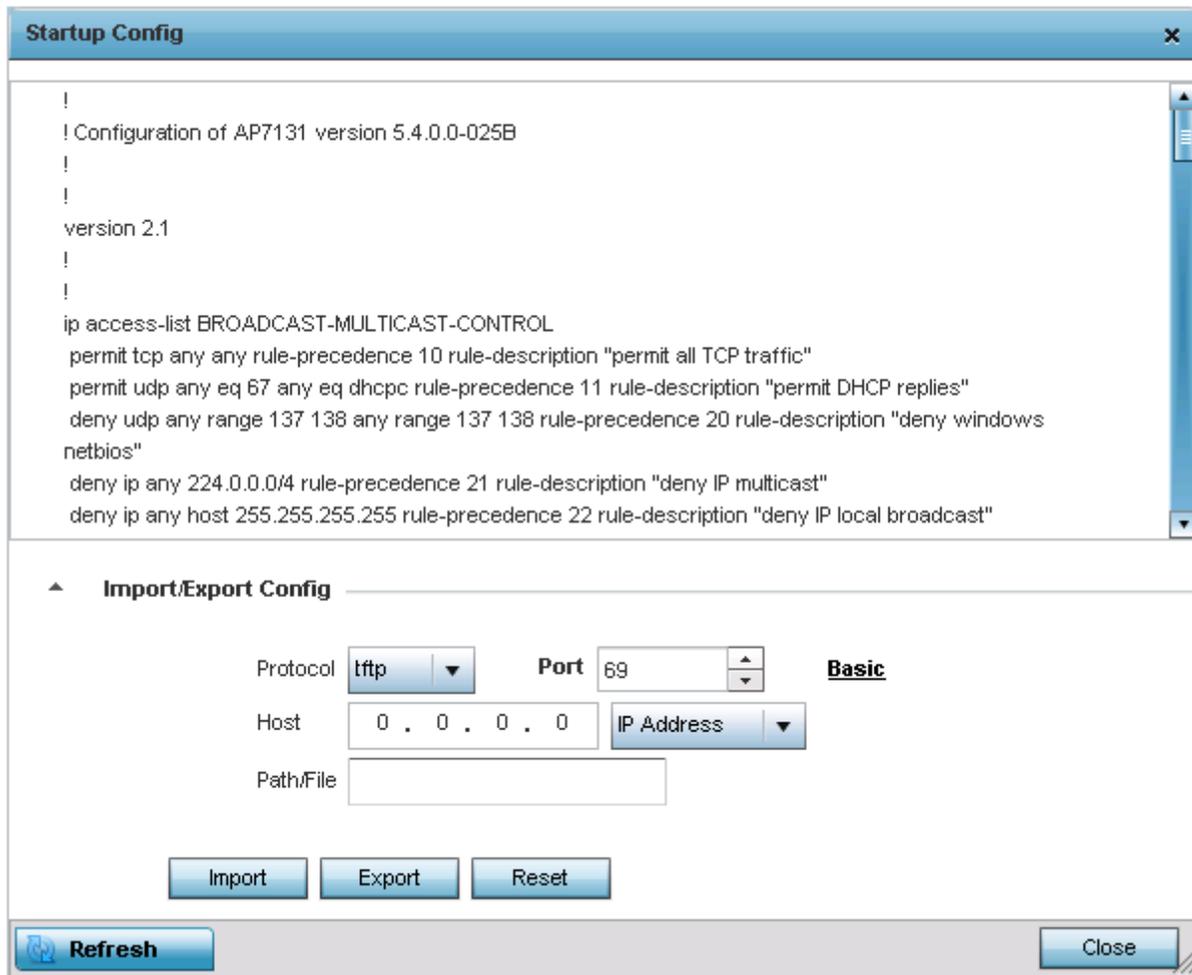
**Figure 12-6** Device Browser

2. Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-7** Device Browser - Options for a device

3. Select **Show Startup Config** to display the *Startup Configuration* window.



**Figure 12-8** Operations - Manage Startup Configuration

- Use the **Import/Export Config** field to configure the parameters required to export or import the startup configuration to or from an external server. Refer to the following to configure the remote server parameters:

<b>Protocol</b>	<p>Select the protocol used for exporting or importing the startup configuration. Available options include:</p> <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> <li>• <i>local</i></li> </ul>
-----------------	---

<b>Port</b>	Use the spinner control or manually enter the value to define the port used by the protocol for exporting or importing the startup configuration. This option is not valid for <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	Enter IP address or the hostname of the server used to export or import the startup configuration to. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> . Use the drop-down to select the type of host information. Host can be one of <i>Host Name</i> or <i>IP Address</i> .
<b>Path/File</b>	Specify the path to the folder to export or import the startup configuration to. Enter the complete relative path to the file on the server.
<b>User Name</b>	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Password</b>	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .

5. Select **Export** button to export the startup configuration using the settings configured in the **Import/Export Config** field. Similarly, Select **Import** button to import the startup configuration.



**NOTE:** Another way to export the startup configuration is to click in the area that displays the configuration, and use the **[ctrl]+a** keyboard combination to select all the contents of the text area into the OS's clipboard. Open a text editor, paste the copied content and save the file.

---



---

6. To update the screen with the latest changes made to the startup configuration, select the **Refresh** button located to the bottom right of the screen.

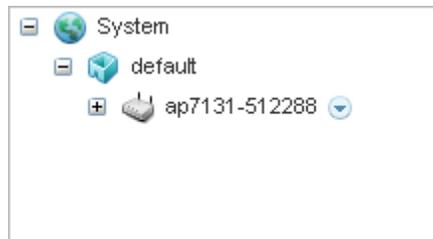
### 12.1.1.3 Managing Crash Dump Files

► *Managing Firmware and Configuration Files*

Crash files are generated when the device encounters a critical error that impairs the performance of the device. When a critical error arises, information about the state of the device at that moment is written to a text file. This file is used by Motorola Solutions Support Center to debug the issue and provide a solution to correct the error condition.

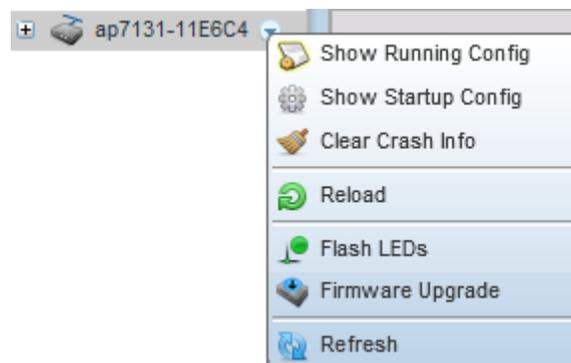
To view and manage the crash information files:

1. Select a target device from the left-hand side of the UI.



**Figure 12-9** Device Browser

2. Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-10** Device Browser - Options for a device

3. Select **Clear Crash Info** to display the *Clear Crash Info* window.

Clear Crash Info			
File Name	Size	Last Modified	Actions
flash:/crashinfo/Crash_001.txt	10771	2012-02-23 04:17:39	 

**Figure 12-11** Clear Crash Info screen

- Refer to the following for more information on the *Clear Crash Info* screen.

<b>File Name</b>	Displays the full path to the crash file
<b>Size</b>	Displays the size of the crash information file in kilobytes.
<b>Last Modified</b>	Displays the timestamp the crash information file was modified last.
<b>Action</b>	Displays icons for the actions that can be performed on the selected crash information file. Use the <b>-</b> icon to delete the selected crash info file. Use the <i>Copy</i> icon to copy the file to a remote location.

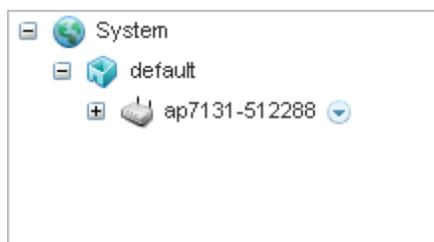
- Use the **Copy** button at the bottom to copy the selected file to a remote location. Use the **Delete** button to delete the selected crash info file.

## 12.1.2 Rebooting the Device

### ► Devices

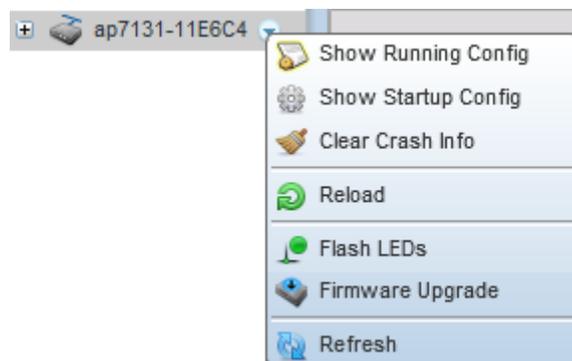
To force the device to restart:

- Select a target device from the left-hand side of the UI.



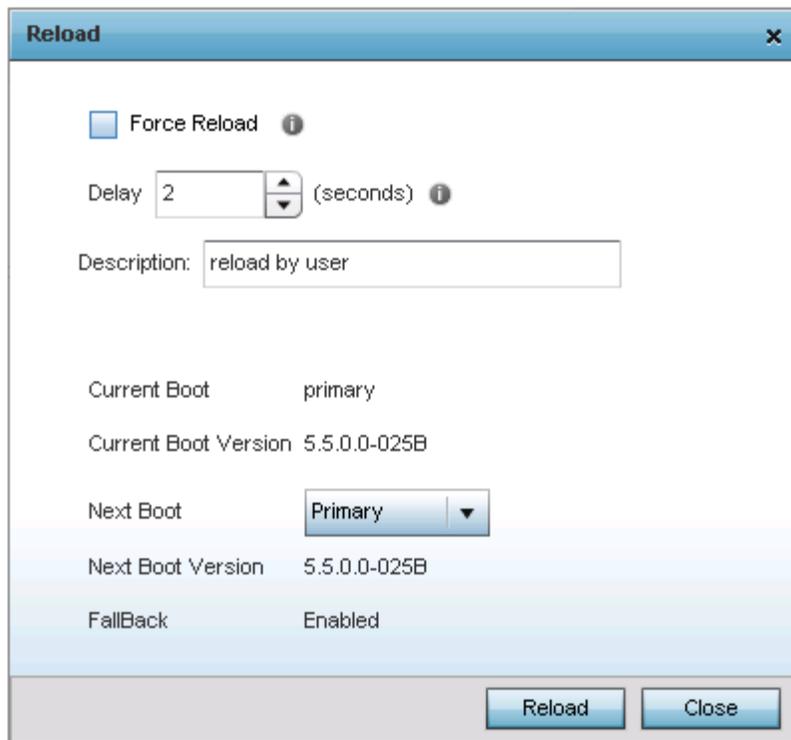
**Figure 12-12** Device Browser

- Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-13** Device Browser - Options for a device

- To reboot the device, select the **Reload** item.



**Figure 12-14** Device - Reload screen

4. Refer the following for more information on this screen:

<b>Force Reload</b>	Select this option to force this device to reload. Use this option for devices that are unresponsive and do not reload normally.
<b>Delay</b>	Use the spinner to configure a delay in seconds before the device is reloaded. Set this value to 0 to reload the device immediately.
<b>Description</b>	Use the text box to provide a brief description detailing the reason to reload this device.
<b>Current Boot</b>	Displays the current running firmware. Displays either <i>primary</i> or <i>secondary</i> .
<b>Current Boot Version</b>	Displays the firmware version number for the running firmware.
<b>Next Boot</b>	Displays the firmware that will be loaded on next boot.
<b>Next Boot Version</b>	Displays the firmware version number that will be loaded on next boot.
<b>Fallback</b>	Displays the status of Fallback. Displays <i>Enabled</i> or <i>Disabled</i> .

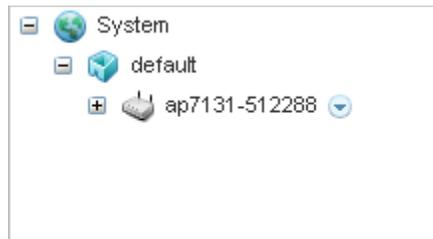
### 12.1.3 Locating a Device

#### ► Devices

In large deployments with a large number of devices, it is very hard to identify a specific device. Use the device's locator feature to find the device. Once configured, the device blinks its LEDs in a color that enables it to be identified amongst all other deployed devices.

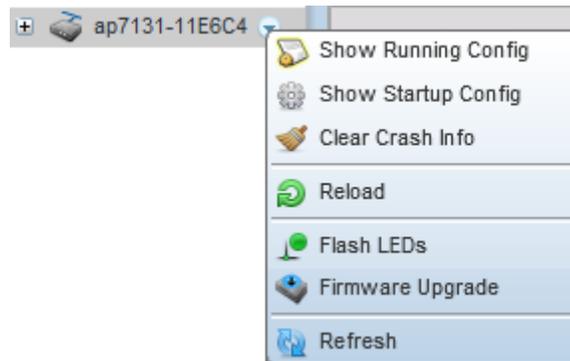
To locate a device:

1. Select the target device from the left-hand side of the UI.



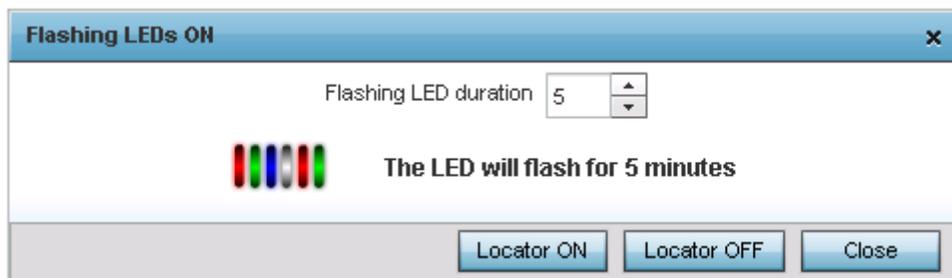
**Figure 12-15** Device Browser

2. Select the down arrow next to the device to view a set of operations that can be performed on the selected device.



**Figure 12-16** Device Browser - Options for a device

3. To locate the device, click the **Flash LEDs** item. The following window displays:



**Figure 12-17** Device Pane - Locator screen

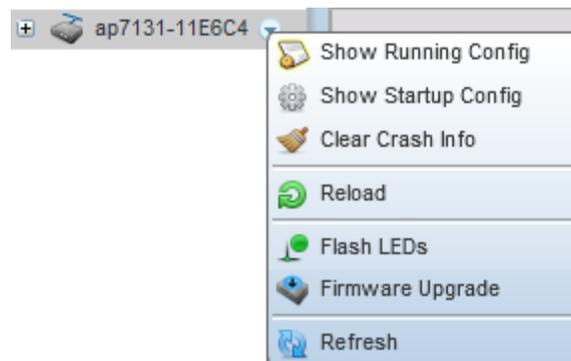
4. Use the spinner to set a value for **Flash LED Duration**. This is the duration, in minutes, the device will flash its LEDs. Once this duration expires, the LEDs starts operating normally.
5. Click **Locator ON** to start flashing the LEDs. Click **Locator OFF** to stop the LEDs from flashing and resume normal operation. Click **Close** to close this window.

## 12.1.4 Upgrading Device Firmware

### ► Devices

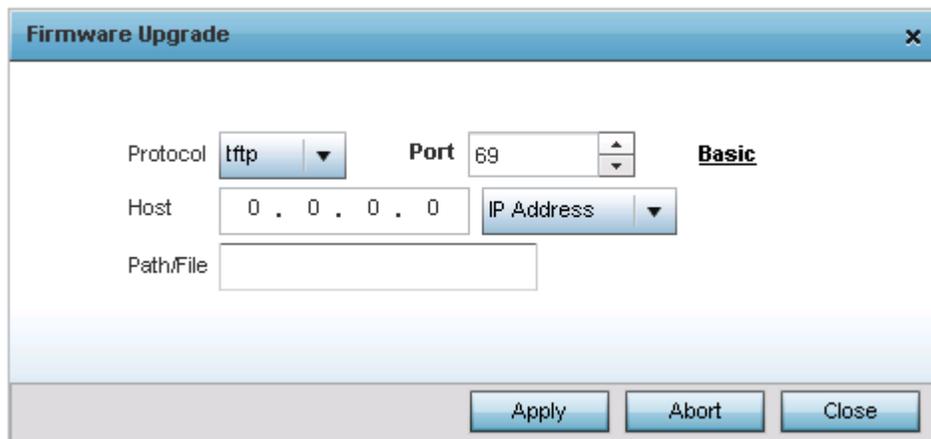
To update the firmware of an access point:

1. Select a target device from the left-hand side of the UI.
2. Select the down arrow next to the device to view a set of operations that can b performed on the selected device.



**Figure 12-18** Device Browser - Options for a device

3. Select the **Firmware Upgrade** button to upgrade the device's firmware.



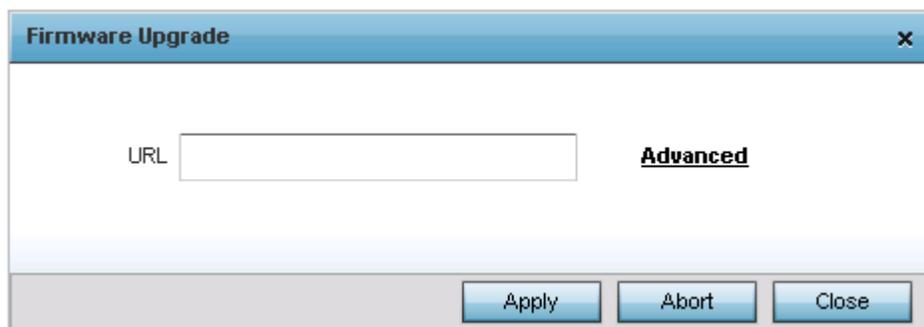
**Figure 12-19** Firmware Upgrade screen

4. Provide the following information to accurately define the location of the target device's firmware file:

<b>Protocol</b>	Select the protocol used for updating the firmware. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> <li>• <i>local</i></li> </ul>
<b>Port</b>	Use the spinner control or manually enter the value to define the port used by the protocol for importing the firmware upgrade file. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	Enter IP address or the hostname of the server used to import the firmware file. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> . Use the drop-down to select the type of host information. The host can be either an IP address or hostname.

<b>Path/File</b>	Specify the path to the firmware file. Enter the complete relative path to the file on the server.
<b>User Name</b>	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Password</b>	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .

5. Select **Apply** to start the firmware update. Select **Abort** to terminate the firmware update. Select **Close** to close the upgrade popup. The upgrade continues in the background.
6. The **Basic** link on the screen displays a simple interface with a text box to provide a **URL** to the upgrade file. Enter the complete relative path to the file on a remote server in the **URL** field. Click **Apply** to start the firmware update.



**Figure 12-20** Firmware Upgrade - Basic screen

## 12.1.5 Viewing Device Summary Information

### ► Devices

Use the **Summary** screen to assess whether a device's firmware or configuration file requires an update to the latest feature set and functionality. To view the **Summary** screen:

1. Select **Operations**.
2. Select **Devices**.
3. Use the navigation pane on the left to navigate to the device to manage the firmware and configuration files on and select it.

The **Device Details Summary** screen displays by default. when the **Operations** menu item is selected from the main menu.



**NOTE:** When displaying the **Summary** screen at the RF Domain level of the UI's hierarchal tree, the screen does not display a field for a device's **Primary** and **Secondary** firmware image. At the RF Domain level, the Summary screen just lists the *Hostname*, *MAC Address*, *Online* status, *Device Type* and *Is Controller* designations for the devices comprising the selected RF Domain. A RF Domain must be selected from the hierarchal tree and expanded to list the devices comprising the RF Domain. From there, individual controllers, service platforms and Access Points can be selected and their properties modified.

Summary Adopted Device Upgrade File Management Adopted Device Restart Captive Portal Pages RAID

Device Type AP71XX

	Primary	Secondary
Version	5.5.0.0-085R	5.5.0.0-083R
Build Date	10:06:2013 14:59:37	09:29:2013 02:46:18
Install Date	10:07:2013 01:48:18	10:03:2013 01:32:00

FallBack Enabled  
 Current Boot secondary  
 Upgrade Status Successful  
 2013-10-07 01:48:18

Firmware Upgrade Reload

Device Type	Is Controller	Online	Offline	Total
ap71xx	✓ Yes	1	0	1

**Figure 12-21** Device Details screen

4. Refer to the following to determine whether a firmware image needs requires an update:

<b>Firmware Version</b>	Displays the <i>Primary</i> and <i>Secondary</i> firmware image version currently utilized by the selected access point.
<b>Build Date</b>	Displays the date the <i>Primary</i> and <i>Secondary</i> firmware image was built for the selected device.
<b>Install Date</b>	Displays the date the firmware was installed on the access point.
<b>Fallback</b>	Lists whether fallback is currently enabled for the selected device. When enabled, the device reverts back to the last successfully installed firmware image if something were to happen in its next firmware upgrade that would render the device inoperable.
<b>Current Boot</b>	Lists whether the primary or secondary firmware image is to be applied the next time the device boots.
<b>Upgrade Status</b>	Displays the status of the last firmware upgrade. For information on upgrading device firmware, see <a href="#">Upgrading Device Firmware on page 12-12</a> .

5. Select **Firmware Upgrade** to upgrade the device's firmware to display the *Firmware Upgrade* screen. For more information, see [Upgrading Device Firmware on page 12-12](#).
6. Select **Reload** to restart the device.

## 12.1.6 Adopted Device Upgrades

► *Devices*

To configure an access point upgrade:



**NOTE:** AP upgrades can only be performed by access points in Virtual Controller AP mode, and cannot be initiated by Standalone APs. Additionally, upgrades can only be performed on access points of the same model as the Virtual Controller AP.

1. Select **Operations** from the main menu.
2. Select **Devices**.
3. Use the navigation pane on the left to navigate to the device to manage the firmware and configuration files on and select it.

Summary
Adopted Device Upgrade
File Management
Adopted Device Restart
Captive Portal Pages
RAID

**Device Type** AP71XX ?

	Primary	Secondary
<b>Version</b>	5.5.0.0-085R	5.5.0.0-083R
<b>Build Date</b>	10:06:2013 14:59:37	09:29:2013 02:46:18
<b>Install Date</b>	10:07:2013 01:48:18	10:03:2013 01:32:00

FallBack Enabled

Current Boot secondary

Upgrade Status Successful  
2013-10-07 01:48:18

Firmware Upgrade
 Reload

Device Type	Is Controller	Online	Offline	Total
ap71xx	✔ Yes	1	0	1

**Figure 12-22** Device Summary screen

4. Select **Adopted Device Upgrade** tab. The following screen displays:

Summary
Adopted Device Upgrade
File Management
Adopted Device Restart
Captive Portal Pages
RAID

Adopted Device Upgrade ?

Device Upgrade List | 
 Device Image File | 
 Upgrade Status | 
 Upgrade History

Device Type List AP71xx ▾

Scheduled Upgrade Time  Now 07/11/2012  0  : 0  (HH:MM)  No Reboot  Staggered Reboot

Scheduled Reboot Time  Now 07/11/2012  0  : 0  (HH:MM)  Force Upgrade

**All Devices**

<input checked="" type="checkbox"/>	Hostname	MAC Address	Device Model	Version	Upload Version
<input type="checkbox"/>	Upbeat	00 - 23 - 68 - 0F - 41 - C8	ap71xx	5.5.0.0-085R	5.5.0.0-085R

Update Firmware

**Figure 12-23** Devices - Adopted AP Upgrade screen



**NOTE:** If selecting the *Device Upgrade* screen from the RF Domain level of the UI, there is an additional **Upgrade from Controller** option to the right of the **Device Type List** drop-down menu. Select this option to provision selected device models within the same RF Domain from this RF Domain manager controller. If expanding a RF Domain and selecting a member device, the upgrade tab is entitled **Adopted Device Upgrade**, as an upgrade is made from an elected RF Domain Manager device. There's also an additional *Device Image File* screen to select the device image type and set the transfer protocol.

5. Refer to the following to configure the required AP upgrade parameters:

<b>Device Type List</b>	Select the access point model to specify which model is available to upgrade by the Virtual Controller AP. Upgrades can only be made to the same access point model. For example, an AP6532 firmware image cannot be used to upgrade an AP7131 model access point. For that reason, the drop-down menu will only display the model deployed.
<b>Scheduled Upgrade Time</b>	To perform the upgrade immediately, select <i>Now</i> . To schedule the upgrade to take place at a specified time, enter a date and time. Select whether you require an immediate reboot once the AP is updated. If you would like a reboot later, schedule the time accordingly. The AP must be rebooted to implement the firmware upgrade. Select <i>No Reboot</i> to ensure the access point remains in operation with its current firmware. This option is useful to ensure the access point remains operational until ready to take it offline for the required reboot.

<b>Schedule Reboot Time</b>	To reboot a target access point immediately, select <i>Now</i> . To schedule the reboot to take place at a specified time in the future, enter a date and time. This feature is helpful when wishing to upgrade an access point's firmware, but wish to keep in operation until the reboot does not impact its current client support and operation.
<b>No Reboot</b>	Select this option to prevent upgraded access points from being rebooted. This ensures that the access point remains in operation with its current firmware. This option is useful to ensure the access point remains operational until ready to take it offline for the required reboot.
<b>Staggered Reboot</b>	Select this option to do a staggered rebooting of upgraded access points. When selected, upgraded access points are not rebooted simultaneously bringing down the network. A few access points at a time are rebooted to preserve network availability.
<b>Force Upgrade</b>	Select this option to force upgrade for the selected access point. When selected, the access points are upgraded even if they have the same firmware as the upgrading wireless controller or service platform or access point.

6. Refer to the **All Devices** table for information about all the access points adopted by this device. Refer to the following for more information:

<b>Hostname</b>	Displays the access point's hostname if configured.
<b>MAC Address</b>	Displays the access point's MAC address.
<b>Device Model</b>	Displays the access point's model and type.
<b>Version</b>	Displays the firmware version installed on the access point,
<b>Upload Version</b>	Displays the firmware version of the image uploaded to the access point.

7. Click the option in the first column for each access point that needs to be updated.
8. Select the **Device Image File** tab to specify the model and network address information to the file used in the access point upgrade operation.

The screenshot shows the 'Adopted AP Upgrade' configuration page. At the top, there are tabs for 'Summary', 'Adopted AP Upgrade', 'File Management', 'Adopted AP Restart', and 'Captive Portal Pages'. The 'Adopted AP Upgrade' tab is active. Below the tabs, there are sub-tabs for 'Device Upgrade List', 'Device Image File', 'Upgrade Status', and 'Upgrade History'. The 'Device Image File' sub-tab is selected.

Configuration parameters include:

- Device Image Type: AP71XX
- Protocol: tftp
- Port: 69
- Host: 0 . 0 . 0 . 0
- Path/File: (empty)
- Mode: Basic

A 'Load Image' button is located at the bottom left. On the right side, there is a table titled 'Images On Device' with the following data:

Device Type	Version
AP81XX	5.5.0.0-085R
AP71XX	5.5.0.0-085R
AP6521	5.5.0.0-085R
AP6532	5.5.0.0-085R
AP621	5.5.0.0-085R
AP6522	5.5.0.0-085R
AP6511	5.5.0.0-085R
AP622	5.5.0.0-085R
AP650	5.5.0.0-085R

**Figure 12-24** AP Upgrade screen - AP Image File

9. Select the **Device Image File** tab and refer to the following configuration parameters:

<b>Device Image Type</b>	Select the access point model to specify which model should be available to upgrade. Upgrades can only be made to the same access point model. For example, an AP6532 firmware image cannot be used to upgrade an AP7131 model access point. For that reason, the drop-down menu will only display the model deployed.
<b>URL</b>	Enter a URL pointing to the location of the image file.
<b>Advanced/Basic</b>	Select <i>Advanced</i> to list additional options for the image file location including protocol, host and path. Additional options display based on the selected protocol. Select <i>Basic</i> to display only the URL field.

<b>Protocol</b>	<p>Select the protocol to retrieve the image files. Available options include:</p> <ul style="list-style-type: none"> <li>• <i>tftp</i> - Select this option to specify a file location using <i>Trivial File Transfer Protocol</i>. A port and IP address or hostname are required. A path is optional.</li> <li>• <i>ftp</i> - Select this option to specify a file location using <i>File Transfer Protocol</i>. A port, IP address or hostname, username and password are required. A path is optional.</li> <li>• <i>sftp</i> - Select this option to specify a file location using <i>Secure File Transfer Protocol</i>. A port, IP address or hostname, username and password are required. A path is optional.</li> <li>• <i>http</i> - Select this option to specify a file location using <i>Hypertext Transfer Protocol</i>. A hostname or IP address is required. Port and path are optional</li> <li>• <i>cf</i> - Select this option to specify a file location on a Compact Flash card installed on the device. This option might not be available on all devices.</li> <li>• <i>usb1/usb2/usb3/usb4</i> - Select this option to specify the file location on one of the USB 1, USB 2, USB 3 or USB 4 ports of the device. This option might not be available on all devices.</li> </ul>
<b>Port</b>	Use the spinner control or manually enter the value to define the port used by the protocol for importing the firmware upgrade file. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> .
<b>Host</b>	Enter IP address or the hostname of the server used to import the firmware file. This option is not valid for <i>local</i> , <i>cf</i> , <i>usb1</i> , <i>usb2</i> , <i>usb3</i> and <i>usb4</i> . Use the drop-down to select the type of host information. Host can be one of <i>Host Name</i> or <i>IP Address</i> .
<b>Path/File</b>	Specify the path to the firmware file. Enter the complete relative path to the file on the server.
<b>User Name</b>	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Password</b>	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .

10. When the AP Image Type and appropriate file location and protocol have been specified, select the **Load Image** button to load all available images to the **Type** and **Version** table.

The table now displays available images and their corresponding versions.

11. Select the **Upgrade Status** tab to review a list of devices being upgraded by this access point.

**Figure 12-25** AP Upgrade screen - Upgrade Status screen

12. Refer to the following fields to understand the status of the number of device being updated:

<b>Number of devices currently being upgraded</b>	Lists the number of firmware upgrades currently in-progress and downloading for selected devices. Once the device has the image it requires a reboot to implement the firmware image.
<b>Number of devices currently being rebooted</b>	Lists the number devices currently booting after receiving an upgrade image. The reboot is required to implement the new image and renders the device offline during that period. Using the <i>Device Upgrade List</i> , reboots can be staggered or placed on hold to ensure device remains in service.
<b>Number of devices waiting in queue to be upgraded</b>	Lists the number of devices waiting to receive a firmware image from their provisioning access point. Each device can have its own upgrade time defined, so the upgrade queue could be staggered.
<b>Number of devices waiting in queue to be rebooted</b>	Lists the number of devices waiting to reboot before actively utilizing its upgraded image. The <i>Device Upgrade List</i> list allows an administrator to disable or stagger the reboot time, so device reboots may not occur immediately after an upgrade. The reboot operation renders the device offline until completed so reboots can scheduled for periods of reduced load.
<b>Number of devices marked for cancellation</b>	Displays the total number of device upgrades that have been manually cancelled during the upgrade operation.

13. Refer to the following fields for more information:

<b>Device Type</b>	Displays the model number of devices pending an upgrade. Each listed device is provisioned an image file unique to that model.
<b>Hostname</b>	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.

<b>MAC Address</b>	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.
<b>Result</b>	Lists the state of an upgrade operation ( <i>downloading, waiting for a reboot</i> etc.).
<b>Upgrade Time</b>	Displays whether the upgrade is immediate or set by an administrator for a specific time. This is helpful to ensure a sufficient number of devices remain in service at any given time.
<b>Reboot Time</b>	Displays whether a reboot is immediate or time set by an administrator for a specific time. Reboots render the device offline, so planning reboots carefully is central to ensuring a sufficient number of devices remain in service.
<b>Last Status</b>	Lists the last reported upgrade and reboot status of each listed in progress or planned upgrade operation.
<b>Upgraded By</b>	Lists the model of the controller, service platform or access point RF Domain manager that's provisioning the image to the listed device.

- Optionally select **Cancel** (from the lower, right-hand corner of the screen) to cancel the upgrade of devices under the selected RF Domain. The **Cancel** button is enabled only if there are device undergoing upgrade and they are selected for cancellation.
- Select the **Upgrade History** tab to review an Upgrade History of access point upgrade operations.

**Figure 12-26** AP Upgrade screen - Upgrade History screen

- Refer to the following to assess devices impacted by upgrade operations and their upgrade status:

<b>Hostname</b>	Displays the hostname of the access point, if configured.
<b>Device Model</b>	Displays the type of access point upgraded.
<b>MAC Address</b>	Displays the primary MAC (or hardware identifier) for each device impacted by an upgrade operation.

<b>Result</b>	Displays the current upgrade status for each listed access point. Possible states include: <ul style="list-style-type: none"> <li>• <i>Waiting</i></li> <li>• <i>Downloading</i></li> <li>• <i>Updating Scheduled</i></li> <li>• <i>Reboot</i></li> <li>• <i>Rebooting Done</i></li> <li>• <i>Cancelled</i></li> <li>• <i>Done</i></li> <li>• <i>No Reboot</i></li> </ul>
<b>Time</b>	Displays the time when the device was upgraded.
<b>Retries</b>	Displays the number of retries, if any, during the upgrade. If this number is more than a few, the upgrade configuration should be revisited.
<b>Upgraded By</b>	Displays the hostname of the device that upgraded this device.
<b>Last Status</b>	Displays the time of the last status update for access points that are no longer upgrading.
<b>Clear History</b>	Selecting the <i>Clear History</i> button clears the history log page for each access point.
<b>Cancel</b>	Clicking the <i>Cancel</i> button will cancel the upgrade process for any selected access points that are upgrading.

17. Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

## 12.1.7 File Management

### ► *Devices*

The access point maintains a File Browser enabling the administration of files currently residing on any internal or external memory location. Directories can be created and maintained for each File Browser location, and folders and files can be moved and deleted as needed.



**NOTE:** The **File Management** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the File Management UI option is available.

To manage files stored on the device:

1. Select **Operations** from the main menu.
2. Select **Devices**.
3. Use the navigation pane on the left to navigate to the device to manage the files on and select it.

Summary Adopted Device Upgrade File Management Adopted Device Restart Captive Portal Pages RAID

Device Type AP71XX ?

	Primary	Secondary
Version	5.5.0.0-085R	5.5.0.0-083R
Build Date	10:06:2013 14:59:37	09:29:2013 02:46:18
Install Date	10:07:2013 01:48:18	10:03:2013 01:32:00

FallBack Enabled

Current Boot secondary

Upgrade Status Successful  
2013-10-07 01:48:18

Firmware Upgrade
Reload

Device Type	Is Controller	Online	Offline	Total
ap71xx	✔ Yes	1	0	1

**Figure 12-27** Device Summary screen

- Click **File Management**. The following screen displays:



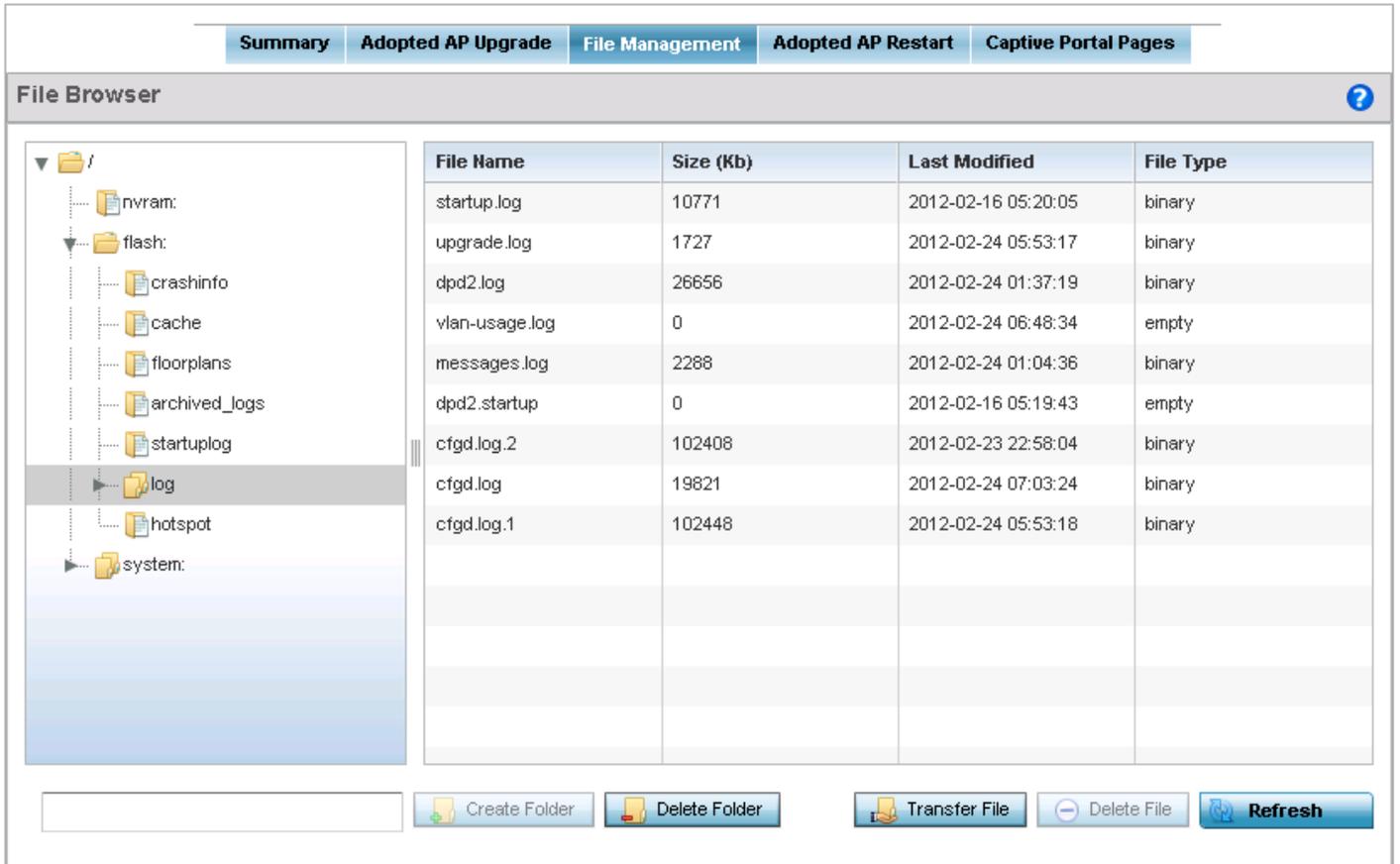


Figure 12-29 Devices - File Management screen

6. Refer to the following for more information:

<b>File Name</b>	Displays the name of the file.
<b>Size (Kb)</b>	Displays the size of the file in kilobytes.
<b>Last Modified</b>	Displays the timestamp for the last modification made to the file.
<b>File Type</b>	Displays the type of file. File type can be <i>binary</i> , <i>empty</i> or <i>text</i> .

- To create a folder, select the parent folder in the directory tree on the left. Enter the directory name in the **Folder Name** text box. Click the **Create Folder** button to create the new folder. Click the **Refresh** button to refresh the view in the screen.
- To delete a folder, select the folder in the directory tree on the left. Click **Delete Folder** button. The following popup displays:



Figure 12-30 Devices - File Management - Delete Confirmation screen

Click **Proceed** to delete the directory. All files in the selected directory also get deleted. Click **Abort** to exit without deleting the directory.

- Click **Transfer File** to transfer files between the device and a remote server. The following window displays:

**Figure 12-31** File Management - File Transfer Dialog

Use this dialog to transfer files between the device and a remote location. The transfer can be done as follows:

- From remote server to the device
- From device to remote server
- From a location on the device to another location on the same device.

- Set the following file management source and target directions as well as the configuration parameters of the required file transfer activity:

<b>Source</b>	<ul style="list-style-type: none"> <li>• Select <i>Server</i> to indicate the source of the file is a remote server.</li> <li>• Select <i>Local</i> to indicate the file is on the access point itself.</li> </ul>
<b>File</b>	If the source is <i>Local</i> , enter the name of the file to be transferred.

<b>Protocol</b>	<p>If <i>Advanced</i> is selected, choose the protocol for file management. Available options include:</p> <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i> and <i>Advanced</i> is selected.</p>
<b>Port</b>	<p>If <i>Advanced</i> is selected, specify the port for transferring files. This option is not available for <i>cf</i>, <i>usb1</i>, <i>usb2</i>, <i>usb3</i> and <i>usb4</i>. Enter the port number directly or use the spinner control.</p> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i>.</p>
<b>IP Address</b>	<p>If <i>Advanced</i> is selected, specify the IP address of the server used to transfer files. This option is not valid for <i>cf</i>, <i>usb1</i>, <i>usb2</i>, <i>usb3</i> and <i>usb4</i>. If IP address of the server is provided, a <i>Hostname</i> is not required.</p> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i>.</p>
<b>Hostname</b>	<p>If needed, specify a Hostname of the server transferring the file. This option is not valid for <i>cf</i>, <i>usb1</i>, <i>usb2</i>, <i>usb3</i> and <i>usb4</i>. If a hostname is provided, an <i>IP Address</i> is not needed.</p> <p>This field is only available when <i>Server</i> is selected in the <i>From</i> field.</p>
<b>Path/File</b>	<p>If <i>Advanced</i> is selected, define the path to the file on the server. Enter the complete relative path to the file.</p> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i>.</p>
<b>User Name</b>	<p>If <i>Advanced</i> is selected, provide a user name to access a FTP or SFTP server.</p> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i>, and the selected protocol is <i>ftp</i> or <i>sftp</i>.</p>
<b>Password</b>	<p>If <i>Advanced</i> is selected, provide a password to access the FTP or SFTP server.</p> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i>, and the selected protocol is <i>ftp</i> or <i>sftp</i>.</p>
<b>Target</b>	<p>If <i>Advanced</i> is selected, set the target destination to transfer the file using FTP or SFTP.</p> <ul style="list-style-type: none"> <li>• Select <i>Server</i> if the destination is a remote server, then provide a URL to the location of the server resource or select <i>Advanced</i> and provide the same network address information described above.</li> <li>• Select Access Point if the destination is an access point.</li> </ul>

11. Select **Ok** to begin the file transfer. Selecting **Cancel** reverts the screen to its last saved configuration.
12. To delete a file, select the file to be deleted and click **Delete File** button. The file is deleted immediately.

## 12.1.8 Adopted Device Restart

### ► Devices

Use the *Adopted Device Restart* screen to restart one or more of the access points adopted by this AP. To view the Adopted Device Restart screen:



**NOTE:** The **Adopted Device Restart** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the Adopted Device Restart option is available.

1. Select **Operations** from the main menu.
2. Select **Devices**.
3. Use the navigation pane on the left to navigate to the device to manage the files on and select it.

Summary
Adopted Device Upgrade
File Management
Adopted Device Restart
Captive Portal Pages
RAID

**Device Type** AP71XX ?

	Primary	Secondary
<b>Version</b>	5.5.0.0-085R	5.5.0.0-083R
<b>Build Date</b>	10:06:2013 14:59:37	09:29:2013 02:46:18
<b>Install Date</b>	10:07:2013 01:48:18	10:03:2013 01:32:00

FallBack Enabled

Current Boot secondary

Upgrade Status Successful

2013-10-07 01:48:18

Firmware Upgrade
Reload

Device Type	Is Controller	Online	Offline	Total
ap71xx	✔ Yes	1	0	1

**Figure 12-32** Device Summary screen

4. Select **Adopted Device Restart**. The following screen displays:



2. Select **Devices**.
3. Use the navigation pane on the left to navigate to the device to manage the files on and select it.

	Primary	Secondary
Version	5.5.0.0-085R	5.5.0.0-083R
Build Date	10:06:2013 14:59:37	09:29:2013 02:46:18
Install Date	10:07:2013 01:48:18	10:03:2013 01:32:00

FallBack Enabled  
Current Boot secondary  
Upgrade Status Successful  
2013-10-07 01:48:18

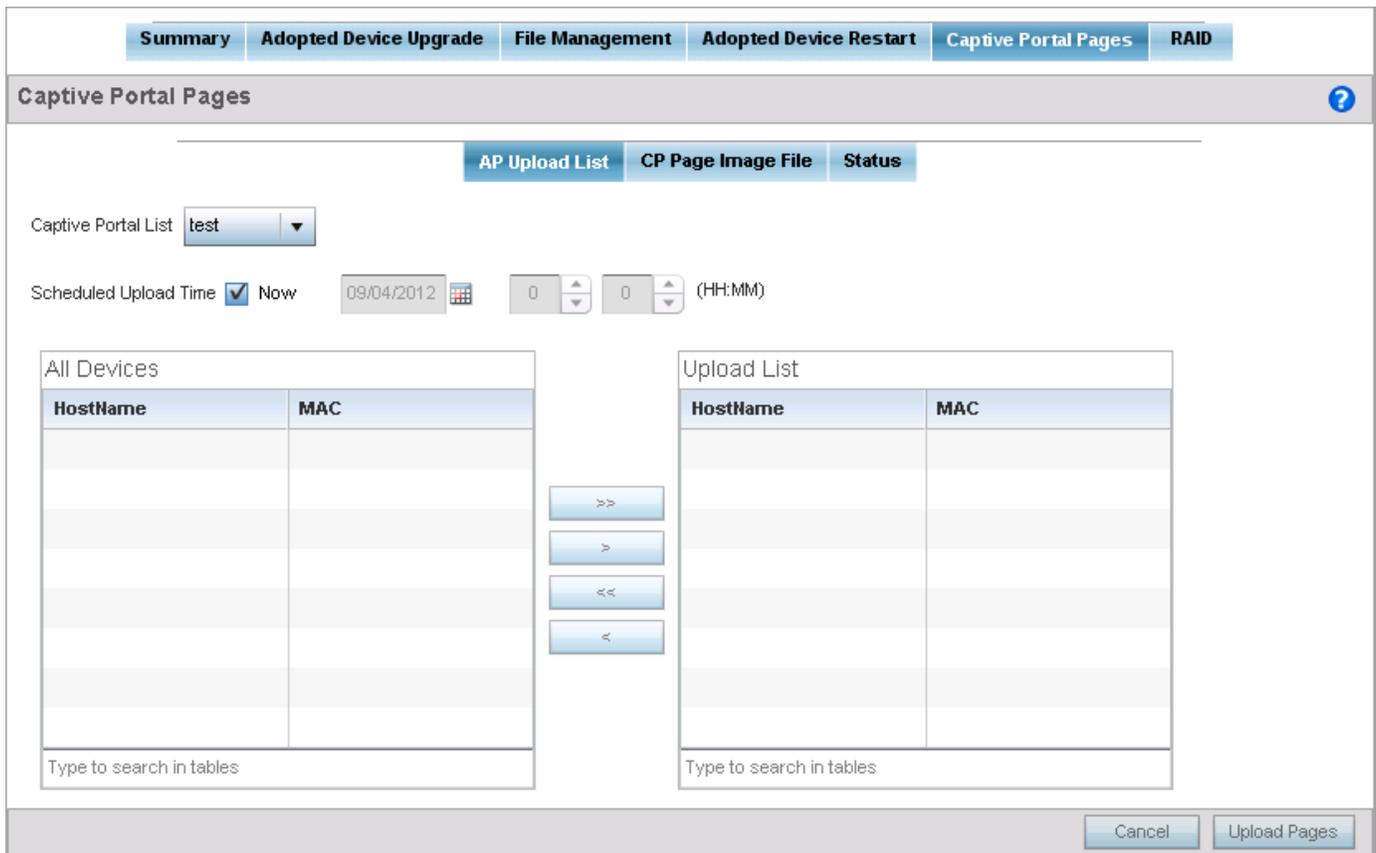
Device Type	Is Controller	Online	Offline	Total
ap71xx	✓ Yes	1	0	1

**Figure 12-34** Device Summary screen

4. Select **Captive Portal Pages**. The following screen displays:



**NOTE:** If selecting the **Captive Portal Pages** screen from the RF Domain level of the UI's hierarchal tree, there's an additional **Upload from Controller** option to the right of the **Captive Portal List** drop-down menu. Select this option to upload captive portal page support from this device's managing controller.



**Figure 12-35** Devices Captive Portal Pages - AP Upload List screen

5. Use the **Captive Portal List** drop-down list to select the captive portal configuration to upload to the adopted access points.
6. Use the **Scheduled Upload Time** field to configure the time of the captive portal pages update. Select **Now** option to immediately start the process of the update. Use the date, hour fields to configure a specific date and time for upload.
7. The **All Devices** table lists the hostname and MAC address of all devices adopted by this access point. Use the arrow buttons to move selected devices from the **All Devices** table to the **Upload List** table. The **Upload List** table lists the devices to which the captive portal pages are updated.
8. Select **Upload Pages** to upload the captive portal pages to the selected devices.
9. Select the **CP Pages Image File** tab. The following screen displays:

**Figure 12-36** Devices Captive Portal Pages - CP Page Image File screen

10. Use the **Captive Portal List** drop-down list to select the captive portal configuration to upload to the adopted access points.
11. Set the following file transfer configuration parameters of the required file transfer activity:

<b>Protocol</b>	<p>If <i>Advanced</i> is selected, choose the protocol for file management. Available options include:</p> <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul> <p>This parameter is required only when <i>Server</i> is selected as the <i>Source</i> and <i>Advanced</i> is selected.</p>
<b>Port</b>	<p>If <i>Advanced</i> is selected, specify the port for transferring files. This option is not available for <i>cf</i>, <i>usb1</i>, <i>usb2</i>, <i>usb3</i> and <i>usb4</i>. Enter the port number directly or use the spinner control.</p>



15. Refer to the **Status** tab to view the history of captive portal pages upload.

<b>Hostname</b>	Displays the hostname of the target device.
<b>MAC</b>	Displays the factory assigned MAC address of the target device.
<b>State</b>	Displays the target device's state.
<b>Progress</b>	Displays the progress of the upload to the target device.
<b>Retries</b>	Displays the number of retries attempted for upload to the target device.
<b>Last Status</b>	Displays the last known status of the upload to the target device.

16. Select **Clear History** to clear the history displayed in the **Status** tab.

### 12.1.10 Re-elect Controller

#### ► Devices

Use the **Controller Re-election** screen to identify available access point resources within a selected RF Domain and optionally make some, or all, of the access points available to initiate tunnel connections.



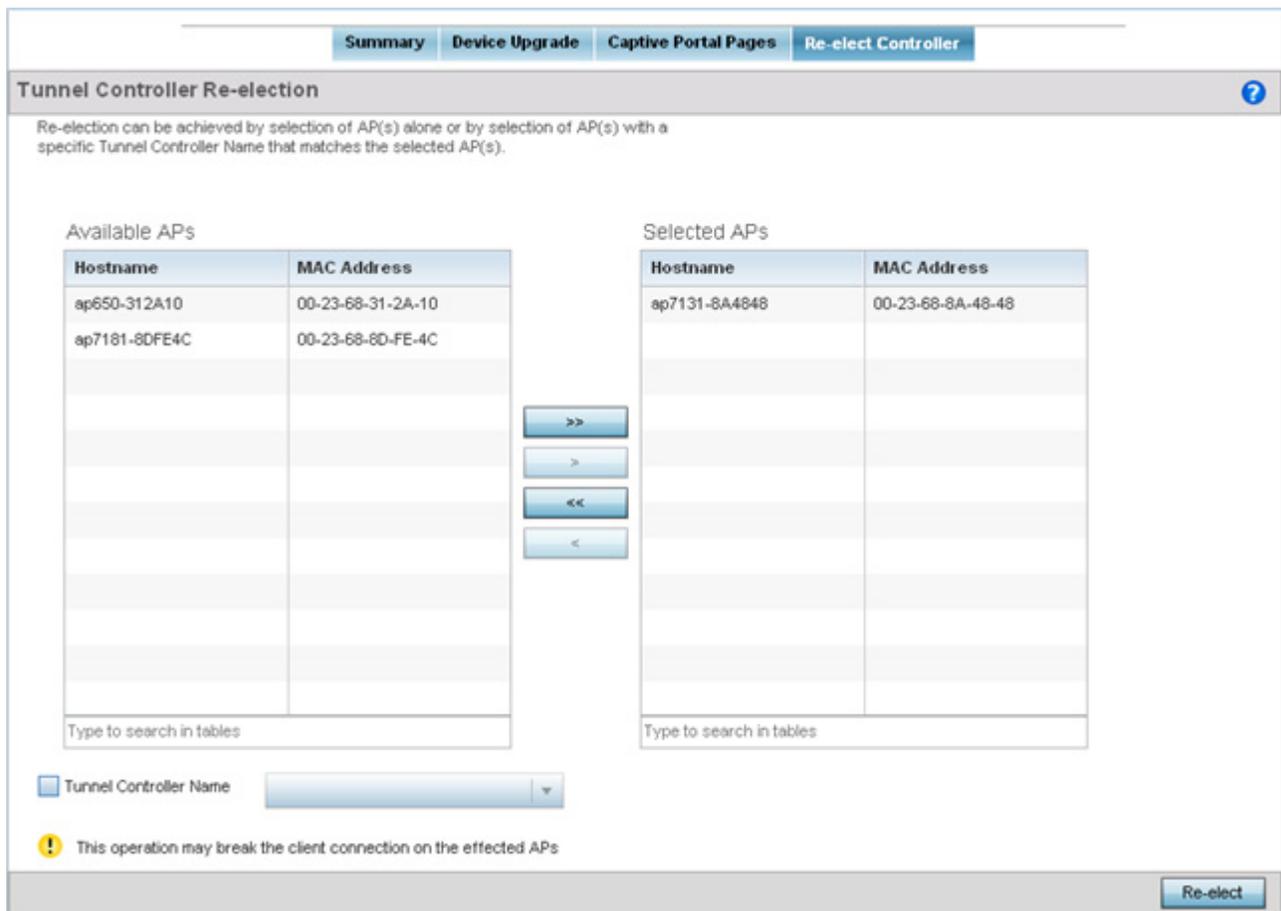
**NOTE:** Take care when selecting access points for controller re-election, as client connections may be broken on upon re-election. Ensure an elected access point's client load can be compensated by another access point in the same RF Domain.

To re-elect controller adoption resources for tunnel establishment:



**NOTE:** The **Re-elect Controller** tab is only available at the RF Domain level of the UI's hierarchal tree and is not available for access points.

1. Select **Operations**.
2. Ensure a **RF Domain** is selected from the Operations menu on the top, left-hand, side of the screen. Otherwise, the Re-elect Controller screen cannot be located, as it does not display at either the system or device levels of the hierarchal tree.
3. Select the **Re-elect Controller** tab.



**Figure 12-38** Re-elect Controller screen

4. Refer to the **Available APs** column, and use the > button to move the selected access point into the list of **Selected APs** available for RF Domain Manager candidacy. Use the >> button to move all listed access points into the Selected APs table. The re-election process can be achieved through the selection of an individual access point, or through the selection of several access points with a specific Tunnel Controller Name matching the selected access points.
5. Select **Re-elect** to designate the Selected AP(s) as resources capable of tunnel establishment.

## 12.2 Certificates

### ► [Security Configuration](#)

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a client to access resources, if properly configured. A RSA key pair must be generated on the client.

For more information on certification activities, refer to the following:

- [Certificate Management](#)
- [RSA Key Management](#)
- [Certificate Creation](#)
- [Generating a Certificate Signing Request \(CSR\)](#)

### 12.2.1 Certificate Management

#### ► [Certificates](#)

If not wanting to use an existing certificate or key with a selected device, an existing *stored* certificate can be leveraged from a different device for use with the target device. Device certificates can be imported and exported to a secure remote location for archive and retrieval as they are required for application to other managed devices.

To configure trustpoints for use with certificates:

1. Select **Operations**.
2. Select **Certificates**.

The screenshot displays the 'Certificate Management' window with the 'Manage Certificates' tab selected. On the left, a table titled 'All Certificates Details' shows a single entry:

Certificates Name	RSA Keys	Valid
default-trustpoint	CN=AP7131-00-23-68-11-E	05:03:2012 05:18:09 UTC

On the right, the 'Certificate Details' section provides the following information:

- Subject Name : CN=AP7131-00-23-68-11-E6-C4
- Alternate Subject Name :
- Issuer Name : CN=AP7131-00-23-68-11-E6-C4
- Serial Number : 070e
- RSA Key Used : default\_rsa\_key
- Is Self Signed :
- RSA Key Used :
- CRL Present :
- Is CA :

The 'Validity' section shows:

- Valid From : 05:03:2012 05:18:09 UTC
- Valid Until : 05:01:2022 05:18:09 UTC

The 'Certificate Authority (CA) Details' section is currently empty.

At the bottom right, there are three buttons: 'Import', 'Export', and 'Delete'.

**Figure 12-39** Certificate Management -Trustpoints screen

The **Trustpoints** screen displays for the selected MAC address.

3. Refer to the **Certificate Details** to review certificate properties, self-signed credentials, validity period and CA information.
4. Select the **Import** button to import a certificate.

**Import New Trustpoint**

Import ⓘ  
 Import CA ⓘ  
 Import CRL ⓘ  
 Import Signed Cert ⓘ

Trustpoint Name \*

**Location of Trustpoint**

From Network

Protocol **ftp** Port 21 **Basic**

Host 0 . 0 . 0 . 0 IP Address

User Name

Password

Path/File

OK Cancel

**Figure 12-40** Certificate Management - Import New Trustpoint screen

5. Define the following configuration parameters required for the **Import** of the Trustpoint:

<b>Import</b>	Select the type of Trustpoint to import. The following Trustpoints can be imported: <ul style="list-style-type: none"> <li>• <i>Import</i> – Select to import any trustpoint.</li> <li>• <i>Import CA</i> – Select to import a <i>Certificate Authority</i> (CA) certificate on to the access point.</li> <li>• <i>Import CRL</i> – Select to import a <i>Certificate Revocation List</i> (CRL), CRLs are used to identify and remove those installed certificates that have been revoked or are no longer valid.</li> <li>• <i>Import Signed Cert</i> – Select to import a self signed certificate.</li> </ul>
<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a *CA certificate*.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A *certificate revocation list* (CRL) is a list of revoked certificates, or certificates no longer valid. A certificate can be revoked if the CA improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

*Signed certificates* (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

6. Define the following configuration to import the Trustpoint from a location on the network. To do so, select **From Network** and provide the following information.

<b>URL</b>	Provide the complete URL to the location of the trustpoint. This option is available by default. Click the <i>Advanced</i> link next to this field to display more fields to provide detailed trustpoint location information.
<b>Protocol</b>	If using <i>Advanced</i> settings, select the protocol used for importing the target trustpoint. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If using <i>Advanced</i> settings, use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>IP Address</b>	If using <i>Advanced</i> settings, enter IP address of the server used to import the trustpoint. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .

<b>Hostname</b>	If using <i>Advanced</i> settings, provide the hostname of the server used to import the trustpoint. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If using <i>Advanced</i> settings, specify the path to the trustpoint. Enter the complete path to the file on the server.

7. Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
8. To optionally export a trustpoint to a remote location, select the **Export** button from the Trustpoints screen.

Once a certificate has been generated on the authentication server, export the self signed certificate. A digital CA certificate is different from a self signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an Active Directory Group Policy for automatic root certificate deployment.

Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

**Export Trustpoint**

**Trustpoint Details**

Trustpoint Name \* default-trustpoint

**Export Location**

To Network

Protocol: ftp Port: 21 **Basic**

Host: 0 . 0 . 0 . 0 IP Address

User Name

Password

Path/File

OK Cancel

**Figure 12-41** Certificate Management - Export Trustpoint screen

9. Define the following configuration parameters required for the **Export** of the trustpoint:

<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
<b>URL</b>	Provide the complete URL to the location of the trustpoint. If needed, select <i>Advanced</i> to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol.
<b>Protocol</b>	Select the protocol used for exporting the target trustpoint. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If using <i>Advanced</i> settings, use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>IP Address</b>	If using <i>Advanced</i> settings, enter IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Hostname</b>	If using <i>Advanced</i> settings, provide the hostname of the server used to export the trustpoint. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path</b>	If using <i>Advanced</i> settings, specify the path to the trustpoint. Enter the complete relative path to the file on the server.

10. Select **OK** to export the trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
11. To optionally delete a trustpoint, select the **Delete** button from the Trustpoints screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select the **Delete RSA Key** option to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the last saved configuration.

## 12.2.2 RSA Key Management

### ► Certificates

Refer to the RSA Keys screen to review existing RSA key configurations that have been applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import or export an existing key to and from a remote location.

*Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1. Select **Operations**.
2. Select **Certificates**.
3. Select **RSA Keys**.

The screenshot shows the 'RSA Keys' management screen. At the top, there are four tabs: 'Manage Certificates', 'RSA Keys', 'Create Certificate', and 'Create CSR'. Below the tabs is a header 'RSA Keys' with a question mark icon. The main content area is titled 'All Certificates Details' and contains a table with the following data:

RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgQDks5UoQxrpQFuq5sVJBPrLAp4/ EUYIDrG2FaphnqYSbbZlifoL4pMiS81bRk8pr7gMz0BK9Cg3TH/QsNaqRkVWVKZd OAsn1wOvOpTwhNsdLMWuGLgT3L2Oe2QaNIAdiOAlyW8lu79jnUM7but5ApPd4uZK L90Ls+tenw9t/st1XwIDAQAB -----END PUBLIC KEY-----

Below the table is a 'Certificate Details' section showing the same information for 'default\_rsa\_key'. At the bottom right of the interface are four buttons: 'Generate Key', 'Import', 'Export', and 'Delete'.

**Figure 12-42** Certificate Management - RSA Keys screen

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

4. Select **Generate Key** to create a new key with a defined size.

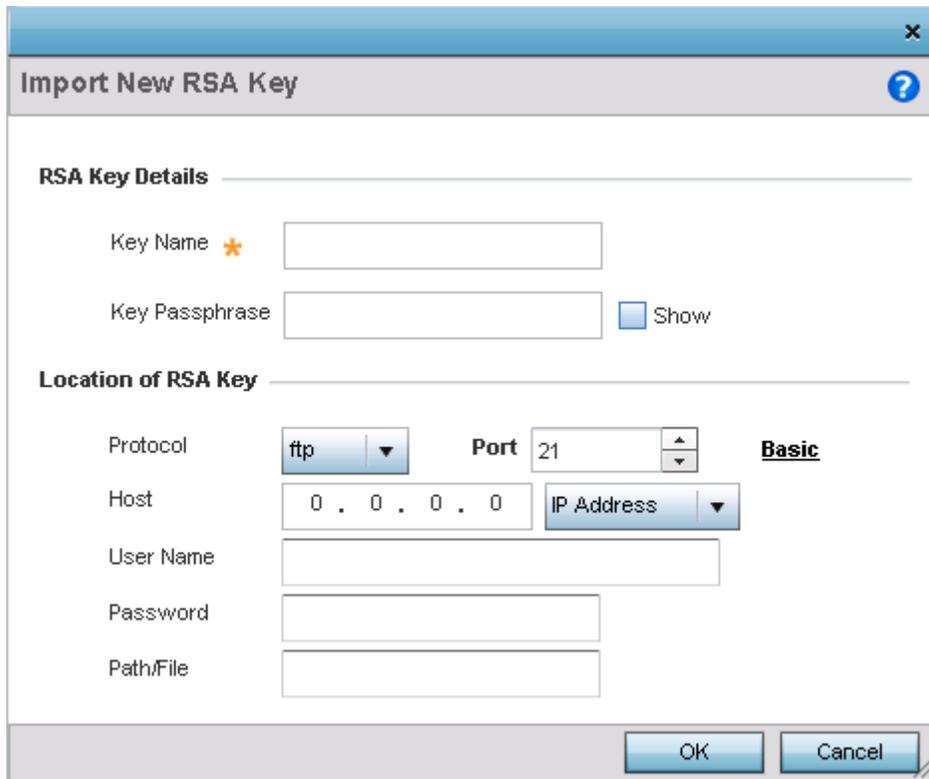


**Figure 12-43** Certificate Management - Generate RSA Key screen

5. Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Size</b>	Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality.

6. To optionally import a RSA Key, select the **Import** button from the RSA Keys screen.



**Figure 12-44** Certificate Management - Import New RSA Key screen

7. Define the following configuration parameters required for the import of the RSA key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to identify the RSA key.
<b>Key Passphrase</b>	Define the key used by the server (or repository) of the target RSA key. Select the <i>Show</i> textbox to expose the actual characters used in the passphrase. Leaving the option unselected displays the passphrase as a series of asterisks <i>***</i> .
<b>URL</b>	Provide the complete URL to the location of the RSA key. If needed, select <i>Advanced</i> to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol.
<b>Protocol</b>	Select the protocol used for importing the target key. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>IP Address</b>	Enter IP address of the server used to import the RSA key. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Hostname</b>	Provide the hostname of the server used to import the RSA key. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path</b>	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

8. Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.
9. To optionally export a RSA key to a remote location, select the **Export** button from the RSA Keys screen.
10. Export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

**Figure 12-45** Certificate Management - Export RSA Key screen

11. Define the following configuration parameters required for the Export of the RSA key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Passphrase</b>	Define the key passphrase used by the server. Select the <i>Show</i> textbox to expose the actual characters used in the passphrase. Leaving the option unselected displays the passphrase as a series of asterisks "***".
<b>URL</b>	Provide the complete URL to the location of the key. If needed, select <i>Advanced</i> to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is also dependent on the selected protocol.
<b>Protocol</b>	Select the protocol used for exporting the RSA key. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1</i></li> <li>• <i>usb2</i></li> <li>• <i>usb3</i></li> <li>• <i>usb4</i></li> </ul>
<b>Port</b>	If using <i>Advanced</i> settings, use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .

<b>IP Address</b>	If using <i>Advanced</i> settings, enter IP address of the server used to export the RSA key. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Hostname</b>	If using <i>Advanced</i> settings, provide the hostname of the server used to export the RSA key. This option is not valid for <i>cf</i> and <i>usb1 - 4</i> .
<b>Username/Password</b>	These fields are enabled if using <i>ftp</i> or <i>sftp</i> protocols. Specify the username and the password for that username to access the remote servers using these protocols.
<b>Path/File</b>	If using <i>Advanced</i> settings, specify the path to the key. Enter the complete relative path to the key on the server.

12. Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to the last saved configuration.
13. To optionally delete a key, select the **Delete** button from within the RSA Keys screen. Provide the key name within the Delete RSA Key screen and select the **Delete Certificates** option to remove the certificate the key supported. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the last saved configuration.

### 12.2.3 Certificate Creation

#### ► Certificates

The Certificate Management screen provides the facility for creating new self-signed certificates. Self signed certificates (often referred to as root certificates) do not use public or private CAs. A self signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate that can be applied to a device:

1. Select **Operations**.
2. Select **Certificates**.
3. Select **Create Certificate**.

**Figure 12-46** Certificate Management - Create Certificate screen

4. Define the following configuration parameters required to **Create New Self-Signed Certificate**:

<b>Certificate Name</b>	Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
<b>RSA Key: Create New</b>	To create a new RSA key, select the radio button to define 32 character name used to identify the RSA key. Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality. For more information on creating a new RSA key, see <a href="#">RSA Key Management on page 12-42</a> .
<b>RSA Key: Use Existing</b>	Select the radio button and use the drop-down menu to select the existing key used by both the access point and the server (or repository) of the target RSA key.

5. Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

<b>Certificate Subject Name</b>	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-configured</i> to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
<b>Country (C)</b>	Define the <i>Country</i> used in the certificate. This is a required field and must not exceed a 2 character country code.

<b>State (ST)</b>	Enter a State/Prov. for the state or province name used in the certificate. This is a required field.
<b>City (L)</b>	Enter a City to represent the city name used in the certificate. This is a required field.
<b>Organization (O)</b>	Define an Organization for the organization used in the certificate. This is a required field.
<b>Organizational Unit (OU)</b>	Enter an Org. Unit for the name of the organization unit used in the certificate. This is a required field.
<b>Common Name (CN)</b>	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

6. Select the following **Additional Credentials** required for the generation of the self signed certificate:

<b>Email Address</b>	Provide an E-mail address used as the contact address for issues relating to this certificate request.
<b>Domain Name)</b>	Enter a <i>fully qualified domain name</i> (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. A FQDN differs from a regular domain name by its absoluteness; as a suffix is not added.
<b>IP Address</b>	Specify the IP address used as the destination for certificate requests.

7. Select the **Generate Certificate** button at the bottom of the Create Certificate screen to produce the certificate.

## 12.2.4 Generating a Certificate Signing Request (CSR)

### ► Certificates

A *certificate signing request* (CSR) is a message from a requestor to a certificate authority to apply for a digital identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1. Select **Operations**.
2. Select **Certificates**.
3. Select **Create CSR**.

**Figure 12-47** Certificate Management - Create CSR screen

- Define the following configuration parameters required to **Create New Certificate Signing Request (CSR)**:

<b>RSA Key: Use Existing</b>	Select the radio button and use the drop-down menu to select the existing key used by both the access point and the server (or repository) of the target RSA key.
<b>RSA Key: Create New</b>	Create or use an existing key by selecting the appropriate radio button. Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality. For more information, see <a href="#">RSA Key Management on page 12-42</a> .

- Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

<b>Certificate Subject Name</b>	Select either the auto-generate radio button to automatically create the certificate's subject credentials or select user-defined to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
<b>Country (C)</b>	Define the Country used in the CSR. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.
<b>State (ST)</b>	Enter a State/Prov. for the state or province name used in the CSR. This is a required field.
<b>City (L)</b>	Enter a City to represent the city name used in the CSR. This is a required field.
<b>Organization (O)</b>	Define an Organization for the organization used in the CSR. This is a required field.

<b>Organizational Unit (OU)</b>	Enter an Org. Unit for the name of the organization unit used in the CSR. This is a required field.
<b>Common Name (CN)</b>	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

6. Select the following **Additional Credentials** required for the generation of the CSR:

<b>Email Address</b>	Provide an E-mail address used as the contact address for issues relating to this CSR.
<b>Domain Name)</b>	Enter a <i>fully qualified domain name</i> (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: somehost.example.com. An FQDN differs from a regular domain name by its absoluteness; as a suffix is not added.
<b>IP Address</b>	Specify the IP address used as the destination for certificate requests.

7. Select the **Generate CSR** button at the bottom of the screen to produce the CSR.



3. Refer to the following to determine whether Smart RF calibrations or interactive calibration is required:

<b>Hostname</b>	Displays the user friendly hostname assigned to each access point within the RF Domain. This value cannot be modified as a part of calibration activity.
<b>AP MAC Address</b>	Displays the hardware encoded MAC address assigned to each access point within the RF Domain. This value cannot be modified as past of a calibration activity.
<b>Radio MAC Address</b>	Displays the hardware encoded MAC address assigned to each access point radio within the RF Domain. This value cannot be modified as past of a calibration activity.
<b>Radio Index</b>	Displays a numerical index assigned to each listed access point radio when it was added to the network. This index helps distinguish this radio from others within the RF Domain with similar configurations. This value is not subject to change as a result of a calibration activity, but each listed radio index can be used in Smart RF calibration.
<b>Old Channel</b>	Lists the channel originally assigned to each listed access point within the RF Domain. This value may have been changed as part an Interactive Calibration process applied to the RF Domain. Compare this Old Channel against the Channel value to right of it (in the table) to determine whether a new channel assignment was warranted to compensate for a coverage hole.
<b>Channel</b>	Lists the current channel assignment for each listed access point, as potentially updated by an Interactive Calibration. Use this data to determine whether a channel assignment was modified as part of an Interactive Calibration. If a revision was made to the channel assignment, a coverage hole was detected on the channel as a result of a potentially failed or under performing access point radio within the RF Domain.
<b>Old Power</b>	Lists the transmit power assigned to each listed access point within the RF Domain. The power level may have been increased or decreased as part an Interactive Calibration process applied to the RF Domain. Compare this Old Power level against the Power value to right of it (in the table) to determine whether a new power level was warranted to compensate for a coverage hole.
<b>Power</b>	This column displays the transmit power level for the listed access point after an Interactive Calibration resulted in an adjustment. This is the new power level defined by Smart RF to compensate for a coverage hole.
<b>Smart Sensor</b>	Defines whether a listed access point is smart sensor on behalf of the other access point radios comprising the RF Domain.
<b>State</b>	Displays the current state of the Smart RF managed access point radio. Possible states include: <i>Normal</i> , <i>Offline</i> and <i>Sensor</i> .
<b>Type</b>	Displays the radio type (802.11an, 802.11ac, 802.11bgn etc.) of each listed access point radio within the RF Domain.

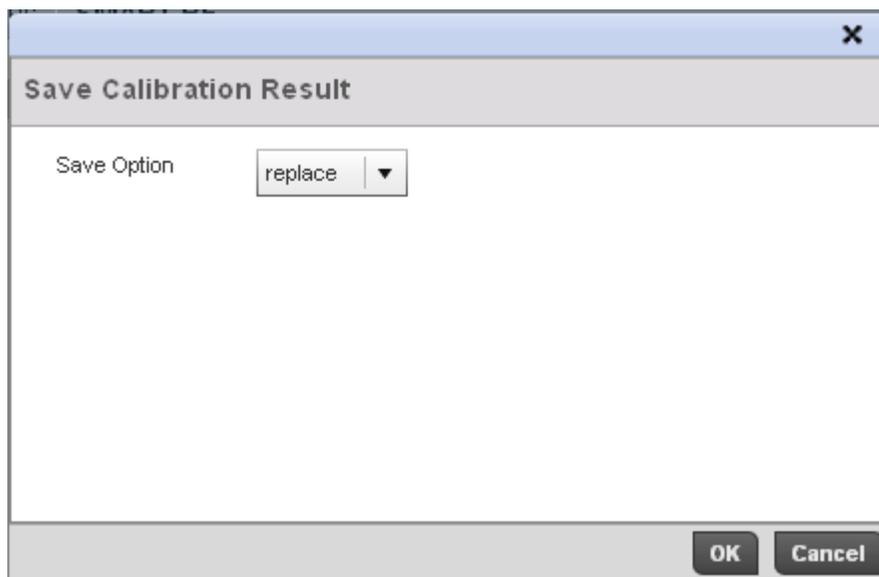
4. Select the **Refresh** button to (as required) to update the contents of the Smart RF screen and the attributes of the devices within the RF Domain.



**CAUTION:** Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections.

Select the **Interactive Calibration** button to initiate a Smart RF calibration using the access points within the RF Domain. The results of the calibration display within the Smart RF screen. Of particular interest are the channel and power adjustments made by the Smart RF module. Expand the screen to display the Event Monitor to track the progress of the Interactive Calibration.

5. Select **Calibration Result Actions** to define the actions taken based on the results of an Interactive Calibration. The results of an Interactive calibration are not applied to radios directly, the administrator has the choice to select one of following options.



**Figure 12-49** Save Calibration Result screen

- *Replace* - Only overwrites the current channel and power values with the new channel power values the Interactive Calibration has calculated.
  - *Write* - Writes the new channel and power values to the radios under their respective device configurations.
  - *Discard* - Discards the results of the Interactive Calibration without applying them to their respective devices.
  - *Commit* - Commits the Smart RF module Interactive Calibration results to their respective access point radios.
6. Select the **Run Calibration** option to initiate a calibration. New channel and power values are applied to radios, they are not written to the running-configuration. These values are dynamic and may keep changing during the course of the run-time monitoring and calibration the Smart RF module keeps performing to continually maintain good coverage. Unlike an Interactive Calibration, the Smart RF screen is not populated with the changes needed on access point radios to remedy a detected coverage hole. Expand the screen to display the Event Monitor to track the progress of the calibration.  
The calibration process can be stopped by selecting the **Stop Calibration** button.

## 12.4 Operations Deployment Considerations

Before defining the access point's configuration using the Operations menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- If an access point's (or its associated device's) firmware is older than the version on the support site, Motorola Solutions recommends updating to the latest firmware version for full functionality and utilization.
  - An access point must be rebooted to implement a firmware upgrade. Take advantage of the reboot scheduling mechanisms available to the access point to ensure its continuously available during anticipated periods of heavy wireless traffic utilization.
  - Within a well planned RF Domain, any associated radio should be reachable by at least one other radio. Keep this in mind when utilizing the Smart RF feature to record signals from neighboring access points. Access point to access point distance is recorded in terms of signal attenuation.
-



# CHAPTER 13

## STATISTICS

This chapter describes statistics displayed by the *graphical user interface* (GUI). Statistics are available for access point and their managed devices.

A Smart RF statistical history is available to assess adjustments made to device configurations to compensate for detected coverage holes or device failures.

Statistics display detailed information about peers, health, device inventories, wireless clients associations, adopted AP information, rogue APs and WLANs. Access point statistics can be exclusively displayed to validate connected access points, their VLAN assignments and their current authentication and encryption schemes.

Wireless client statistics are available for an overview of client health. Wireless client statistics includes RF quality, traffic utilization and user details. Use this information to assess if configuration changes are required to improve network performance.

For more information, see:

- [System Statistics](#)
  - [RF Domain Statistics](#)
  - [Access Point Statistics](#)
  - [Wireless Client Statistics](#)
-

## 13.1 System Statistics

### ► *Statistics*

The **System** screen displays information supporting managed devices. Use this information to assess the overall state of the devices comprising the system. Systems data is organized as follows:

- *Health*
- *Inventory*
- *Adopted Devices*
- *Pending Adoptions*
- *Offline Devices*
- *Device Upgrade*
- *Licenses*

### 13.1.1 Health

#### ► *System Statistics*

The *Health* screen displays the overall performance of the managed network (system). This includes device availability, overall RF quality, resource utilization and network threat perception.

To display the health of the network:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Health** from the left-hand side of the UI.

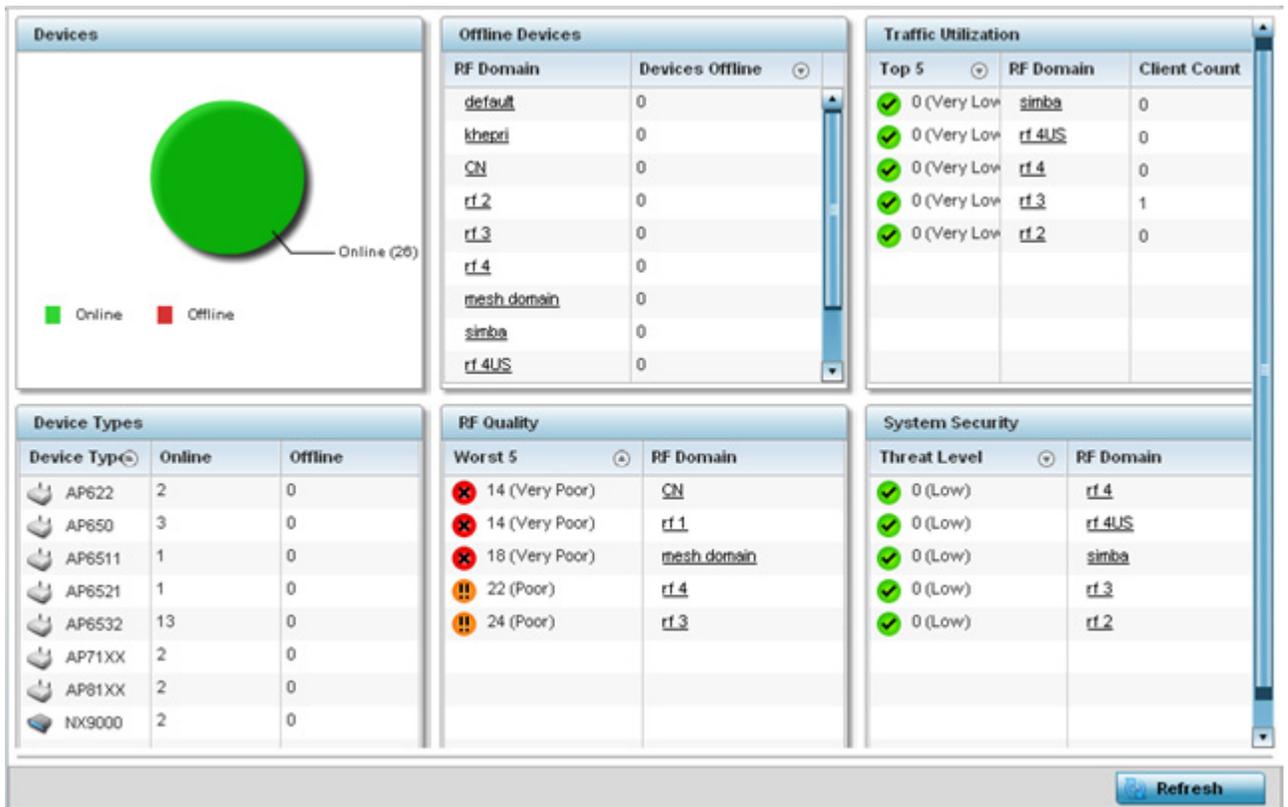


Figure 13-1 System - Health screen

- The **Devices** table displays the total number of devices in the network. The pie chart is a proportional view of how many devices are functional and currently online. Green indicates online devices and red offline devices detected within the network.
- The **Offline Devices** table displays a list of detected devices in the network that are currently offline but available as potential managed resources.  
The table displays the number of offline devices within each impacted RF Domain. Assess whether the configuration of a particular RF Domain is contributing to an excessive number of offline devices.
- The **Traffic Utilization** table displays the top 5 RF Domains with the most effective resource utilization. Utilization is dependent on the number of devices connected to the RF Domain.

<b>Top 5</b>	Displays the top 5 RF Domains in terms of usage index. Utilization index is a measure of how efficiently the domain is utilized. This value is defined as a percentage of current throughput relative to the maximum possible throughput. The values are: <ul style="list-style-type: none"> <li>• 0-20 – Very low utilization</li> <li>• 20-40 – Low utilization</li> <li>• 40-60 – Moderate utilization</li> <li>• 60 and above – High utilization</li> </ul>
<b>RF Domain</b>	Displays the name of the RF Domain.
<b>Client Count</b>	Displays the number of wireless clients associated with the RF Domain.

- The **Device Types** table displays the kinds of devices detected within the system. Each device type displays the number currently online and offline.

8. Use the **RF Quality** table to isolate poorly performing radio devices within specific RF Domains. This information is a starting point to improving the overall quality of the network. The **RF Quality** area displays the RF Domain performance. Quality indices are:

- 0 – 50 (Poor)
- 50 – 75 (Medium)
- 75 – 100 (Good).

The RF Quality field displays the following:

<b>Worst 5</b>	Displays five RF Domains with the lowest quality indices in the wireless controller managed network. The value can be interpreted as: <ul style="list-style-type: none"> <li>• 0-50 – Poor quality</li> <li>• 50-75 – Medium quality</li> <li>• 75-100 – Good quality</li> </ul>
<b>RF Domain</b>	Displays the name of the RF Domain wherein system statistics are polled for the poorly performing device.

9. The **Security** table defines a Threat Level as an integer value indicating a potential threat to the system. It's an average of the threat indices of all the RF Domains managed by the wireless controller.

<b>Threat Level</b>	Displays the threat perception value. This value can be interpreted as: <ul style="list-style-type: none"> <li>• 0-2 – Low threat level</li> <li>• 3-4 – Moderate threat level</li> <li>• 5 – High threat level</li> </ul>
<b>RF Domain</b>	Displays the name of the target RF Domain for which the threat level is displayed.

10. Select **Refresh** at any time to update the statistics counters to their latest values.

## 13.1.2 Inventory

### ▶ System Statistics

The *Inventory* screen displays information about the physical hardware managed within the system by its members. Use this information to assess the overall performance of wireless devices.

To display the inventory statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Inventory** from the left-hand side of the UI.

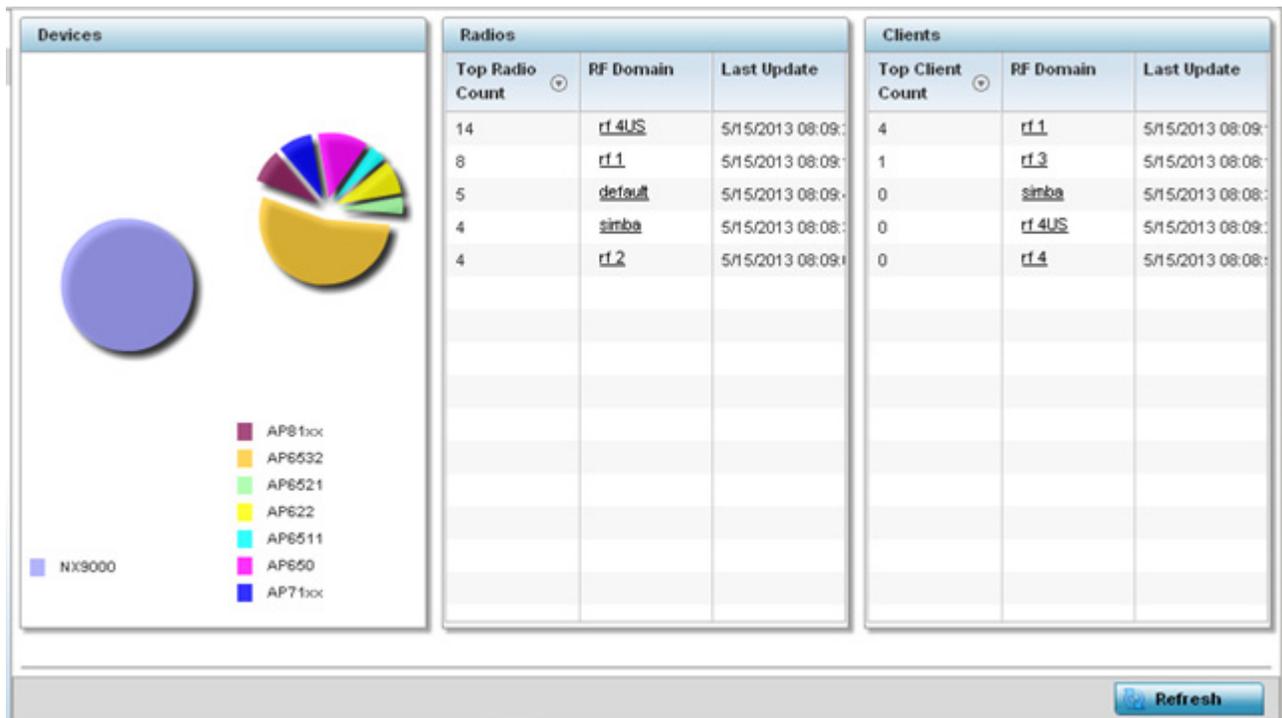


Figure 13-2 System - Inventory screen

- The **Devices** table displays an exploded pie chart depicting controller, service platform and access point device type distribution by model. Use this information to assess whether these are the correct models for the original deployment objective.
- The **Radios** table displays radios deployed within the network. This area displays the total number of managed radios and top 5 RF Domains in terms of radio count. The **Total Radios** value is the total number of radios in this system.

<b>Top Radio</b>	Displays the radios index of each listed top radio.
<b>RF Domain</b>	Displays the name of the RF Domain the listed radios belong. The RF Domain displays as a link that can be selected to display configuration and network address information in greater detail.
<b>Last Update</b>	Displays the UTC timestamp when each listed client was last seen on the network.

- The **Clients** table displays the total number of wireless clients managed by the access point. This **Top Client Count** table lists the top 5 RF Domains, in terms of the number of wireless clients adopted:

<b>Top Client</b>	Displays the client index of each listed top performing client.
<b>RF Domain</b>	Displays the name of the client RF Domain.
<b>Last Update</b>	Displays the UTC timestamp when the client count was last reported.

- Select **Refresh** to update the statistics counters to their latest values.

### 13.1.3 Adopted Devices

► *System Statistics*

The *Adopted Devices* screen displays a list of devices adopted to the network (entire system). Use this screen to view a list of devices and their current status.

To view adopted AP statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Adopted Devices** from the left-hand side of the UI.

	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Config Errors	Adopter Hostname	Adoption Time	Startup Time
▼	ap622-57F5F0	AP622	simba	AP-0622-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap622-5864A0	AP622	simba	AP-0622-6i	configured		rx9500-0C9848	Tue May 14	Tue May 14 20
▼	ap650-312908	AP65C	rf 4	AP-0650-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap650-3129EC	AP65C	rf 4	AP-0650-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap650-312A10	AP65C	default	AP-0650-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6511-8A4B15	AP651	rf 3	AP-6511-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6521-970C06	AP652	CN	AP-6521-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-3118E0	AP653	rf 2	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-34503C	AP653	rf 1	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347110	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-3475E4	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347638	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-34776C	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347800	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347830	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347854	AP653	mesh domain	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20
▼	ap6532-347B7C	AP653	rf 4US	AP-6532-6i	configured		rx9500-0C9848	Mon May 13	Mon May 13 20

Type to search in tables  Row Count: 24 [Refresh](#)

**Figure 13-3** System - Adopted Devices screen

The **Adopted Devices** screen provides the following:

<b>Adopted Device</b>	Displays administrator assigned hostname of the adopted device. Select the adopted device to display configuration and network address information in greater detail.
<b>Type</b>	Displays the adopted access point's model type.
<b>RF Domain Name</b>	Displays the domain the adopted AP has been assigned to. Select the RF Domain to display configuration and network address information in greater detail.
<b>Model Number</b>	Lists the model number of each AP that's been adopted since this screen was last refreshed.
<b>Config Status</b>	Displays the configuration file version in use by each listed adopted device. Use this information to determine whether an upgrade would increase the functionality of the adopted device.
<b>Config Errors</b>	Lists any errors encountered when the listed device was adopted.
<b>Adopter Hostname</b>	Lists the administrator hostname assigned to the adopting controller or service platform.
<b>Adoption Time</b>	Displays a timestamp for each listed device that reflects when the device was adopted by the controller or service platform.
<b>Startup Time</b>	Provides a date stamp when the adopted device was restarted post adoption.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.



<b>Add to Devices</b>	Select a listed AP and select the <i>Add to Devices</i> button to begin the adoption process for this detected AP.
<b>Refresh</b>	Click the <i>Refresh</i> button to update the list of pending adoptions.

### 13.1.5 Offline Devices

#### ► System Statistics

The *Offline Devices* screen displays a list of devices in the network or RF Domain that are currently offline. Review the contents of this screen to help determine whether an offline status is still warranted.

To view offline device potentially available for adoption:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Offline Devices** from the left-hand side of the UI.

Hostname	MAC Address	Type	RF Domain Name	Reporter	Area	Floor	Connected To	Last Update
ap622-57F5F	B4-C7-99-57	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap622-5864A	B4-C7-99-58	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap650-3129C	00-23-68-31	AP650	rf 4	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap650-3129E	00-23-68-31	AP650	rf 4	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap650-312A1	00-23-68-31	AP650	default	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6511-8A4E	5C-0E-8B-8A	AP6511	rf 3	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6521-970C	5C-0E-8B-97	AP6521	CN	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6522-5A84	B4-C7-99-5A	AP6522	default	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3118	00-23-68-31	AP6532	rf 2	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3450	5C-0E-8B-34	AP6532	rf 1	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3471	5C-0E-8B-34	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3475	5C-0E-8B-34	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3476	5C-0E-8B-34	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3477	5C-0E-8B-34	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM ▶
ap6532-3478	5C-0E-8B-34	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM ▶

Type to search in tables Row Count: 27

[Refresh](#)

**Figure 13-5** System - Offline Devices screen

The **Offline Devices** screen provides the following:

<b>Hostname</b>	Lists the administrator assigned hostname provided when the device was added to the network.
<b>MAC Address</b>	Displays the factory encoded MAC address of each listed offline device.
<b>Type</b>	Displays the offline access point's model type.
<b>RF Domain Name</b>	Displays the name of the offline device's RF Domain membership, if applicable. Select the RF Domain to display configuration and network address information in greater detail.
<b>Reporter</b>	Displays the hostname of the device reporting the listed device as offline. Select the reporting device name to display configuration and network address information in greater detail.

<b>Area</b>	Lists the administrator assigned deployment area where the offline device has been detected.
<b>Floor</b>	Lists the administrator assigned deployment floor where the offline device has been detected.
<b>Connected To</b>	Lists the offline's device's connected controller, service platform or peer model access point.
<b>Last Update</b>	Displays the date and time stamp of the last time the device was detected within the network. Click the arrow next to the date and time to toggle between standard time and UTC.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.

### 13.1.6 Device Upgrade

► *System Statistics*

The *Device Upgrade* screen displays available licenses for devices within a cluster. It displays the total number of AP licenses. To view a licenses statistics within the network:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Device Upgrade** from the left-hand side of the UI.

Upgraded By Device	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:51 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:32 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:30 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:31 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:00:42 AM	1	done
nx9500-0C9848	ap622	ap622-5864	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 03:59:45 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:47 AM	0	done
nx9500-0C9848	ap6532	ap6532-311	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:50 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:02 AM	1	done
nx9500-0C9848	ap81xx	ap8132-73B	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:18 AM	0	done
nx9500-0C9848	ap6532	ap6532-A65	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:23 AM	0	done
nx9500-0C9848	ap650	ap650-3129	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:38 AM	0	done
nx9500-0C9848	ap6511	ap6511-8A4	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:48 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:55 AM	0	done
nx9500-0C9848	ap6521	ap6521-970	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:22 AM	0	done
nx9500-0C9848	ap650	ap650-312A	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:47 AM	0	done
nx9500-0C9848	ao81xx	ao8132-73B	B4-C7-99-0C-98-48.1368	Start Upgrade	Mon May 13 2013 03:58:58 AM	3	failed

Figure 13-6 System - Device Upgrade screen

4. Select **Device Upgrade** from the left-hand side of the UI:

<b>Upgraded By Device</b>	Displays the MAC address of the controller, service platform or peer model access point that performed an upgrade.
<b>Type</b>	Displays the model type of the adopting controller, service platform or access point. An updating access point must be of the same model as the access point receiving the update.

<b>Device Hostname</b>	List the administrator assigned hostname of the device receiving an update.
<b>History ID</b>	Displays a unique timestamp for the upgrade event.
<b>Last Update Status</b>	Displays the initiation, completion or error status of each listed upgrade operation.
<b>Time Last Upgraded</b>	Lists the date and time of each upgrade operation.
<b>Retries Count</b>	Displays the number of retries required in an update operation.
<b>State</b>	Displays the done or failed state of an upgrade operation.
<b>Clear History</b>	Select <i>Clear History</i> to clear the screen of its current status and begin a new data collection.
<b>Refresh</b>	Select <i>Refresh</i> to update the screen's statistics counters to their latest values.

### 13.1.7 Licenses

#### ▶ *System Statistics*

The *Licenses* statistics screen displays available licenses for devices within a cluster. It displays the total number of AP licenses.

To view a licenses statistics within the network:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Licenses** from the left-hand side of the UI.

Summary
Details

**Local Licenses**

Cluster/ Hostnam..	AP Licenses Installed	Lent AP Licenses	Total AP Licenses	AP Licenses Usage	Remaining AP Licenses	AAP Licenses Installed	Lent AAP Licenses	Total AAP...	AAP Licenses Usage	Remaining AAP Licenses	Validity
10240	0	0	10240	0	10240	500	0	500	2	498	

**Global Licenses**

Cluster AP Adoption Licenses	0
Cluster Total AP Licenses	10276
Cluster AAP Adoption Licenses	2
Cluster Total AAP Licenses	836

**AP Licenses**

Cluster Maximum APs	0
---------------------	---

**Feature Licenses**

Hostname	Advanced Security	Advanced WIPS	Hotspot Analytics
rx9500-6C86AF	✗	✗	✓

Refresh

**Figure 13-7** System - Licenses screen

4. The **Local Licenses** table provides the following information:

<b>Cluster/Hostname</b>	Lists the administrator assigned cluster hostname whose license count and utilization is tallied in this <i>Local Licenses</i> table.
<b>AP Licenses Installed</b>	Lists the number of access point connections available to this device under the terms of the current license.
<b>Lent AP Licenses</b>	Displays the number of access point licenses lent (from a controller or service platform) to a cluster member to compensate for an access point's license deficiency.
<b>Total AP Licenses</b>	Displays the total number of access point connection licenses currently available to this device.
<b>AP License Usage</b>	Lists the number of access point connections currently utilized by this device out of the total available under the terms of the current license.
<b>Remaining AP Licenses</b>	Lists the remaining number of AP licenses available from the pooled license capabilities of all the members of the cluster.
<b>AAP Licenses Installed</b>	Lists the number of <i>Adaptive Access Point</i> connections available to this device under the terms of the current license.

<b>Lent AAP Licenses</b>	Displays the number of Adaptive Access Point licenses lent (from this device) to a cluster member to compensate for an access point licenses deficiency.
<b>Total AAP Licenses</b>	Displays the total number of Adaptive Access Point connection licenses currently available to this device.
<b>AAP Licenses Usage</b>	Lists the number of Adaptive Access Point connections currently utilized by this device out of the total available under the terms of the current license.
<b>Remaining AAP Licenses</b>	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
<b>Validity</b>	Displays validity information for the license's legal usage with the device.

5. The **Global Licenses** table provides the following information:

<b>Cluster AP Adoption Licenses</b>	Displays the current number of access point adoption licenses utilized by controller or service platform connected access points within a cluster.
<b>Cluster Total AP Licenses</b>	Displays the total number of access point adoption licenses available to controller or service platform connected access point within a cluster.
<b>Cluster AAP Adoption Licenses</b>	Displays the current number of Adaptive Access Point adoption licenses utilized by controller or service platform connected access point within a cluster.
<b>Cluster Total AAP Licenses</b>	Displays the total number of Adaptive Access Point adoption licenses available to controller or service platform connected access point within a cluster.

6. The **AP Licenses** table provides the following information:

<b>Cluster Maximum AP</b>	Lists the maximum number of access points permitted in a cluster under the terms of the current license.
---------------------------	--

7. The **Featured Licenses** area provides the following information:

<b>Hostname</b>	Displays the administrator assigned hostname of the controller, service platform or access point whose potentially implemented a advanced security or WIPS feature licenses.
<b>Advanced Security</b>	Displays whether the separately licensed Advanced Security application is installed for each hostname.
<b>Advanced WIPS</b>	Displays whether a separately licensed Advanced WIPS application is installed for each hostname.
<b>Hotspot Analytics</b>	Displays whether a separately licensed Analytics application is installed for supported NX9500 and NX9510 service platforms.

8. Select the **Details** tab.

Refer to the **Details** screen to further assess the total number of cluster member licenses available, cluster memberships, current utilization versus total licenses available, borrowed licenses, remaining licenses and license validity.

Refer to the following license utilization data:

<b>Cluster/Hostname</b>	Lists the administrator assigned cluster hostname whose license count and utilization is listed and tallied for access points.
<b>AP Licenses Installed</b>	Lists the number of access point connections available to this peer access point under the terms of the current license.
<b>Borrowed AP Licenses</b>	Displays the number of access point licenses temporarily borrowed from a cluster member to compensate for an AP license deficiency.
<b>Total AP Licenses</b>	Displays the total number of access point connection licenses currently available to clustered devices.
<b>AP Licenses Usage</b>	Lists the number of access point connections currently utilized out of the total available under the terms of current licenses.
<b>Remaining AP Licenses</b>	Lists the remaining number of AP licenses available from the pooled license capabilities of cluster members.
<b>AAP Licenses Installed</b>	Lists the number of Adaptive Access Point connections available under the terms of current licenses.
<b>Borrowed AAP Licenses</b>	Displays the number of Adaptive Access Point licenses temporarily borrowed from a cluster member to compensate for an AAP license deficiency.
<b>Total AAP Licenses</b>	Displays the total number of Adaptive Access Point connection licenses currently available to clustered devices.
<b>AAP Licenses Usage</b>	Lists the number of Adaptive Access Point connections currently utilized out of the total available under the terms of the current licenses.
<b>Remaining AAP Licenses</b>	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
<b>Validity</b>	Displays validity information for the license's legal usage by cluster member devices.
<b>Refresh</b>	Select <i>Refresh</i> to update the screen's statistics counters to their latest values.

## 13.2 RF Domain Statistics

### ► *Statistics*

The **RF Domain** screens display status for a selected RF domain. This includes the RF Domain *health* and *device inventory*, *wireless clients* and *Smart RF* functionality. RF Domains allow administrators to assign regional, regulatory and RF configuration to devices deployed in a common coverage area such as on a building floor, or site. Each RF Domain contains regional, regulatory and sensor server configuration parameters and may also be assigned policies that determine Access, SMART RF and WIPS configuration.

Use the following information to obtain an overall view of the performance of the selected RF Domain and troubleshoot issues with the domain or any member device.

- *Health*
- *Inventory*
- *Devices*
- *AP Detection*
- *Wireless Clients*
- *Device Upgrade*
- *Wireless LANs*
- *Radios*
- *Mesh*
- *Mesh Point*
- *SMART RF*
- *WIPS*
- *Captive Portal*

### 13.2.1 Health

#### ► *RF Domain Statistics*

The *Health* screen displays general status information for a selected RF Domain, including data polled from all its members.

To display the health of an access point's RF Domain:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Health** from the **RF Domain** menu.

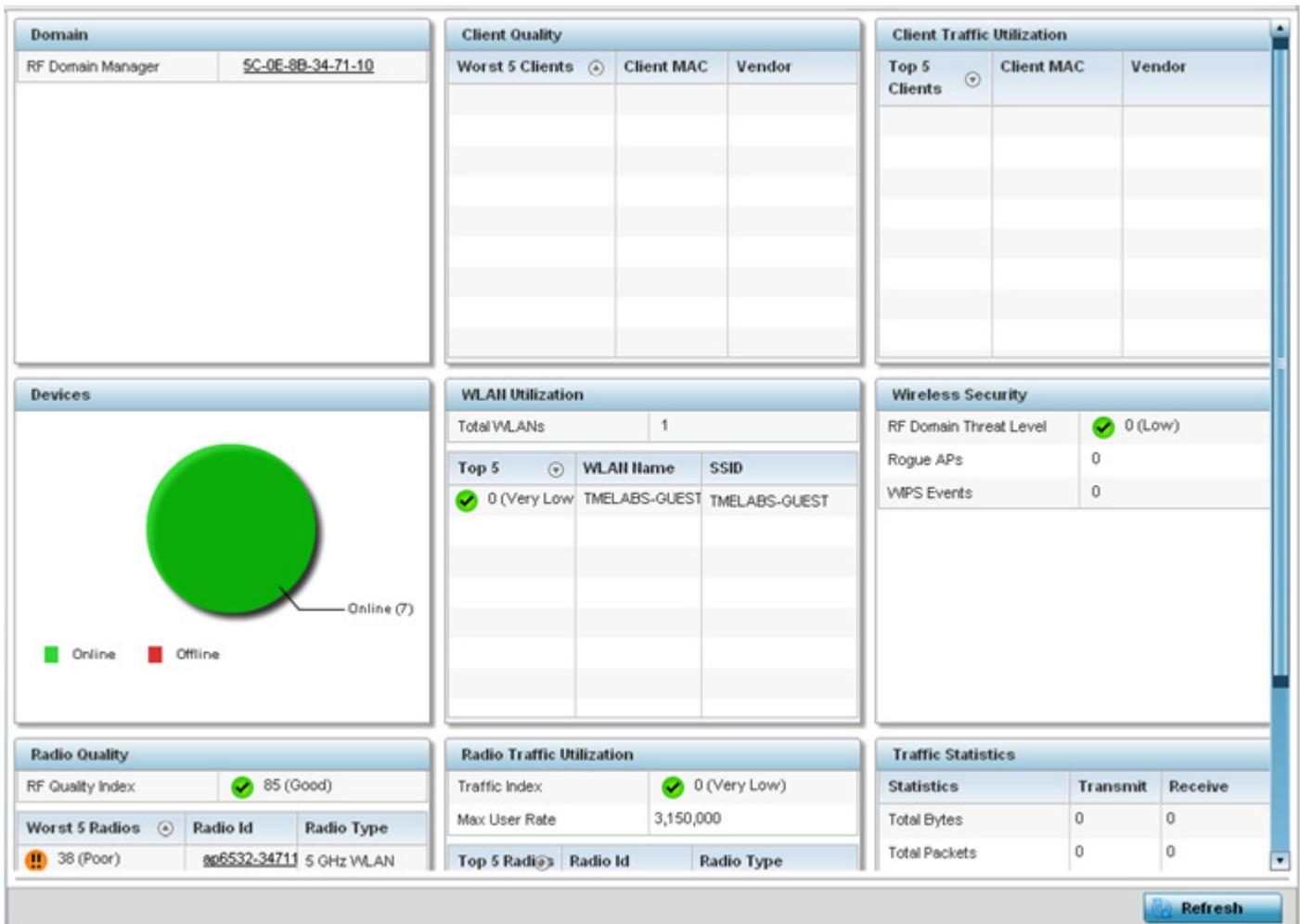


Figure 13-8 RF Domain - Health screen

- The **Domain** field displays the name of the RF Domain manager. The RF Domain manager is the focal point for the radio system and acts as a central registry of applications, hardware and capabilities. It also serves as a mount point for all the different pieces of the hardware system file.
- The **Devices** field displays the total number of online versus offline devices in the RF Domain, and an exploded pie chart depicts their status.
- The **Radio Quality** field displays information on the RF Domain's RF quality. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. This area also lists the worst 5 performing radios in the RF Domain.

The RF Quality Index can be interpreted as:

- 0-20 – Very poor quality
  - 20-40 – Poor quality
  - 40-60 – Average quality
  - 60-100 – Good quality
- Refer to the **Radio Quality** table for RF Domain member radios requiring administration to improve performance:

<b>Worst 5 Radios</b>	Displays five radios with the lowest average quality in the RF Domain.
-----------------------	--

<b>Radio ID</b>	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3).
<b>Radio Type</b>	Displays the radio type as either 5 GHz or 2.4 GHz.

8. Refer to the **Client Quality** table for RF Domain connected clients requiring administration to improve performance:

<b>Worst 5 Clients</b>	Displays the five clients having the lowest average quality indices.
<b>Client MAC</b>	Displays the hard coded radio MAC of the wireless client.
<b>Vendor</b>	Displays the vendor name of the wireless client.

9. Refer to the **WLAN Utilization** field to assess the following:

<b>Total WLANs</b>	Displays the total number of WLANs managed by RF Domain member access points.
<b>Top 5</b>	Displays the five RF Domain utilized WLANs with the highest average quality indices.
<b>WLAN Name</b>	Displays the WLAN Name for each of the Top 5 WLANs in the access point RF Domain.
<b>Radio Type</b>	Displays the radio type as either 5 GHz or 2.4 GHz.

10. The **Radio Traffic Utilization** area displays the following:

<b>Max. User Rate</b>	Displays the maximum recorded user rate in kbps.
<b>Top 5 Radios</b>	Displays five radios with the best average quality in the RF Domain.
<b>Radio ID</b>	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3).
<b>Radio Type</b>	Displays the radio type as either 5 GHz or 2.4 GHz.

11. Refer to the **Client Traffic Utilization** table:

<b>Top 5 Clients</b>	Displays the five clients having the highest average quality indices.
<b>Client MAC</b>	Displays the client's hard coded MAC address used a hardware identifier.
<b>Vendor</b>	Lists each client's manufacturer.

12. The **Wireless Security** area indicates the security of the transmission between WLANs and the wireless clients they support. This value indicates the vulnerability of the WLANs.

<b>RF Domain Threat Level</b>	Indicates the threat from the wireless clients trying to find network vulnerabilities within the access point RF Domain. The threat level is represented by an integer.
<b>Rogue APs</b>	Lists the number of unauthorized access points detected by RF domain member devices.
<b>WIPS Events</b>	Lists the number of WIPS events generated by RF Domain member devices.

13. The **Traffic Statistics** statistics table displays the following information for transmitted and received packets:

<b>Total Bytes</b>	Displays the total bytes of data transmitted and received within the access point RF Domain.
<b>Total Packets</b>	Lists the total number of data packets transmitted and received within the access point RF Domain.
<b>User Data Rate</b>	Lists the average user data rate within the access point RF Domain.
<b>Bcast/Mcast Packets</b>	Displays the total number of broadcast/multicast packets transmitted and received within the access point RF Domain.
<b>Management Packets</b>	This is the total number of management packets processed within the access point RF Domain.
<b>Tx Dropped Packets</b>	Lists total number of dropped data packets within the access point RF Domain.
<b>Rx Errors</b>	Displays the number of errors encountered during data transmission within the access point RF Domain. The higher the error rate, the less reliable the connection or data transfer.

14. The **SMART RF Activity** area displays the following:

<b>Time Period</b>	Lists the time period when Smart RF calibrations or adjustments were made to compensate for radio coverage holes or interference.
<b>Power Changes</b>	Displays the total number of radio transmit power changes that have been made using SMART RF within the access point RF Domain.
<b>Channel Changes</b>	Displays the total number of radio transmit channel changes that have been made using SMART RF within the access point RF Domain.
<b>Coverage Changes</b>	Displays the total number of radio coverage area changes that have been made using SMART RF within the access point RF Domain.

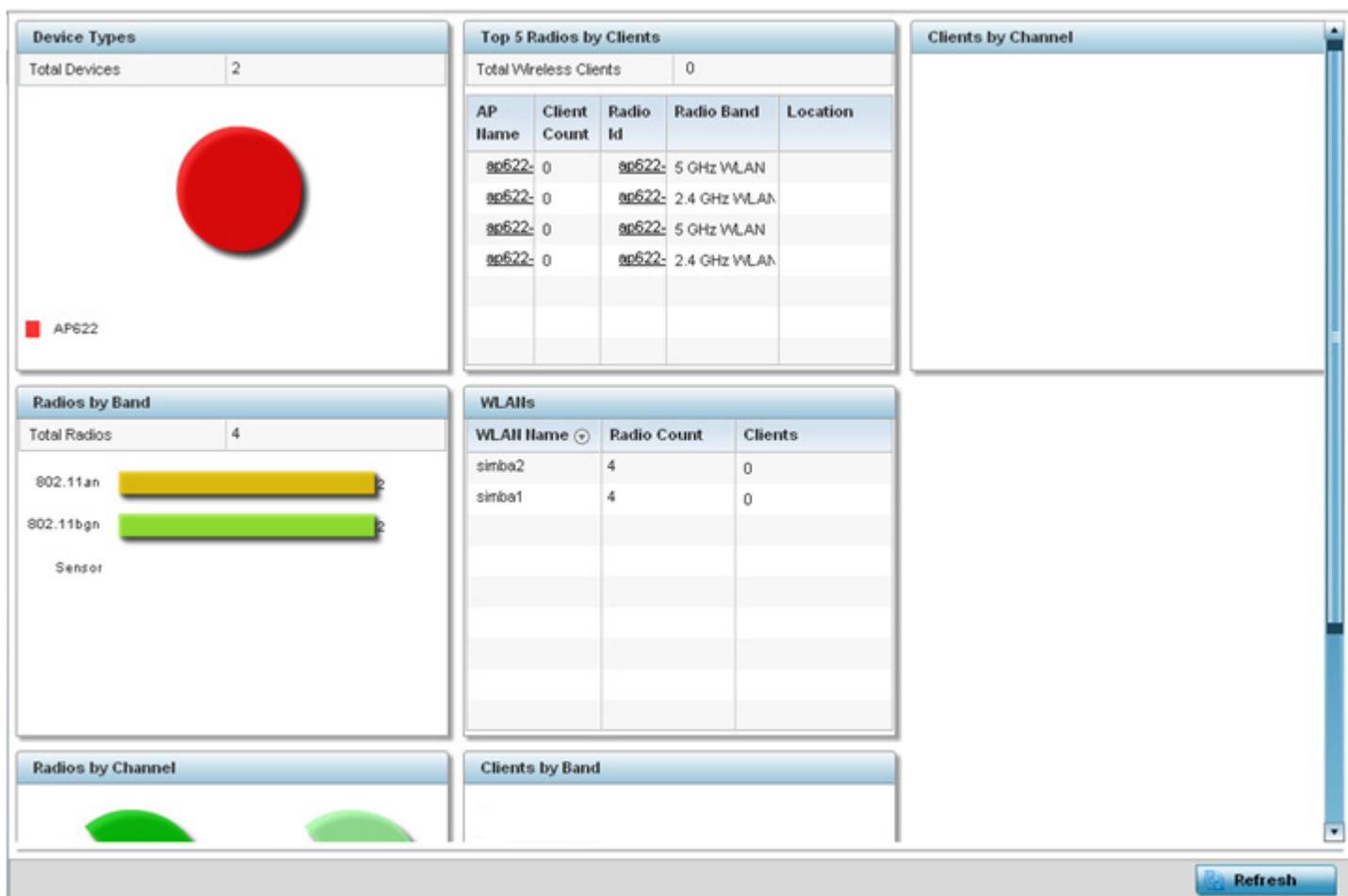
## 13.2.2 Inventory

### ▶ RF Domain Statistics

The *Inventory* screen displays an inventory of RF Domain member access points, connected wireless clients, wireless LAN utilization and radio availability.

To display RF Domain inventory statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Inventory** from the **RF Domain** menu.



**Figure 13-9** RF Domain - Inventory screen

- The **Device Types** table displays the total members in the RF Domain. The exploded pie chart depicts the distribution of RF Domain members by controller and access point model type.
- The **Radios by Band** field displays the total number of radios using 802.11acn and 802.11bgn bands within the RF Domain. The number of radios designated as sensors is also represented.
- The **Radios by Channel** field displays the radio channels utilized by RF Domain member devices in two separate charts. One chart displays for 5 GHz channels and the other for 2.4 GHz channels.
- The **Top 5 Radios by Clients** table displays the highest 5 performing wireless clients connected to RF Domain members.

<b>Total Wireless Clients</b>	Displays the total number of clients connected to RF Domain members.
<b>AP Name</b>	Displays the clients connected and reporting access point. The name displays as a link that can be selected to display access point data in greater detail.
<b>Client Count</b>	List the number of connected clients to each listed RF Domain member access point.
<b>Radio</b>	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 etc.).
<b>Radio Band</b>	Lists each client's operational radio band.
<b>Location</b>	Displays system assigned deployment location for the client.

8. Refer to the **WLANs** table to review RF Domain WLAN, radio and client utilization. Use this information to help determine whether the WLANs within this RF Domain have an optimal radio and client utilization.
9. The **Clients by Band** bar graph displays the total number of RF Domain member clients by their IEEE 802.11 radio type.
10. The **Clients by Channel** pie charts displays the channels used by RF Domain member clients using 5GHz and 2.4GHz radios.
11. Periodically select **Refresh** to update the contents of the screen to their latest values.

### 13.2.3 Devices

▶ *RF Domain Statistics*

The **Devices** screen displays RF Domain member hardware data, connected client counts, radio data and network IP address.

To display RF Domain member device statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Devices** from the **RF Domain** menu.

Device	AP MAC Address	Type	Client Count	Radio Count	IP Address
<a href="#">ap81xx-711630</a>	B4-C7-99-71-16-30	AP81XX	0	2	172.168.6.132
<a href="#">ap8132-73BE2C</a>	B4-C7-99-73-BE-2C	AP81XX	0	2	172.168.6.137

Type to search in tables Row Count: 2

[Refresh](#)

**Figure 13-10** RF Domain - Devices screen

<b>Device</b>	Displays the system assigned name of each device that's a member of the RF Domain. The name displays as a link that can be selected to display configuration and network address information in greater detail.
<b>AP MAC Address</b>	Displays each device's factory encoded MAC address as its hardware identifier.
<b>Type</b>	Displays each device model within the selected RF Domain.
<b>Client Count</b>	Displays the number of clients connected with each listed device. AP6532, AP6522, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models can support up to 256 clients per access point. AP6511 and AP6521 models can support up to 128 clients per access point.



<b>RSSI</b>	Displays the <i>Received Signal Strength Indicator</i> (RSSI) of the detected access point. Use this variable to help determine whether a device connection would improve network coverage or add noise.
<b>Reported by</b>	Displays the MAC address of the RF Domain member reporting the access point.
<b>Clear All</b>	Select <i>Clear All</i> to reset the statistics counters to zero and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

### 13.2.5 Wireless Clients

► *RF Domain Statistics*

The *Wireless Clients* screen displays device information for wireless clients connected to RF Domain member access points. Review this content to determine whether a client should be removed from access point association within the selected RF Domain.

To review a RF Domain’s connected wireless clients:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Wireless Clients** from the **RF Domain** menu.

	MAC Address	IP Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active	RF Domain Name
▼	<a href="#">00-40-96-AE-18-87</a>	32.32.0.88	motorola-4c3	ROLE4	Windows	Cisco Sy	11a	ap6532-A6f	5C-0E-8E	11Dtest	32	Sat May	rf 1
▼	<a href="#">38-16-D1-77-E8-5B</a>	32.32.0.91	38-16-D1-77	#system-	Android-	Samsung	11bgn	ap6532-A6f	5C-0E-8E	11Dtest	32	Sat May	rf 1
▼	<a href="#">40-83-DE-38-F6-68</a>	32.32.0.86	android-b28t	ROLE5	Appleph	Motorola	11an	ap6532-345	5C-0E-8E	11Dtest	32	Sat May	rf 1
▼	<a href="#">50-EA-D6-45-F4-C9</a>	32.32.0.90	Neerajs-iPho	ROLE5	Appleph	Apple Inc	11bgn	ap6532-A6f	5C-0E-8E	11Dtest	32	Sat May	rf 1
▼	<a href="#">A4-D1-D2-C0-A1-E3</a>	32.32.0.89	A4-D1-D2-C0	ROLE5	Appleph	Apple Inc	11bgn	ap6532-A6f	5C-0E-8E	11Dtest	32	Sat May	rf 1

Type to search in tables Row Count: 5

**Figure 13-12** RF Domain - Wireless Clients screen

The **Wireless Clients** screen displays the following:

<b>MAC Address</b>	Displays the hostname (MAC address) of each listed wireless client. This address is hard-coded at the factory and can not be modified. The hostname address displays as a link that can be selected to display configuration and network address information in greater detail.
<b>IP Address</b>	Displays the current IP address the wireless client is using for a network identifier.

<b>Hostname</b>	Displays the unique administrator assigned hostname when the client's configuration was originally set.
<b>Role</b>	Lists the role assigned to each controller, service platform or access point managed client.
<b>Client Identity</b>	Lists the client's operating system vendor identity (Android, Windows etc.)
<b>Vendor</b>	Displays the vendor (or manufacturer) of the wireless client.
<b>Band</b>	Lists the 2.4 or 5 GHz radio band the listed client is currently utilizing with its connected access point within the RF Domain.
<b>AP Hostname</b>	Displays the administrator assigned hostname of the access point to which the client is connected.
<b>Radio MAC</b>	Lists the hardware encoded MAC address of the access point radio to which the client is currently connected within the RF Domain.
<b>WLAN</b>	Displays the name of the WLAN the wireless client is currently using for its interoperation within the RF Domain.
<b>VLAN</b>	Displays the VLAN ID the client's connected access point has defined for use as a virtual interface.
<b>Last Active</b>	Displays the time when this wireless client was last detected by a RF Domain member.
<b>RF Domain Name</b>	Lists each client's RF Domain membership as defined by its connected access point.
<b>Disconnect All Clients</b>	Select the <i>Disconnect All Clients</i> button to terminate each listed client's connection and RF Domain membership.
<b>Disconnect Client</b>	Select a specific client MAC address and select the <i>Disconnect Client</i> button to terminate this client's connection and RF Domain membership.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

## 13.2.6 Device Upgrade

### ▶ [RF Domain Statistics](#)

The *Device Upgrade* screen reports information about devices receiving updates the RF Domain member provisioning the device. Use this screen to assess version data and upgrade status.

To view wireless device upgrade data for RF Domain members:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Device Upgrade** from the **RF Domain** menu.

Upgraded By Device	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1351858f	Reboot failed, re	Fri Nov 2 2012 05:39:37 AM	1	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1351858f	-	Fri Nov 2 2012 05:29:31 AM	0	done
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1346145f	-	Tue Aug 28 2012 02:39:53 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1346145f	-	Tue Aug 28 2012 02:39:41 AM	0	done
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345980f	-	Sun Aug 26 2012 04:51:35 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1345980f	-	Sun Aug 26 2012 04:50:26 AM	0	done
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345810f	-	Fri Aug 24 2012 05:32:42 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1345810f	-	Fri Aug 24 2012 05:32:19 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1345806f	-	Fri Aug 24 2012 04:06:22 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345806f	-	Fri Aug 24 2012 04:06:10 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345803f	-	Fri Aug 24 2012 03:37:29 AM	0	done
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345803f	-	Fri Aug 24 2012 03:37:22 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1345727f	-	Thu Aug 23 2012 06:20:06 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345727f	-	Thu Aug 23 2012 06:19:55 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6f	5C-0E-8B-34-50-3C.1345722f	-	Thu Aug 23 2012 05:10:10 AM	0	done
ap6532-34503C	ap6532	ap6532-311	5C-0E-8B-34-50-3C.1345722f	-	Thu Aug 23 2012 05:09:59 AM	0	done

Type to search in tables Row Count: 56

Figure 13-13 RF Domain - Device Upgrade screen

The **Device Upgrade** screen displays the following for RF Domain member devices:

<b>Upgraded By Device</b>	Lists the name of the device performing an update on behalf of a peer device.
<b>Type</b>	Displays the model of the device receiving an update. An updating access point must be of the same model as the access point receiving the update.
<b>Device Hostname</b>	Lists the administrator assigned hostname of each device receiving an update from a RF Domain member
<b>History Id</b>	Lists the RF Domain member device's MAC address along with a history ID appended to it for each upgrade operation.
<b>Last update Status</b>	Displays the last status message from the RF Domain member device performing the upgrade operation.
<b>Time Last Upgrade</b>	Displays a timestamp for the last successful upgrade.
<b>Retries Count</b>	Lists the number of retries needed for each listed RF Domain member update operation.
<b>State</b>	Lists whether the upgrade operation is completed, in-progress and whether an update was made without a device reboot.
<b>Clear History</b>	Select <i>Clear History</i> to remove the upgrade records for RF Domain member devices. Unlike the <i>Refresh</i> function (that updates existing data), <i>Clear History</i> removes the update record from the screen.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.



<b>Rx User Data Rate</b>	Displays the average data rate per user for packets received on each listed RF Domain member WLAN.
<b>Disconnect All Clients</b>	Select the <i>Disconnect All Clients</i> button to terminate each listed client's WLAN membership from this RF Domain.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

## 13.2.8 Radios

### ▶ RF Domain Statistics

The **Radio** screens displays information on RF Domain member access point radios. Use these screens to troubleshooting radio issues negatively impacting RF Domain performance.

For more information, refer to the following:

- [Status](#)
- [RF Statistics](#)
- [Traffic Statistics](#)

### 13.2.8.1 Status

To view the RF Domain radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Expand **Radios** from the **RF Domain** menu and select **Status**.

Radio	Radio MAC	Radio Type	Access Point	AP Type	State	Channel Current(Config)	Power Current(Config)	Clients
<a href="#">ap8132-738E2C.R1</a>	B4-C7-99-8B	2.4 GHz WLA	<a href="#">ap8132-738E2</a>	AP81XX	On	12 (smt)	17 (smt)	0
<a href="#">ap8132-738E2C.R2</a>	B4-C7-99-8B	5 GHz WLAN	<a href="#">ap8132-738E2</a>	AP81XX	On	104 (smt)	17 (smt)	0
<a href="#">ap81xx-711630.R1</a>	B4-C7-99-78	2.4 GHz WLA	<a href="#">ap81xx-71163</a>	AP81XX	On	1 (smt)	1 (smt)	0
<a href="#">ap81xx-711630.R2</a>	B4-C7-99-78	5 GHz WLAN	<a href="#">ap81xx-71163</a>	AP81XX	On	112 (smt)	17 (smt)	0

Type to search in tables Row Count: 4

[Refresh](#)

**Figure 13-15** RF Domain - Radio Status screen

The **Radio Status** screen displays the following:

<b>Radio</b>	Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that can be selected to display radio information in greater detail.
<b>Radio MAC</b>	Displays the MAC address as a numerical value factory hard coded to each listed RF Domain member access point radio.

<b>Radio Type</b>	Defines whether the radio is operating within the 2.4 or 5 GHz radio band.
<b>Access Point</b>	Displays the user assigned name of the RF Domain member access point to which the radio resides. AP7131N models can have from 1-3 radios depending on the SKU. AP6532, AP6522, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models have two radios, while AP6511 and AP6521 models have 1 radio. An ES6510 is a controller or service platform managed Ethernet Switch, with no embedded device radios.
<b>AP Type</b>	Lists the model type of each RF Domain member access point.
<b>State</b>	Displays the radio's current operational state.
<b>Channel Current (Config)</b>	Displays the current channel each listed RF Domain member access point radio is broadcasting on.
<b>Configured Channel</b>	Lists each radio's defined operating channel to help assess if the radio is no longer transmitting on its configured channel. Neighbor radios are often required to assist non-functioning peers in the same coverage area.
<b>Power Current (Config)</b>	Displays the current power level the radio is using for its transmissions.
<b>Configured Power</b>	Lists each radio's defined transmit power to help assess if the radio is no longer transmitting using its assigned power. Neighbor radios are often required to increase power to compensate for failed peer radios in the same coverage area.
<b>Clients</b>	Displays the number of clients currently connected to each listed RF Domain member access point radio. AP6522, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models can support up to 256 clients per radio. AP6511 and AP6521 models can support up to 128 clients per radio.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

### 13.2.8.2 RF Statistics

To view the RF Domain radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Expand **Radios** from the **RF Domain** menu and select **RF Statistics**.

Radio	Signal	Noise	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Avg. Retry Number	Error Rate	RF Quality Index
<a href="#">ap6521-970CC6.R1</a>	0 dbm	-87 dbm	0 db	0 Mbps	0 Mbps	0	41 pps	✔ 100 (Good)

Type to search in tables Row Count: 1

[Refresh](#)

**Figure 13-16** RF Domain - Radio RF Statistics screen

The **RF Statistics** screen displays the following:

<b>Radio</b>	Displays the name assigned to each listed RF Domain member radio. Each name displays as a link that can be selected to display radio information in greater detail.
<b>Signal</b>	Displays the power of listed RF Domain member radio signals in dBm.
<b>Noise</b>	Lists the level of noise (in - X dbm format) reported by each listed RF Domain member access point.
<b>SNR</b>	Displays the <i>signal to noise ratio</i> (SNR) of each listed RF Domain member radio.
<b>Tx Physical Layer Rate</b>	Displays the data transmit rate for each RF Domain member radio’s physical layer. The rate is displayed in Mbps.
<b>Rx Physical Layer Rate</b>	Displays the data receive rate for each RF Domain member radio’s physical layer. The rate is displayed in Mbps.
<b>Avg Retry Number</b>	Displays the average number of retries for each RF Domain member radio.
<b>Error Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
<b>RF Quality Index</b>	Displays an integer (and performance icon) that indicates the overall RF performance for each listed radio. The RF quality indices are: <ul style="list-style-type: none"> <li>• 0 – 50 (Poor)</li> <li>• 50 – 75 (Medium)</li> <li>• 75 – 100 (Good)</li> </ul>





<b>Portal Radio MAC</b>	Displays the hardware encoded MAC address for each radio in the RF Domain mesh network.
<b>Connect Time</b>	Displays the total connection time for each listed client in the RF Domain mesh network.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

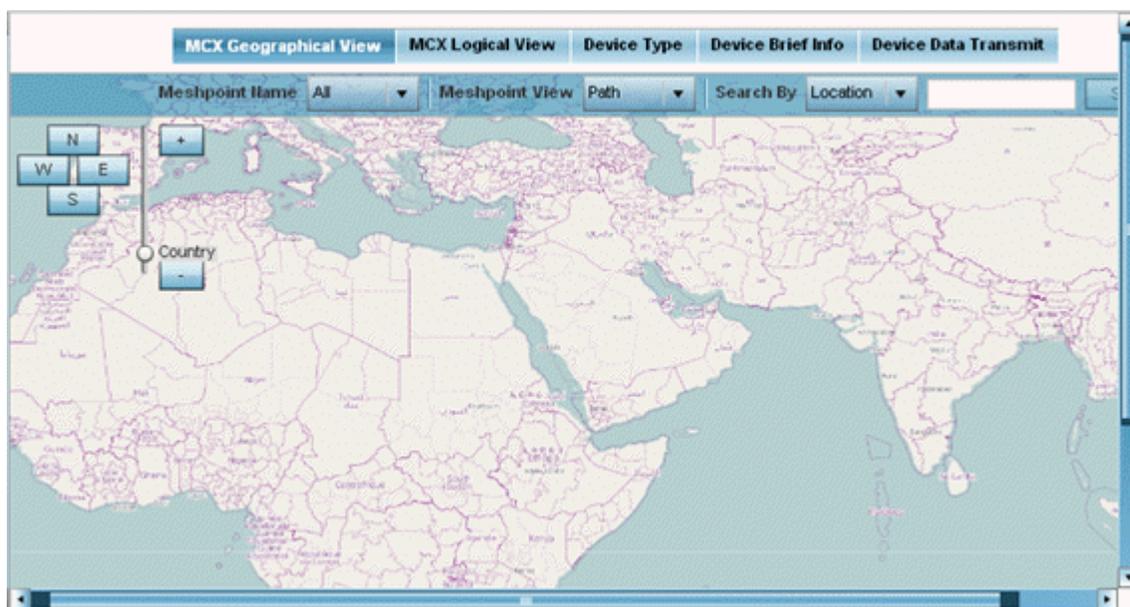
### 13.2.10 Mesh Point

#### ▶ RF Domain Statistics

To view *Mesh Point* statistics for RF Domain member access point and their connected clients:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **Mesh Point**.

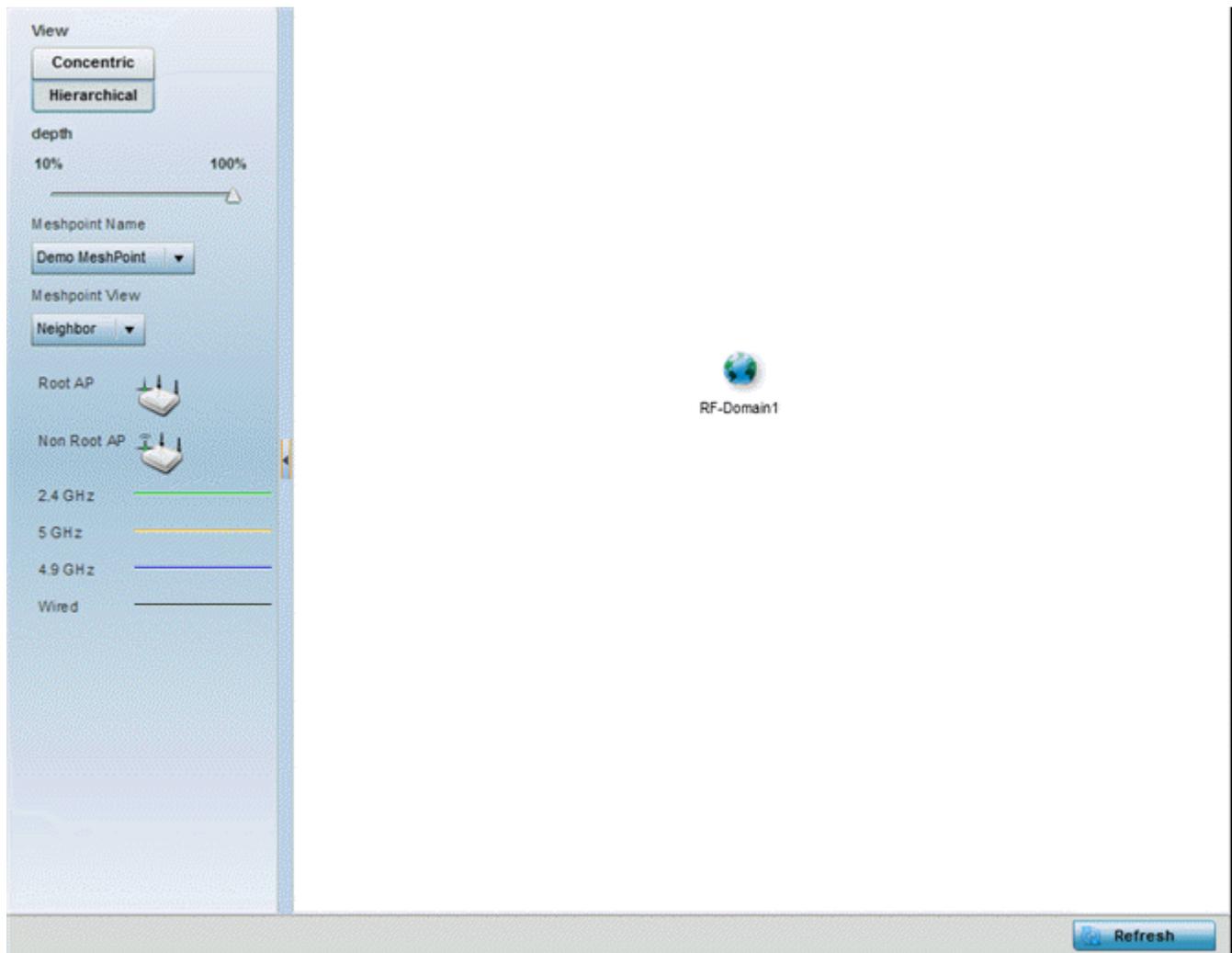
The **MCX Geographical View** displays by default.



**Figure 13-19** RF Domain - Mesh Point MCX Geographical View screen

The **MCX Geographical View** screen displays a map where icons of each device in the RF Domain is overlaid. This provides a geographical overview of the location of each RF Domain member device.

4. Use the *N*, *W*, *S* and *E* buttons to move the map in the North, East, West and South directions respectively. The slider next to these buttons enables zooming in and out of the view. The available fixed zoom levels are *World*, *Country*, *State*, *Town*, *Street* and *House*.
5. Use the **Maximize** button to maximize this view to occupy the complete screen. Use the **Refresh** button to update the status of the screen.
6. Select the **MCX Logical View** tab to view a logical representation of the mesh point.



**Figure 13-20** RF Domain - Mesh Point MCX Logical View screen

The **Concentric** and **Hierarchical** buttons define how the mesh point is displayed in the *MCX Logical View* screen. In the *Concentric* mode, the mesh is displayed as a concentric arrangement of devices with the root mesh at the centre and the other mesh device arranged around it.

In the *Hierarchical* arrangement, the root node of the mesh is displayed at the top of the mesh tree and the relationship of the mesh nodes are displayed as such.

Use the **Meshpoint Name** drop down to select a mesh point to see the graphical representation of that mesh point. The view can further be filtered based on the values *Neighbor* or *Path* selected in the **Meshpoint Type** field.

7. Select the **Device Type** tab.

Mesh Point Name	MAC	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Interface ID	Radio Interface	Next Hop IFID	Next Hops use time	Root Hops	Root MP ID	Root bound time	IFID Count
Demo MeshPoint	AA-11-00-00-00-00		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-00-00-00-00		13
Demo MeshPoint	AA-22-00-00-00-00		✗ No	✗ No	10-10-10-1					10-10-10-1	00-00-00-00-00-00		13
Demo MeshPoint	AA-11-00-00-00-00		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-00-00-00-00		13
Demo MeshPoint	AA-33-00-00-00-00		✗ No	✗ No	10-10-10-1					10-10-10-1	00-00-00-00-00-00		13
Demo MeshPoint	AA-44-00-00-00-00		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-00-00-00-00		13

**Figure 13-21** RF Domain - Mesh Point Device Type screen

The **Root** field displays the Mesh ID and MAC Address of the configured root mesh points in the RF Domain.

8. The **Non Root** field displays the Mesh ID and MAC Address of all configured non-root mesh points in the RF Domain.
9. The **Mesh Point Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>MAC</b>	Displays the MAC Address of each configured mesh point in the RF Domain.
<b>Hostname</b>	Displays the administrator assigned hostname for each configured mesh point in the RF Domain.
<b>Configured As Root</b>	Indicates whether a mesh point is configured to act as a root device. (Yes/No).
<b>Is Root</b>	A root mesh point is defined as a mesh point connected to the WAN and provides a wired backhaul to the network. (Yes/No)

<b>Meshpoint Identifier</b>	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
<b>Interface ID</b>	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.
<b>Radio Interface</b>	Uniquely identifies the radio interface on which the mesh point operates.
<b>Next Hop IFID</b>	Lists the ID of the interface on which the next hop for the mesh network can be found.
<b>Next Hops Use Time</b>	Lists the time when the next hop in the mesh network topology was last utilized.
<b>Root Hops</b>	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
<b>Root MP ID</b>	Displays the ID of the root device for this mesh point.
<b>Root Bound Time</b>	Displays the duration this mesh point has been connected to the mesh root.
<b>IFID Count</b>	Displays the number of <i>Interface IDs</i> (IFIDs) associated with all the configured mesh points in the RF Domain.

The **Path** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Meshpoint Identifier</b>	The identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Next Hop IFID</b>	The Interface ID of the mesh point that traffic is being directed to.
<b>Is Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
<b>MiNT ID</b>	Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain.
<b>Hops</b>	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
<b>Mobility</b>	Displays whether the mesh point is a mobile or static node. Displays <i>True</i> when the device is mobile and <i>False</i> when the device is not mobile.
<b>Metric</b>	A measure of the quality of the path. A lower value indicates a better path.
<b>State</b>	Indicates whether the path is currently <i>Valid</i> or <i>Invalid</i> .
<b>Binding</b>	Indicates whether the path is bound or unbound.
<b>Timeout</b>	The timeout interval in mili-seconds. The interpretation this value will vary depending on the value of the state.

<b>Sequence</b>	The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination.
-----------------	---

The **Root** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Recommended</b>	Displays the root that is recommended by the mesh routing layer.
<b>Root MPID</b>	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
<b>Next Hop IFID</b>	The IFID of the next hop. The IFID is the MAC Address on the destination device.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.
<b>Bound</b>	Indicates whether the root is bound or unbound.
<b>Metric</b>	Displays the computed path metric between the neighbor and their root mesh point.
<b>Interface Bias</b>	This field lists any bias applied because of <i>Preferred Root Interface Index</i> .
<b>Neighbor Bias</b>	This field lists any bias applied because of <i>Preferred Root Next-Hop Neighbor IFID</i> .
<b>Root Bias</b>	This field lists any bias applied because of <i>Preferred Root MPID</i> .

The **Multicast Path** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Subscriber Name</b>	The identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
<b>Subscriber MPID</b>	Lists the subscriber ID to distinguish between other mesh point neighbor devices in the RF Domain.
<b>Group Address</b>	Displays the MAC address used for the group in the mesh point.
<b>Timeout</b>	The timeout interval in seconds. The interpretation of this value will vary depending on the value of the state. If the state is <i>Init</i> or <i>In Progress</i> , the timeout duration has no significance. If the state is <i>Enabled</i> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <i>Failed</i> , the timeout duration is the amount of time after which the system will retry.

The **Neighbors** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	Displays the MeshID (MAC Address) of each mesh point in the RF Domain.

<b>Neighbor MP ID</b>	The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor.
<b>Neighbor IFID</b>	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
<b>Root MP ID</b>	The MAC Address of the neighbor's root mesh point.
<b>Is Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. <i>Yes</i> if the mesh point that is the neighbor is a root mesh point or <i>No</i> if the mesh point that is the neighbor is not a root mesh point.
<b>Mobility</b>	Displays whether the mesh point is a mobile or static node. Displays <i>True</i> when the device is mobile and <i>False</i> when the device is not mobile.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.
<b>Mesh Root Hops</b>	The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be <i>0</i> . If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be <i>1</i> . Each mesh point between the neighbor and its root mesh point is counted as 1 hop.
<b>Resourced</b>	Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays <i>True</i> when the device is resourced and <i>False</i> when the device is not.
<b>Link Quality</b>	An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest).
<b>Link Metric</b>	This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point.
<b>Root Metric</b>	The computed path metric between the neighbor and their root mesh point.

<b>Rank</b>	<p>The rank is the level of importance and is used for automatic resource management.</p> <p>8– The current next hop to the recommended root.</p> <p>7– Any secondary next hop to the recommended root to has a good potential route metric.</p> <p>6– A next hop to an alternate root node.</p> <p>5– A downstream node currently hopping through to get to the root.</p> <p>4– A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue).</p> <p>3– A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node.</p> <p>2– Reserved for active peer to peer routes and is not currently used.</p> <p>1 - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7.</p> <p>0– A neighbor bound to a different root node.</p> <p>-1 – Not a member of the mesh as it has a different mesh ID.</p> <p>All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.</p>
<b>Age</b>	Displays the number of mili seconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.
<b>Interface ID</b>	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.
<b>State</b>	<p>Displays the Link State for each mesh point:</p> <ul style="list-style-type: none"> <li>• <i>Init</i> - indicates the link has not been established or has expired.</li> <li>• <i>Enabled</i> - indicates the link is available for communication.</li> <li>• <i>Failed</i> - indicates the attempt to establish the link failed and cannot be retried yet.</li> <li>• <i>In Progress</i> - indicates the link is being established but is not yet available.</li> </ul>
<b>Timeout</b>	Displays the maximum value in seconds that the link is allowed to stay in the <i>In Progress</i> state before timing out.
<b>Keep Alive</b>	<i>Yes</i> indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). <i>No</i> indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

The **Proxy** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.

<b>Proxy Address</b>	Displays the MAC Address of the proxy used in the mesh point.
<b>Age</b>	Displays the age of the proxy connection for each of the mesh points in the RF Domain.
<b>Proxy Owner</b>	The owner's (MPID) is used to distinguish the neighbor device.
<b>Persistence</b>	Displays the persistence (duration) of the proxy connection for each of the mesh points in the RF Domain.
<b>VLAN</b>	The VLAN ID used as a virtual interface with this proxy. A value of <i>4095</i> indicates that there is no VLAN ID.

10. Select the **Device Brief Info** tab from the top of the screen.

The *Device Brief Info* screen is divided into 2 fields, **All Roots and Mesh Points** and **MeshPoint Details**.

**All Roots and Mesh Points**

MAC	Mesh Point Name	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Root Hops	IFID Count
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-22-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-44-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-55-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13

RowCount: 10

**MeshPoint Details**

AA-11-00-00-00-00 Hostname **General** | Path | Root | Multicast Path | Neighbors | Security | Proxy

Mesh Point Name	MAC	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Next Hop IFID	Next Hops use time	Root Hops	Root MP ID	Root bound time	IFID Count
Demo MeshP	AA-11-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13
Demo MeshP	AA-22-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	00-00-00-00-		13
Demo MeshP	AA-11-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13

Refresh

Figure 13-22 RF Domain - Mesh Point Device Brief Info screen

The **All Roots and Mesh Points** field displays the following:

<b>MAC</b>	Displays the MAC Address of each configured mesh point in the RF Domain.
<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.

<b>Hostname</b>	Displays the administrator assigned hostname for each configured mesh point in the RF Domain.
<b>Configured as Root</b>	A root mesh point is defined as a mesh point connected to the WAN, providing a wired backhaul to the network (Yes/No).
<b>Is Root</b>	Indicates whether the current mesh point is a root mesh point (Yes/No).
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Root Hops</b>	The number of devices between the selected mesh point and the destination device.
<b>IFID Count</b>	Displays the number of Interface IDs (IFIDs) associated with all the configured mesh points in the RF Domain.

11. The **MeshPoint Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>MAC</b>	Displays the MAC Address of each configured mesh point in the RF Domain.
<b>Hostname</b>	Displays the hostname for each configured mesh point in the RF Domain.
<b>Configured as Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. (Yes/No)
<b>Is Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. (Yes/No)
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Interface ID</b>	Uniquely identifies an interface associated with the ID. Each mesh point on a device can be associated with one or more interfaces.
<b>Root Interface</b>	Lists the radio interface on which the mesh point operates.
<b>Next Hop IFID</b>	Identifies the ID of the interface on which the next hop for the mesh network can be found.
<b>Next Hops Use Time</b>	Lists the time when the next hop in the mesh network topology was last utilized.
<b>Root Hops</b>	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
<b>Root MP ID</b>	Lists the interface ID of the interface on which the next hop for the mesh network can be found.
<b>Root Bound time</b>	Displays the duration this mesh point has been connected to the mesh root.
<b>IFID Count</b>	Displays the number of <i>Interface IDs</i> (IFIDs) associated with all the configured mesh points in the RF Domain.

The **Path** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Destination</b>	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
<b>Is Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
<b>MiNT ID</b>	Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain.
<b>Next Hop IFID</b>	The Interface ID of the mesh point that traffic is being directed to.
<b>Hops</b>	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
<b>Mobility</b>	Displays whether the mesh point is a mobile or static node. Displays <i>True</i> when the device is mobile and <i>False</i> when the device is not mobile.
<b>Metric</b>	A measure of the quality of the path. A lower value indicates a better path.
<b>State</b>	Indicates whether the path is currently Valid or Invalid.
<b>Binding</b>	Indicates whether the path is bound or unbound.
<b>Timeout</b>	The timeout interval in seconds. The interpretation this value will vary depending on the value of state. If the state is <i>Init</i> or <i>In Progress</i> , the timeout duration has no significance. If the state is <i>Enabled</i> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <i>Failed</i> , the timeout duration is the amount of time after which the system will retry.
<b>Sequence</b>	The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination.

The **Root** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Recommended</b>	Displays the root that is recommended by the mesh routing layer.
<b>Root MPID</b>	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
<b>Next Hop IFID</b>	The IFID of the next hop. The IFID is the MAC address on the destination device.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.

<b>Bound</b>	Indicates whether the root is <i>bound</i> or <i>unbound</i> .
<b>Metric</b>	Displays the computed path metric between the neighbor and their root mesh point.
<b>Interface Bias</b>	This field lists any bias applied because of preferred root Interface Index.
<b>Neighbor Bias</b>	This field lists any bias applied because of preferred root next-hop Neighbor IFID.
<b>Root Bias</b>	This field lists any bias applied because of preferred root MPID.

The **Multicast Path** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Subscriber Name</b>	Lists the subscriber name is used to distinguish between other mesh point neighbors both on the same device and on other devices.
<b>Subscriber MPID</b>	Lists the subscriber ID to distinguish between other mesh point neighbors both on the same device and on other devices.
<b>Group Address</b>	Displays the MAC address used for the group in the mesh point.
<b>Path Timeout</b>	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is <i>Init</i> or <i>In Progress</i> , the timeout duration has no significance. If the state is <i>Enabled</i> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <i>Failed</i> , the timeout duration is the amount of time after which the system will retry.

The **Neighbors** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Neighbor MP ID</b>	The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor.
<b>Neighbor IFID</b>	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
<b>Root MP ID</b>	The mesh point ID of the neighbor's root mesh point.
<b>Is Root</b>	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. <i>Yes</i> if the mesh point that is the neighbor is a root mesh point or <i>No</i> if the mesh point that is the neighbor is not a root mesh point.
<b>Mobility</b>	Displays whether the mesh point is a mobile or static node. Displays <i>True</i> when the device is mobile and <i>False</i> when the device is not mobile.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.

<b>Mesh Root Hops</b>	The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be <i>0</i> . If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be <i>1</i> . Each mesh point between the neighbor and its root mesh point is counted as 1 hop.
<b>Resourced</b>	Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays <i>True</i> when the device is resourced and <i>False</i> when the device is not.
<b>Link Quality</b>	An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest).
<b>Link Metric</b>	This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point.
<b>Root Metric</b>	The computed path metric between the neighbor and their root mesh point.
<b>Rank</b>	The rank is the level of importance and is used for automatic resource management. 8– The current next hop to the recommended root. 7– Any secondary next hop to the recommended root to has a good potential route metric. 6– A next hop to an alternate root node. 5– A downstream node currently hopping through to get to the root. 4 – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue). 3– A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node. 2– Reserved for active peer to peer routes and is not currently used. 1 - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7. 0– A neighbor bound to a different root node. -1 – Not a member of the mesh as it has a different mesh ID. All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.
<b>Age</b>	Displays the number of mili seconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

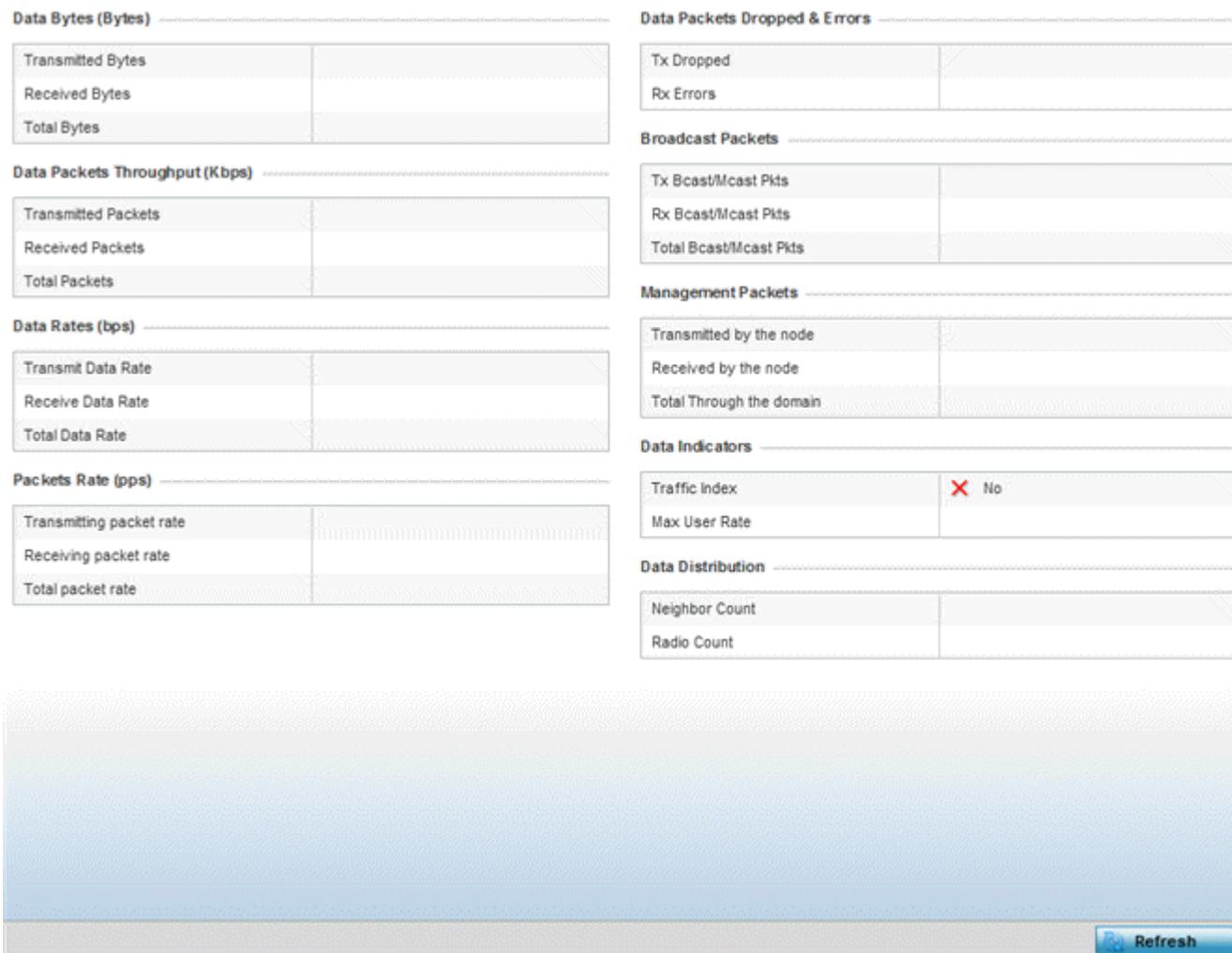
<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Radio Interface</b>	This indicates the interface that is used by the device to communicate with this neighbor. The values are <i>2.4</i> and <i>5.0</i> , indicating the frequency of the radio that is used to communicate with the neighbor.
<b>Interface ID</b>	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.

<b>State</b>	Displays the Link State for each mesh point: <ul style="list-style-type: none"> <li>• <i>Init</i> - indicates the link has not been established or has expired.</li> <li>• <i>Enabled</i> - indicates the link is available for communication.</li> <li>• <i>Failed</i> - indicates the attempt to establish the link failed and cannot be retried yet.</li> <li>• <i>In Progress</i> - indicates the link is being established but is not yet available.</li> </ul>
<b>Timeout</b>	Displays the maximum value in seconds that the link is allowed to stay in the <i>In Progress</i> state before timing out.
<b>Keep Alive</b>	<i>Yes</i> indicates the local MP acts as a supplicant to authenticate the link and not let it expire (if possible). <i>No</i> indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

The **Proxy** tab displays the following:

<b>Mesh Point Name</b>	Displays the name of each configured mesh point in the RF Domain.
<b>Destination Addr</b>	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
<b>Proxy Address</b>	Displays the MAC Address of the proxy used in the mesh point.
<b>Age</b>	Displays the age of the proxy connection for each of the mesh points in the RF Domain.
<b>Proxy Owner</b>	The owner (MPID) is used to distinguish the device that is the neighbor.
<b>VLAN</b>	The VLAN ID used as a virtual interface with this proxy. A value of <i>4095</i> indicates that there is no VLAN ID.

12. Select **Device Data Transmit**.



**Figure 13-23** RF Domain - Mesh Point Device Data Transmit screen

Review the following transmit and receive statistics for Mesh nodes:

<b>Data Bytes (Bytes): Transmitted Bytes</b>	Displays the total amount of data, in Bytes, that has been transmitted by mesh points in the RF Domain.
<b>Data Bytes (Bytes): Received Bytes</b>	Displays the total amount of data, in Bytes, that has been received by mesh points in the RF Domain.
<b>Data Bytes (Bytes): Total Bytes</b>	Displays the total amount of data, in Bytes, that has been transmitted and received by mesh points in the RF Domain.
<b>Data Packets Throughput (Kbps): Transmitted Packets</b>	Displays the total amount of data, in packets, transmitted by mesh points in the RF Domain.
<b>Data Packets Throughput (Kbps): Received Packets</b>	Displays the total amount of data, in packets, received by mesh points in the RF Domain.
<b>Data Packets Throughput (Kbps): Total Packets</b>	Displays the total amount of data, in packets, transmitted and received by mesh points in the RF Domain.

<b>Data Rates (bps): Transmit Data Rate</b>	Displays the average data rate, in kbps, for all data transmitted by mesh points in the RF Domain.
<b>Data Rates (bps): Receive Data Rate</b>	Displays the average data rate, in kbps, for all data received by mesh points in the RF Domain.
<b>Data Rates (bps): Total Data Rate</b>	Displays the average data rate, in kbps, for all data transmitted and received by mesh points in the RF Domain.
<b>Packets Rate (pps): Transmitting Packet rate</b>	Displays the average packet rate, in packets per second, for all data transmitted and received by mesh points in the RF Domain.
<b>Packets Rate (pps): Received Packet rate</b>	Displays the average packet rate, in packets per second, for all data received and received by mesh points in the RF Domain.
<b>Packets Rate (pps): Total Packet Rate</b>	Displays the average data packet rate, in packets per second, for all data transmitted and received by mesh points in the RF Domain.
<b>Data Packets Dropped and Errors: Tx Dropped</b>	Displays the total number of transmissions that were dropped mesh points in the RF Domain.
<b>Data Packets Dropped and Errors: Rx Errors</b>	Displays the total number of receive errors from mesh points in the RF Domain.
<b>Broadcast Packets: Tx Bcast/Mcast Pkts</b>	Displays the total number of broadcast and multicast packets transmitted from mesh points in the RF Domain.
<b>Broadcast Packets: Rx Bcast/Mcast Pkts</b>	Displays the total number of broadcast and multicast packets received from mesh points in the RF Domain.
<b>Broadcast Packets: Total Bcast/Mcast Pkts</b>	Displays the total number of broadcast and multicast packets transmitted and received from mesh points in the RF Domain.
<b>Management Packets: Transmitted by the node</b>	Displays the total number of management packets transmitted through the mesh point node.
<b>Management Packets: Received by the node</b>	Displays the total number of management packets received through the mesh point node.
<b>Management Packets: Total Through the domain</b>	Displays the total number of management packets that were transmitted and received through the mesh point node.
<b>Data Indicators: Traffic Index</b>	Displays <i>True</i> or <i>False</i> to indicate whether or not a traffic index is present.
<b>Data Indicators: Max User Rate</b>	Displays the maximum user throughput rate for mesh points in the RF Domain.
<b>Data Distribution: Neighbor Count</b>	Displays the total number of neighbors known to the mesh points in the RF Domain.
<b>Data Distribution: Neighbor Count</b>	Displays the total number of neighbor radios known to the mesh points in the RF Domain.

### 13.2.11 SMART RF

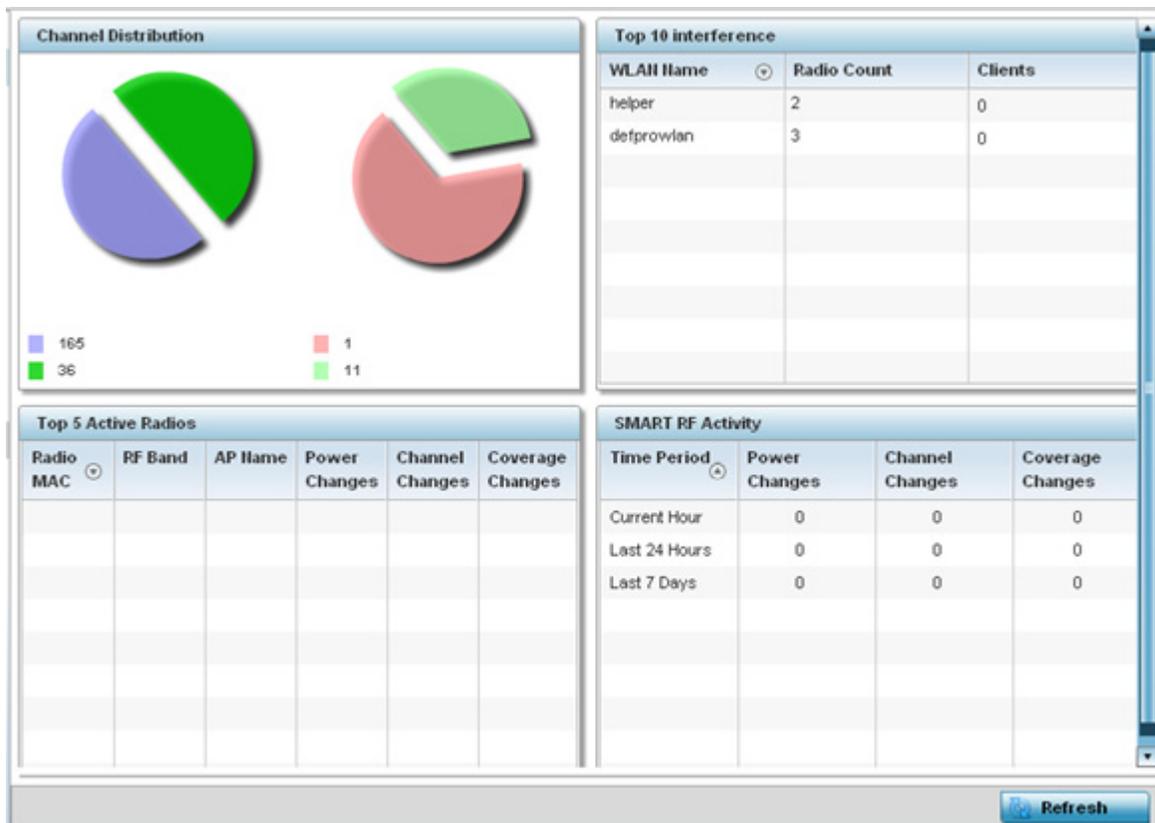
► *RF Domain Statistics*

When invoked by an administrator, *Self-Monitoring At Run Time* (Smart RF) instructs access point radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member access point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, un-managed radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

To view the Smart RF summary for RF Domain member access point radios:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Select **SMART RF** from the **RF Domain** menu.
4. Expand the **SMART RF** menu and select **Summary**.

The summary screen enables administrators to assess the efficiency of RF Domain member device channel distributions, sources of interference potentially requiring Smart RF adjustments, top performing RF Domain member device radios and the number of power, channel and coverage changes required as part of a Smart RF performance compensation activity.



**Figure 13-24** RF Domain - Smart RF Summary screen

5. The **Channel Distribution** table lists how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance.

6. Review the **Top 10 interference** table to assess RF Domain member WLANs whose radios are contributing the highest levels of detected interference within the RF Domain.

<b>WLAN Name</b>	Lists the WLANs whose member device radios are contributing to the highest levels of interference detected within the RF Domain.
<b>Radio Count</b>	Displays the number of radios within each listed WLAN that are contributing to the RF Domain's high levels of detected interference. These are the radios subject to Smart RF power compensations to reconcile the high levels of interference.
<b>Clients</b>	Lists the number of connected clients detected for the WLAN member device radios.

7. Review the **Top 5 Active Radios** to assess the significance of any Smart RF initiated compensations versus their reported top performance.

<b>Radio MAC</b>	Lists the hardware encoded MAC address of each listed top performing RF Domain member device radio.
<b>RF Band</b>	Displays the top performing radio's operation band. This may help administrate whether more changes were required in the 2.4 GHz band then 5 GHz or vice versa.
<b>AP Name</b>	Lists the administrator assigned access point name used to differentiate from other RF Domain member access point radios.
<b>Power Changes</b>	Displays the number of Smart RF initiated power level changes reported for this top performing RF Domain member radio.
<b>Channel Changes</b>	Displays the number of Smart RF initiated channel changes reported for this top performing RF Domain member radio.
<b>Coverage Changes</b>	Displays the number of Smart RF initiated coverage changes reported for this top performing RF Domain member radio.

8. Refer to the **SMART RF Activity** table to view the trending of Smart RF compensations.

<b>Time Period</b>	Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the <i>Current Hour</i> , <i>Last 24 Hours</i> or the <i>Last Seven Days</i> . Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods.
<b>Power Changes</b>	Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week.
<b>Channel Changes</b>	Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week.
<b>Coverage Changes</b>	Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week.



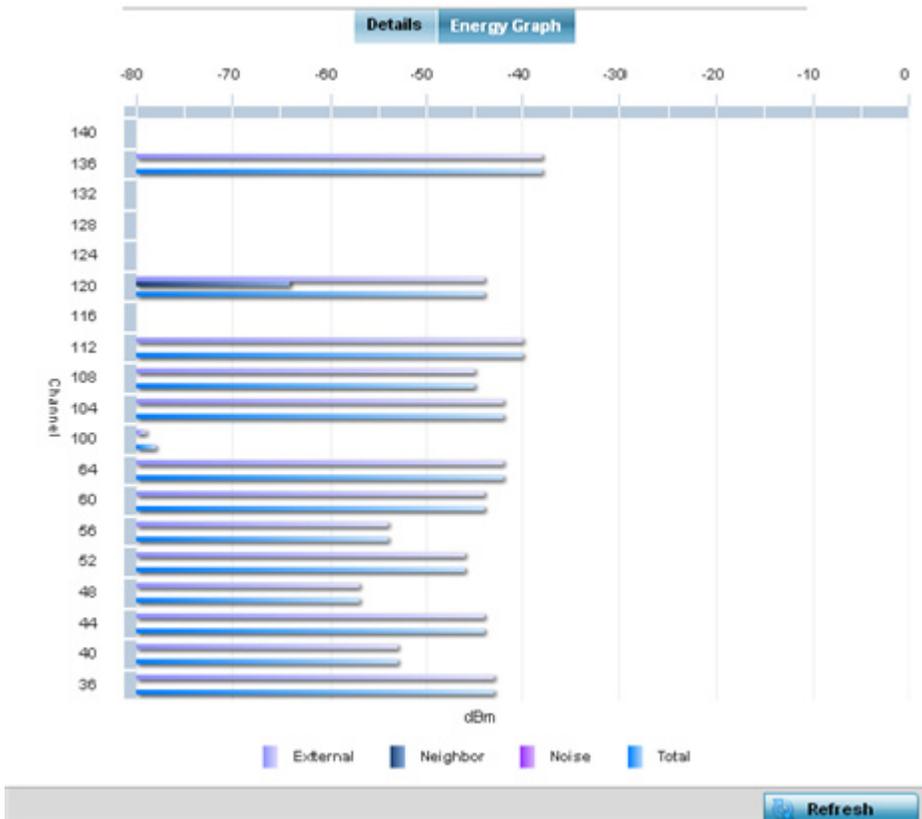


Figure 13-26 RF Domain - Smart RF Energy Graph

12. Select **Smart RF History** to review the descriptions and types of Smart RF events impacting RF Domain member devices.

Time	Type	Description
5/17/2013 12:54:52 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 136 to 112
5/17/2013 01:22:14 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 03:59:06 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/13/2013 04:01:24 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) removed
5/13/2013 04:02:05 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/17/2013 01:22:14 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/17/2013 01:25:38 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 112 to 120
5/18/2013 11:58:06 PM	Interference Recovery	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) channel changed from 4 to 8

Row Count: 303

Figure 13-27 RF Domain - Smart RF History screen

The **SMART RF History** screen displays the following RF Domain member historical data:

<b>Time</b>	Displays a time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain.
-------------	--

<b>Type</b>	Lists a high-level description of the Smart RF activity initiated for a RF Domain member device.
<b>Description</b>	Provides a more detailed description of the Smart RF event in respect to the actual Smart RF calibration or adjustment made to compensate for detected coverage holes and interference.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.



<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.
----------------	--

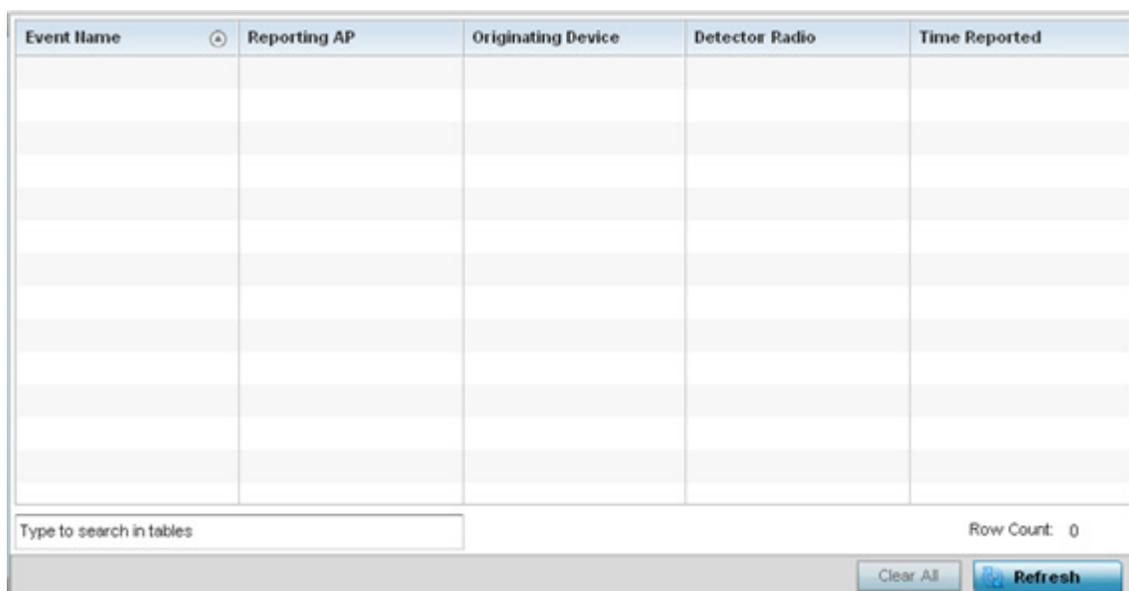
### 13.2.12.2 WIPS Events

▶ *WIPS*

Refer to the *WIPS Events* screen to assess WIPS events detected by RF Domain member access point radios and reported to the controller or service platform.

To view the rogue access point statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.
3. Expand the **WIPS** menu item and select **WIPS Events**.



**Figure 13-29** RF Domain - WIPS Events screen

The **WIPS Events** screen displays the following:

<b>Event Name</b>	Displays the event name of the intrusion detected by a RF Domain member access point.
<b>Reporting AP</b>	Displays the MAC address of the RF Domain member access point reporting the event.
<b>Originating Device</b>	Displays the MAC address of the device generating the event.
<b>Detector Radio</b>	Displays Access Point radio number detecting the event. AP7131N models can have from 1-3 radios depending on the SKU. AP6522, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models have 2 radios, while AP6511 and AP6521 models have 1 radio. An ES6510 is a controller or service platform managed Ethernet Switch, with no embedded device radios.
<b>Time Reported</b>	Displays a time stamp of when the event was reported by the RF Domain member access point radio.
<b>Clear All</b>	Select the <i>Clear All</i> button to clear the statistics counters and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.



<b>VLAN</b>	Displays the name of the VLAN the client would use as a virtual interface for captive portal operation with the access point.
<b>Remaining Time</b>	Displays the time after which a connected client is disconnected from the captive portal.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the statistics counters to their latest values.

## 13.3 Access Point Statistics

### ► *Statistics*

The Access Point statistics screens displays controller or service platform connected access point *performance, health, version, client support, radio, mesh, interface, DHCP, firewall, WIPS, sensor, captive portal, NTP* and *load* information. Access point statistics consists of the following:

- *Health*
  - *Device*
  - *Device Upgrade*
  - *Adoption*
  - *AP Detection*
  - *Wireless Clients*
  - *Wireless LANs*
  - *Policy Based Routing*
  - *Radios*
  - *Mesh*
  - *Interfaces*
  - *RTLS*
  - *PPPoE*
  - *OSPF*
  - *L2TPv3 Tunnels*
  - *VRRP*
  - *Critical Resources*
  - *LDAP Agent Status*
  - *GRE Tunnels*
  - *Dot1x*
  - *Network*
  - *DHCP Server*
  - *Firewall*
  - *VPN*
  - *Certificates*
  - *WIPS*
  - *Sensor Servers*
  - *Bonjour Services*
  - *Captive Portal*
  - *Network Time*
  - *Load Balancing*
  - *Environmental Sensors (AP8132 Models Only)*
-

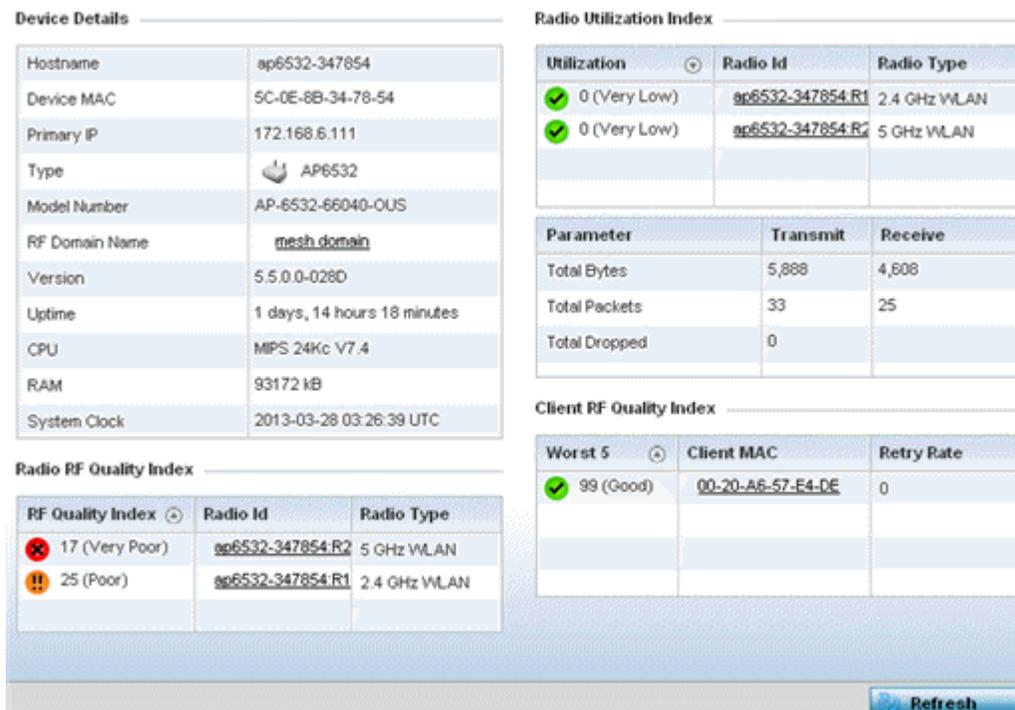
### 13.3.1 Health

► *Access Point Statistics*

The *Health* screen displays a selected access point's hardware version and software version. Use this information to fine tune the performance of an access point. This screen should also be the starting point for troubleshooting an access point since it's designed to present a high level display of access point performance efficiency.

To view the access point health:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Health**.



**Figure 13-31** Access Point - Health screen

The **Device Details** field displays the following information:

<b>Hostname</b>	Displays the AP's unique name as assigned within the network. A hostname is assigned to a device connected to a computer network.
<b>Device MAC</b>	Displays the MAC address of the AP. This is factory assigned and cannot be changed.
<b>Primary AP</b>	Displays the IP address of assigned to this device either through DHCP or through static IP assignment.
<b>Type</b>	Displays the access point's model type.
<b>Model Number</b>	Displays the access point's model number to help further differentiate the access point from others of the same model series and defined country of operation.

<b>RF Domain Name</b>	Displays the access point's RF Domain membership. Unlike a controller or service platform, an access point can only belong to one RF Domain based on its model. The domain name appears as a link that can be selected to show RF Domain utilization in greater detail.
<b>Version</b>	Displays the access point's current firmware version. Use this information to assess whether an upgrade is required for better compatibility.
<b>Uptime</b>	Displays the cumulative time since the access point was last rebooted or lost power.
<b>CPU</b>	Displays the processor core.
<b>RAM</b>	Displays the free memory available with the RAM.
<b>System Clock</b>	Displays the system clock information.

The **Radio RF Quality Index** field displays the following:

<b>RF Quality Index</b>	Displays access point radios having very low quality indices. RF quality index indicates the overall RF performance. The RF quality indices are: <ul style="list-style-type: none"> <li>• 0 – 50 (poor)</li> <li>• 50 – 75 (medium)</li> <li>• 75 – 100 (good)</li> </ul>
<b>Radio Id</b>	Displays a radio's hardware encoded MAC address. The ID appears as a link that can be selected to show radio utilization in greater detail.
<b>Radio Type</b>	Identifies whether the radio is a 2.4 or 5 GHz.

The **Radio Utilization** field displays the following:

<b>Total Bytes</b>	Displays the total bytes of data transmitted and received by the access point since the screen was last refreshed.
<b>Total Packets</b>	Lists the total number of data packets transmitted and received by the access point since the screen was last refreshed.
<b>Total Dropped</b>	List the number of dropped data packets by an access point radio since the screen was last refreshed.

The **Client RF Quality Index** field displays the following:

<b>Worst 5</b>	Displays clients having lowest RF quality within the network.
<b>Client MAC</b>	Displays the MAC addresses of the clients with the lowest RF indices.
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

4. Select the **Refresh** button as needed to update the screen's statistics counters to their latest values.

## 13.3.2 Device

### ► Access Point Statistics

The *Device* screen displays basic information about the selected access point. Use this screen to gather version information, such as the installed firmware image version, the boot image and upgrade status.

To view the device statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Device**.

The screenshot displays the 'Device' screen for an access point. It is divided into several sections:

- System:** A table with the following data:
 

Model Number	AP-6532-66040-OUS
Serial Number	10260522200899
Version	5.5.0.0-028D
Boot Partition	secondary
Fallback Enabled	✓ Enabled
Fallback Image Triggered	✗ No
Next Boot	secondary
- Firmware Images:** A table with the following data:
 

Primary Build Date	03:21:2013 08:33:04
Primary Install Date	03:22:2013 13:08:42
Primary Version	5.5.0.0-027D
Secondary Build Date	03:23:2013 20:12:04
Secondary Install Date	03:26:2013 13:07:41
Secondary Version	5.5.0.0-028D
FPGA Version	Unknown
PoE Firmware Version	Unknown
- System Resources:** A table with the following data:
 

Available Memory (MB)	38,688
Total Memory (MB)	93,172
Currently Free RAM	41.5%
Recommended Free RAM	10.0%
Current File Descriptors	585
Maximum File Descriptors	25,500
CPU Load 1 Minute	2.8%
CPU Load 5 Minutes	2.9%
CPU Load 15 Minutes	2.9%
- Upgrade Status:** A table with the following data:
 

Upgrade Status	Successful
Upgrade Status Time	2013-03-26 13:07:41
- Sensor Lock:** A table with the following data:
 

Sensor Lock State	✗ No
-------------------	------

A 'Refresh' button is located at the bottom right of the screen.

**Figure 13-32** Access Point - Device screen

The **System** field displays the following:

<b>Model Number</b>	Displays the model of the selected access point to help distinguish its exact SKU and country of operation.
<b>Serial Number</b>	Displays the numeric serial number set for the access point.
<b>Version</b>	Displays the software (firmware) version on the access point.
<b>Boot Partition</b>	Displays the boot partition type.
<b>Fallback Enabled</b>	Displays whether this option is enabled. This method enables a user to store a known legacy version and a new version in device memory. The user can test the new software, and use an automatic fallback, which loads the old version on the access point if the new version fails.
<b>Fallback Image Triggered</b>	Displays whether the fallback image was triggered. The fallback image is an old version of a known and operational software stored in device memory. This allows a user to test a new version of software. If the new version fails, the user can use the old version of the software.

<b>Next Boot</b>	Designates this version as the version used the next time the access point is booted.
------------------	---

The **System Resources** field displays the following:

<b>Available Memory (MB)</b>	Displays the available memory (in MB) available on the access point.
<b>Total Memory (MB)</b>	Displays the access point's total memory.
<b>Currently Free RAM</b>	Displays the access point's free RAM space. If its very low, free up some space by closing some processes.
<b>Recommended Free RAM</b>	Displays the recommended RAM required for routine operation.
<b>Current File Description</b>	Displays the access point's current file description.
<b>Maximum File Description</b>	Displays the access point's maximum file description.
<b>CPU Load 1 Minute</b>	Lists this access point's CPU utilization over a 1 minute span.
<b>CPU Load 5 Minutes</b>	Lists this access point's CPU utilization over a 5 minute span.
<b>CPU Load 15 Minutes</b>	Lists this access point's CPU utilization over a 15 minute span.

The **Fan Speed** field displays the following:

<b>Number</b>	Displays the number of fans supported on the this access point.
<b>Speed (Hz)</b>	Displays the fan speed in Hz.

The **Temperature** field displays the following:

<b>Number</b>	Displays the number of temperature elements used by the access point.
<b>Temperature</b>	Displays the current temperature (in Celsius) to assess a potential access point overheat condition.

The **Kernal Buffers** field displays the following:

<b>Buffer Size</b>	Lists the sequential buffer size.
<b>Current Buffers</b>	Displays the current buffers available to the selected access point.
<b>Maximum Buffers</b>	Lists the maximum buffers available to the selected access point.

The **IP Domain** field displays the following:

<b>IP Domain Name</b>	Displays the name of the IP Domain service used with the selected access point.
<b>IP Domain Lookup state</b>	Lists the current state of an IP lookup operation.

The **IP Name Servers** field displays the following:

<b>Name Server</b>	Displays the names of the servers designated to provide DNS resources to this access point.
<b>Type</b>	Displays the type of server for each server listed.

The **Firmware Images** field displays the following:

<b>Primary Build Date</b>	Displays the build date when this access point firmware version was created.
<b>Primary Install Date</b>	Displays the date this version was installed.
<b>Primary Version</b>	Displays the primary version string.
<b>Secondary Build Date</b>	Displays the build date when this version was created.
<b>Secondary Install Date</b>	Displays the date this secondary version was installed.
<b>Secondary Version</b>	Displays the secondary version string.
<b>FPGA Version</b>	Displays whether a FPGA supported firmware load is being utilized.
<b>PoE Firmware Version</b>	Displays whether a PoE supported firmware load is being utilized.

The **Upgrade Status** field displays the following:

<b>Upgrade Status</b>	Displays the status of the image upgrade.
<b>Upgrade Status Time</b>	Displays the time of the image upgrade.

The **Sensor Lock** field displays the following:

<b>Sensor Lock</b>	Displays whether a lock has been applied to access point sensor capabilities.
--------------------	---

The **Power Management** field displays the following:

<b>Power Management Mode</b>	Displays the power mode currently invoked by the selected access point.
<b>Power Management Status</b>	Lists the power status of the access point.
<b>Ethernet Power Status</b>	Displays the access point's Ethernet power status.
<b>Radio Power Status</b>	Displays the power status of the access point's radios.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.

### 13.3.3 Device Upgrade

#### ► Access Point Statistics

The *Device Upgrade* screen displays information about devices receiving updates and the devices used to provision them. Use this screen to gather version data, install firmware images, boot an image and upgrade status.





<b>Errors</b>	Lists any configuration errors that may be hindering a clean adoption.
<b>Adopted By</b>	Lists the adopting access point.
<b>Adoption time</b>	Displays each listed access point's time of adoption.
<b>Startup Time</b>	Displays each listed access point's in service time since last offline.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.4.2 AP Adoption History

#### ► Adoption

The *AP Adoption History* screen displays a list of peer access point and their adoption event status.

To review a selected access point's adoption history:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain and select one of its connected access points.
3. Expand the **Adoption** menu item.
4. Select **AP Adoption History**.

Event Name	AP MAC Address	Reason	Event Time
Adopted	00-23-68-8D-FE-4C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	B4-C7-99-5A-84-2C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	5C-0E-8B-34-7B-7C	N.A.	Tue Aug 20 2013 05:01:49 PM
Adopted	5C-0E-8B-A6-57-2C	N.A.	Tue Aug 20 2013 05:01:50 PM
Adopted	00-23-68-31-18-E0	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-77-6C	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-78-00	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	00-23-68-31-29-D8	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	B4-C7-99-58-64-A0	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	B4-C7-99-71-16-30	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-76-38	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-50-3C	N.A.	Tue Aug 20 2013 05:01:52 PM
Admitted	5C-0F-8B-8A-4F-15	N.A.	Tue Aug 20 2013 05:01:52 PM

Type to search in tables Row Count: 26

**Refresh**

**Figure 13-35** Access Point - AP Adoption History screen

The **Adopted Devices** screen describes the following historical data for adopted access points:

<b>Event Name</b>	Displays the adoption status of each listed access point as either adopted or un-adopted.
<b>AP MAC Address</b>	Displays the MAC address of each access point this access point has attempted to adopt.
<b>Reason</b>	Displays the reason code for each event listed.
<b>Event Time</b>	Displays day, date and time for each access point adoption attempt.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.4.3 AP Self Adoption History

► *Adoption*

The *AP Self Adoption History* displays an event history of peer access points that have adopted to the selected access point.

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain and select one of its connected access points.
3. Expand the **Adoption** menu item.
4. Select **AP Self Adoption History**.

Event History	Mac	Reason	Adoption Time
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 26 2013 05:09:10 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 26 2013 05:22:34 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 19 2013 08:17:10 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 26 2013 06:12:07 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Fri Mar 22 2013 06:33:02 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 19 2013 08:37:33 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Fri Mar 22 2013 06:13:52 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Fri Mar 22 2013 06:04:30 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 26 2013 05:52:50 AM
Adopted	B4-C7-99-DC-98-48	N.A.	Tue Mar 19 2013 08:25:48 AM
un-adopted	B4-C7-99-DC-98-48	Adopter 19.0C.98.48 is no longer rei	Fri Mar 22 2013 06:30:39 AM
un-adopted	B4-C7-99-DC-98-48	Adopter 19.0C.98.48 is no longer rei	Tue Mar 19 2013 08:35:09 AM
un-adopted	B4-C7-99-DC-98-48	Adopter 19.0C.98.48 is no longer rei	Tue Mar 26 2013 05:20:08 AM

Type to search in tables Row Count: 16

**Refresh**

**Figure 13-36** Access Point - AP Self Adoption History screen

The **AP Self Adoption History** screen describes the following historical data for adopted access points:

<b>Event History</b>	Displays the self adoption status of each access point as either <i>Adopted</i> or <i>un-adopted</i> .
<b>MAC</b>	Displays the hardware encoded <i>Media Access Control</i> (MAC) of the auto adopted access point.
<b>Reason</b>	Displays the adoption reason code for an access point's auto adoption.
<b>Adoption Time</b>	Displays a timestamp for the access point's auto-adoption.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.4.4 Pending Adoptions

► *Adoption*

The *Pending Adoptions* screen displays a list of devices yet to be adopted to this peer access point, or access points in the process of adoption.

To view pending access point statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain and select one of its connected access points.





### 13.3.6 Wireless Clients

#### ▶ Access Point Statistics

The *Wireless Clients* screen displays credential information for wireless clients associated with an access point. Use this information to assess if configuration changes are required to improve network performance.

To view wireless client statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Wireless Clients**.

Client MAC	IP Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
<a href="#">00-21-5A-72-DB-F2</a>	157.235.90.38	WINDOWS-7EB	N/A	Unknownr	Intel Corp	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:22
<a href="#">10-0B-A9-6D-FC-80</a>	157.235.90.60	TWQ463-Win7	N/A	Unknownr	Intel Corp	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:22
<a href="#">24-77-03-61-87-04</a>	157.235.90.45	CMW072-W7	N/A	Unknownr	Intel Corp	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:22
<a href="#">5C-96-9D-68-BA-3D</a>	157.235.90.44	MFK876-02M	N/A	Unknownr	Apple Inc	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:22
<a href="#">9C-04-EB-74-31-7C</a>	157.235.90.107	Ravis-iPad	N/A	Unknownr	Apple Inc	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:21
<a href="#">BC-3B-AF-DF-1D-24</a>	157.235.90.180	IPad	N/A	Unknownr	Apple Inc	11an	AN-04-7034	B4-C7-9	STOVLB	30	Wed Sep 11 14:22

Type to search in tables Row Count: 6

[Disconnect Client](#) [Refresh](#)

**Figure 13-39** Access Point - Wireless Clients screen

The **Wireless Clients** screen displays the following:

<b>Client MAC</b>	Displays the hardcoded MAC address assigned to the client at the factory. The address displays as a link that can be selected to display configuration and network address information in greater detail.
<b>IP Address</b>	Displays the unique IP address of the client. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
<b>Hostname</b>	Displays the hostname (MAC addresses) of connected wireless clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail.
<b>Role</b>	Lists the client's defined role within the access point managed network.
<b>Client Identity</b>	Displays the unique identity of the listed client as it appears to its adopting access point.
<b>Vendor</b>	Displays the name of the client vendor (manufacturer).
<b>Band</b>	Displays the 802.11 radio band on which the listed wireless client operates.
<b>AP Hostname</b>	Displays the administrator assigned hostname of the access point to which this access point is adopted.



<b>SSID</b>	Displays each listed WLAN's <i>Service Set ID</i> (SSID) used as the WLAN's network identifier.
<b>Traffic Index</b>	Displays the traffic utilization index, which measures how efficiently the WLAN's traffic medium is used. It's defined as the percentage of current throughput relative to maximum possible throughput. Traffic indices are: <ul style="list-style-type: none"> <li>• 0 – 20 (very low utilization)</li> <li>• 20 – 40 (low utilization)</li> <li>• 40 – 60 (moderate utilization)</li> <li>• 60 and above (high utilization)</li> </ul>
<b>Radio Count</b>	Displays the cumulative number of peer access point radios deployed within each listed WLAN.
<b>Tx Bytes</b>	Displays the average number of transmitted bytes sent on each listed WLAN.
<b>Tx User Data Rate</b>	Displays the transmitted user data rate in kbps for each listed WLAN.
<b>Rx Bytes</b>	Displays the average number of packets in bytes received on each listed WLAN.
<b>Rx User Data Rate</b>	Displays the received user data rate on each listed WLAN.
<b>Disassociate All Clients</b>	Select an WLAN then <i>Disassociate All Clients</i> to terminate the client connections within that WLAN.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.



<b>Secondary Next Hop State</b>	Displays whether the secondary hop is applied to incoming routed packets (UP/UNREACHABLE).
<b>Default Next Hop IP</b>	If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This is either the IP address of the next hop or the outgoing interface. Only one default next hop is available. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse.
<b>Default Next Hop State</b>	Displays whether the default hop is being applied to incoming routed packets.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.9 Radios

#### ▶ [Access Point Statistics](#)

The *Radio* statistics screens display information on access point radios. The actual number of radios depend on the access point model and type. This screen displays information on a per radio basis. Use this information to refine and optimize the performance of each radio and therefore improve network performance.

The access point's radio statistics screens provide details about associated radios. It provides radio ID, radio type, RF quality index etc. Use this information to assess the overall health of radio transmissions and access point placement. An AP7131N model access point can support from 1-3 radios depending on the SKU purchased. AP6522, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX access points are dual radio models and AP6511 and AP6532 models are both single radio models. An ES6510 is a controller or service platform managed Ethernet Switch, with no embedded device radios.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- [Status](#)
- [RF Statistics](#)
- [Traffic Statistics](#)

Individual access point radios display as selectable links within each of the three access point radio screens. To review a radio's configuration in greater detail, select the link within the Radio column of either the *Status*, *RF Statistics* or *Traffic Statistics* screens.

Additionally, navigate the *Traffic*, *WMM TSPEC*, *Wireless LANs* and *Graph* options available on the upper, left-hand side, of the screen to review radio traffic utilization, WMM QoS settings, WLAN advertisement and radio graph information in greater detail. This information can help determine whether the radio is properly configured in respect to its intended deployment objective.





<b>Traffic Index</b>	Displays the traffic utilization index of the radio. This is expressed as an integer value. 0 – 20 indicates very low utilization, and 60 and above indicate high utilization.
<b>Quality Index</b>	Displays an integer that indicates overall RF performance. The RF quality indices are: <ul style="list-style-type: none"> <li>• 0 – 50 (poor)</li> <li>• 50 – 75 (medium)</li> <li>• 75 – 100 (good)</li> </ul>
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.9.3 Traffic Statistics

Refer to the *Traffic Statistics* screen to review access point radio transmit and receive statistics, data rate, and packets dropped during both transmit and receive operations.

To view the access point radio traffic statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Expand **Radios**.
4. Select **Traffic Statistics**.

Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Error Rate
<a href="#">ap7131-8A4848R1</a>	0	0	0	0	0 kbps	0 kbps	0	10
<a href="#">ap7131-8A4848R2</a>	298	2,409	4	17	0 kbps	0 kbps	0	5

Type to search in tables Row Count: 2

[Refresh](#)

**Figure 13-44** Access Point - Radio Traffic Statistics screen

The **Traffic Statistics** screen displays the following:

<b>Radio</b>	Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data.
<b>Tx Bytes</b>	Displays the total number of bytes transmitted by each listed radio. This includes all user data as well as any management overhead data.
<b>Rx Bytes</b>	Displays the total number of bytes received by each listed radio. This includes all user data as well as any management overhead data.



The **Mesh** screen describes the following:

<b>Client</b>	Displays the system assigned name of each member of the mesh network.
<b>Client Radio MAC</b>	Displays the MAC address of each client radio in the mesh network.
<b>Portal</b>	Mesh points connected to an external network and forward traffic in and out are mesh portals. Mesh points must find paths to a portal to access the Internet. When multiple portals exist, the mesh point must select one.
<b>Portal Radio MAC</b>	Lists the MAC addresses of those access points serving as mesh portals.
<b>Connect Time</b>	Displays the elapsed connection time for each listed client in the mesh network.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.11 Interfaces

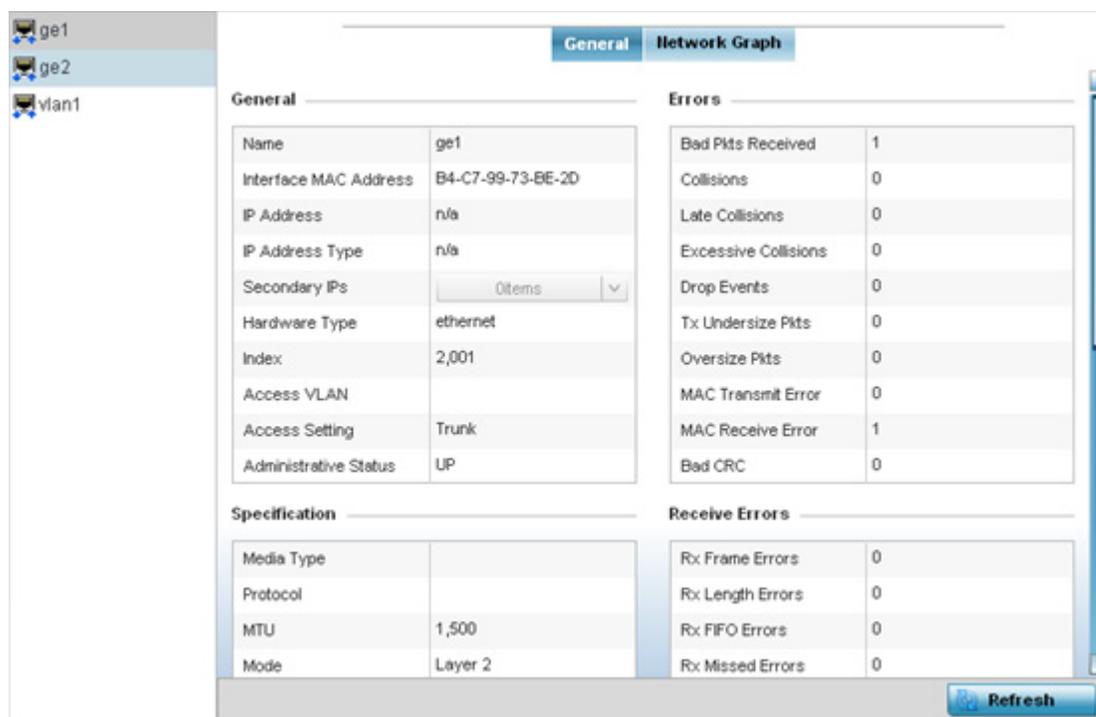
▶ [Access Point Statistics](#)

The *Interface* screen provides detailed statistics on each of the interfaces available on the selected access point. Use this screen to review the statistics for each interface. Interfaces vary amongst supported access point models.

To review access point interface statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Interfaces**.

The **General** tab displays by default.



**Figure 13-46** Access Point- General Interface screen

Interface Statistics support the following:

- [General Interface Details](#)
- [Network Graph](#)

### 13.3.11.1 General Interface Details

#### ► [Interfaces](#)

The *General* tab provides information on a selected access point interface such as its MAC address, type and TX/RX statistics.

The **General** table displays the following:

<b>Name</b>	Displays the name of the access point interface <i>ge1, vlan1</i> etc.
<b>Interface MAC Address</b>	Displays the MAC address of the interface.
<b>IP Address</b>	IP address of the interface.
<b>IP Address Type</b>	Displays the IP address type, either <i>IPv4</i> or <i>IPv6</i> .
<b>Secondary IP</b>	Displays a list of secondary IP resources assigned to this interface.
<b>Hardware Type</b>	Displays the networking technology.
<b>Index</b>	Displays the unique numerical identifier for the interface.
<b>Access VLAN</b>	Displays the tag assigned to the native VLAN.
<b>Access Setting</b>	Displays the VLAN mode as either <i>Access</i> or <i>Trunk</i> .
<b>Administrative Status</b>	Displays whether the interface is currently <i>UP</i> or <i>DOWN</i> .

The **Specification** table displays the following information:

<b>Media Type</b>	Displays the physical connection type of the interface. Medium types include: <i>Copper</i> - Used on RJ-45 Ethernet ports <i>Optical</i> - Used on fibre optic gigabit Ethernet ports
<b>Protocol</b>	Displays the routing protocol used by the interface.
<b>MTU</b>	Displays the <i>maximum transmission unit</i> (MTU) setting configured on the interface. The MTU value represents the largest packet size that can be sent over a link. 10/100 Ethernet ports have a maximum setting of 1500.
<b>Mode</b>	Lists whether traffic on the listed port is Layer 2 or Layer 3.
<b>Metric</b>	Displays the metric associated with the interface's route.
<b>Maximum Speed</b>	Displays the maximum speed the interface uses to transmit or receive data.
<b>Admin Speed</b>	Displays the speed the port can transmit or receive. This value can be either <i>10, 100, 1000</i> or <i>Auto</i> . This value is the maximum port speed in Mbps. Auto indicates the speed is negotiated between connected devices.
<b>Operator Speed</b>	Displays the current speed of data transmitted and received over the interface.
<b>Admin Duplex Setting</b>	Displays the administrator's duplex setting.
<b>Current Duplex Setting</b>	Displays the interface as either <i>half duplex, full duplex</i> or <i>unknown</i> .

The **Traffic** table displays the following:

<b>Good Octets Sent</b>	Displays the number of octets (bytes) with no errors sent by the interface.
<b>Good Octets Received</b>	Displays the number of octets (bytes) with no errors received by the interface.
<b>Good Packets Sent</b>	Displays the number of good packets transmitted.
<b>Good Packets Received</b>	Displays the number of good packets received.
<b>Mcast Pkts Sent</b>	Displays the number of multicast packets sent through the interface.
<b>Mcast Pkts Received</b>	Displays the number of multicast packets received through the interface.
<b>Ucast Pkts Sent</b>	Displays the number of unicast packets sent through the interface.
<b>Ucast Pkts Received</b>	Displays the number of unicast packets received through the interface.
<b>Bcast Pkts Sent</b>	Displays the number of broadcast packets sent through the interface.
<b>Bcast Pkts Received</b>	Displays the number of broadcast packets received through the interface.
<b>Packet Fragments</b>	Displays the number of packet fragments transmitted or received through the interface.
<b>Jabber Pkts</b>	Displays the number of packets transmitted through the interface larger than the MTU.

The **Errors** table displays the following:

<b>Bad Pkts Received</b>	Displays the number of bad packets received through the interface.
<b>Collisions</b>	Displays the number of collisions over the selected interface.
<b>Late Collisions</b>	A late collision is any collision that occurs after the first 64 octets of data have been sent. Late collisions are not normal, and usually the result of out of specification cabling or a malfunctioning device.
<b>Excessive Collisions</b>	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently.
<b>Drop Events</b>	Displays the number of dropped packets transmitted or received through the interface.
<b>Tx Undersize Pkts</b>	Displays the number of undersized packets transmitted through the interface.
<b>Oversize Pkts</b>	Displays the number of oversized packets transmitted through the interface.
<b>MAC Transmit Error</b>	Displays the number of failed transmits due to an internal MAC sublayer error (that's not a late collision), due to excessive collisions or a carrier sense error.
<b>MAC Receive Error</b>	Displays the number of received packets that failed due to an internal MAC sublayer (that's not a late collision), an excessive number of collisions or a carrier sense error.
<b>Bad CRC</b>	Displays the CRC error. The CRC is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a bad CRC.

The **Receive Errors** table displays the following:

<b>Rx Frame Errors</b>	Displays the number of frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
<b>Rx Length Errors</b>	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was either less or over the Ethernet standard.
<b>Rx FIFO Errors</b>	Displays the number of FIFO errors received at the interface. First-in First-out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
<b>Rx Missed Errors</b>	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.
<b>Rx Over Errors</b>	Displays the number of overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following:

<b>Tx Errors</b>	Displays the number of packets with errors transmitted on the interface.
<b>Tx Dropped</b>	Displays the number of transmitted packets dropped from the interface.
<b>Tx Aborted Errors</b>	Displays the number of packets aborted on the interface because a <i>clear-to-send</i> request was not detected.
<b>Tx Carrier Errors</b>	Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
<b>Tx FIFO Errors</b>	Displays the number of FIFO errors transmitted at the interface. <i>First-in First-Out</i> (FIFO) queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction.
<b>Tx Heartbeat Errors</b>	Displays the number of heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.
<b>Tx Window Errors</b>	Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest value.

### 13.3.11.2 Network Graph

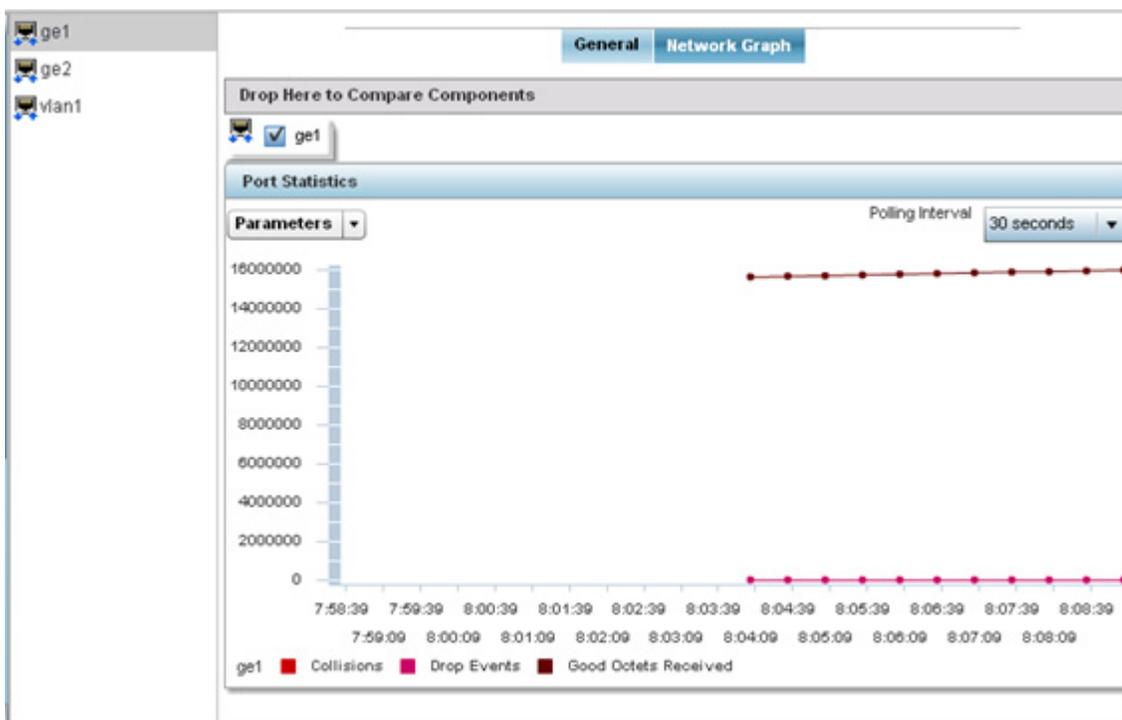
#### ► Interfaces

The *Network Graph* displays statistics the access point continuously collects for its interfaces. Even when the interface statistics graph is closed, data is still collected. Display the interface statistics graph periodically for assessing the latest interface information. Up to three different stats can be selected and displayed within the graph.

To view a detailed graph for an interface, select an interface and drop it on to the graph. The graph displays *Port Statistics* as the Y-axis and the *Polling Interval* as the X-axis. Use the **Polling Interval** from-down menu to define the increment data is displayed on the graph.

To view the Interface Statistics graph:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Interfaces**.
4. Select **Network Graph**.



**Figure 13-47** Access Point- Interface Network Graph screen

### 13.3.12 RTLS

#### ▶ Access Point Statistics

The *real time locationing system* (RTLS) enables accurate location determination and presence detection capabilities for Wi-Fi-based devices, Wi-Fi-based active RFID tags and passive RFID tags. While the operating system does not support locationing locally, it does report the locationing statistics of both Aeroscout and Ekahau tags.

To review a selected access point's RTLS statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **RTLS**.

The screenshot shows a web interface for RTLS (Real-Time Location System) statistics. It is divided into two sections: 'Aeroscout' and 'Ekahau'. The 'Aeroscout' section contains a table with 12 rows of statistics, all showing a value of 0. The 'Ekahau' section contains a single row for 'Tag Reports' with a value of 0. A 'Refresh' button is located at the bottom right of the interface.

Aeroscout	
Engine IP	0.0.0.0
Engine Port	0
Send Count	0
Recv Count	0
Tag Reports	0
Nacks	0
Acks	0
Lbs	0
AP Status	0
AP Notifications	0
Send Errors	0
Error Message Count	0

Ekahau	
Tag Reports	0

**Figure 13-48** Access Point - RTLS screen

The **Access Point RTLS** screen displays the following for Aeroscout tags:

<b>Engine IP</b>	Lists the IP address of the Aeroscout locationing engine.
<b>Engine Port</b>	Displays the port number of the Aeroscout engine.
<b>Send Count</b>	Lists the number location determination packets sent by the locationing engine.
<b>Recv Count</b>	Lists the number location determination packets received by the locationing engine.
<b>Tag Reports</b>	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.
<b>Nacks</b>	Displays the number of <i>Nack</i> (no acknowledgement) frames received from RTLS supported radio devices providing locationing services.
<b>Acks</b>	Displays the number of <i>Ack</i> (acknowledgment) frames received from RTLS supported radio devices providing locationing services.
<b>Lbs</b>	Displays the number of <i>location based service</i> (LBS) frames received from RTLS supported radio devices providing locationing services.
<b>AP Status</b>	Provides the status of peer access points providing locationing assistance.
<b>AP Notifications</b>	Displays a count of the number of notifications sent to access points that may be available to provide RTLS support.
<b>Send Errors</b>	Lists the number of send errors received by the RTLS initiating access point.
<b>Error Message Count</b>	Displays a cumulative count of error messages received from RTLS enabled access point radios.

The **Access Point RTLS** screen displays the following for Ekahau tags:

<b>Tag Reports</b>	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

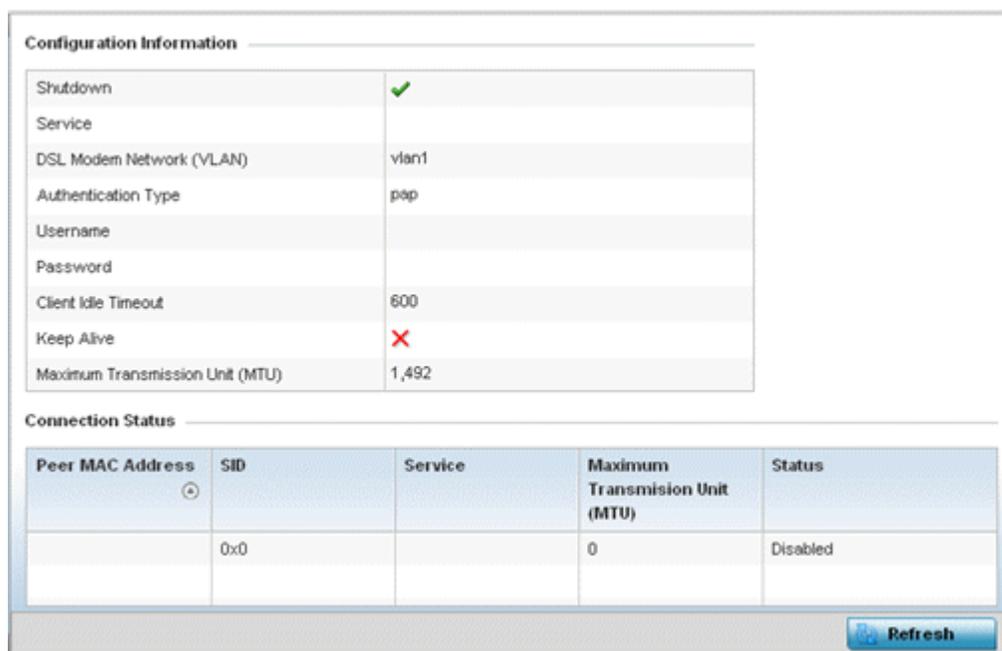
### 13.3.13 PPPoE

► [Access Point Statistics](#)

The *PPPoE* statistics screen displays stats derived from the AP's access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To review a selected access point's PPPoE statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **PPPoE**.



**Figure 13-49** Access Point - PPPoE screen

The **Configuration Information** field screen displays the following:

<b>Shutdown</b>	Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol.
<b>Service</b>	Lists the 128 character maximum PPPoE client service name provided by the service provider.
<b>DSL Modem Network (VLAN)</b>	Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem.

<b>Authentication Type</b>	Lists authentication type used by the PPPoE client whose credentials must be shared by its peer access point. Supported authentication options include <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> and <i>MSCHAP-v2</i> .
<b>Username</b>	Displays the 64 character maximum username used for authentication support by the PPPoE client.
<b>Password</b>	Displays the 64 character maximum password used for authentication by the PPPoE client.
<b>Client Idle Timeout</b>	The access point uses the listed timeout so it does not sit idle waiting for input from the PPPoE client and the server, that may never come.
<b>Keep Alive</b>	If a keep alive is utilized, the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
<b>Maximum Transmission Unit (MTU)</b>	Displays the PPPoE client <i>maximum transmission unit</i> (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size.

4. Refer to the **Connection Status** field.

The Connection Status table lists the MAC address, SID, Service information MTU and status of each route destination peer. To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN were to fail.

5. Select the **Refresh** button to update the screen's statistics counters to their latest values.

### 13.3.14 OSPF

#### ▶ [Access Point Statistics](#)

*Open Shortest Path First* (OSPF) is a *link-state interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

Refer to the following for detailed descriptions of the tabs available within the OSPF statistics screen:

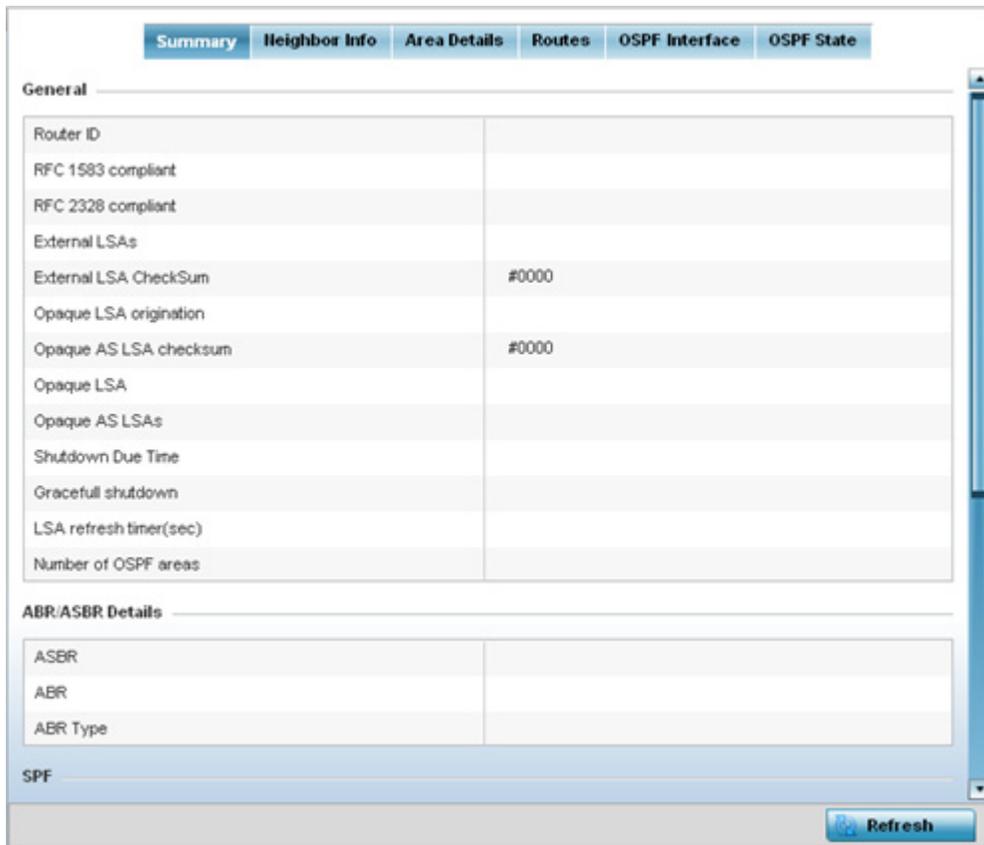
- [OSPF Summary](#)
- [OSPF Neighbors](#)
- [OSPF Area Details](#)
- [OSPF Route Statistics](#)
- [OSPF Route Statistics](#)
- [OSPF State](#)

### 13.3.14.1 OSPF Summary

▶ *OSPF*

To view OSPF summary statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.
3. Select **OSPF**. The *Summary* tab displays by default.



**Figure 13-50** Access Point - OSPF Summary tab

The **Summary** tab describes the following information fields:

<p><b>General</b></p>	<p>The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data. OSPF version 2 was originally defined within RFC versions 1583 and 2328. The general field displays whether compliance to these RFCs have been satisfied. The OSPF Link-State Advertisement (LSA) Throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds. LSA information is provided for both external and opaque LSAs. Opaque LSAs carrying type-length-value elements. These extensions allow OSPF to run completely out of band of the data plane network. This means that it can also be used on non-IP networks, such as optical networks.</p>
-----------------------	--

<b>ABR/ASBR</b>	Lists <i>Autonomous System Boundary Router</i> (ASBR) data relevant to OSPF routing, including the ASBR, ABR and ABR type. An <i>Area Border Router</i> (ABR) is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected. An ASBR is a router connected to more than one Routing protocol and exchanges routing information with routers in other protocols. ASBRs typically also run an exterior routing protocol (for example, BGP), or use static routes, or both. An ASBR is used to distribute routes received from other, external ASs throughout its own autonomous system. Routers in other areas use ABR as next hop to access external addresses. Then the ABR forwards packets to the ASBR announcing the external addresses.
<b>SPF</b>	Refer to the SPF field to assess the status of the <i>shortest path forwarding</i> (SPF) <i>execution</i> , <i>last SPF execution</i> , <i>SPF delay</i> , <i>SPF due in</i> , <i>SPF hold multiplier</i> , <i>SPF hold time</i> , <i>SPF maximum hold time</i> and <i>SPF timer due flag</i> .
<b>Stub Router</b>	The summary screen displays information relating to stub router advertisements and shutdown and startup times. An OSPF stub router advertisement allows a new router into a network without immediately routing traffic through the new router and allows a graceful shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the OSPF protocol to advertise a maximum or infinite metric to all neighbors.

4. Select the **Refresh** button to update the statistics counters to their latest values.



<b>Request Count</b>	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router.
<b>Retransmit Count</b>	Lists the connection retransmission count attempted in order to connect to the router interface, discover neighbors and elect a designated router. A <i>designated router</i> (DR) is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast.
<b>Dead Time</b>	Lists the dead time between neighbors in the network topology that are currently utilizing the listed router ID.
<b>Self Neighbor State</b>	Displays the self-neighbor status assessment used to discover neighbors and elect a designated router.
<b>Source Address</b>	Displays the single source address used by all neighbor routers to obtain topology and connection status. This form of multicasting significantly reduces network load.
<b>Summary Count</b>	Routes that originate from other areas are called summary routes. Summary routes are not flooded in a totally stubby or NSSA totally stubby area.

5. Select the **Refresh** button to update the statistics counters to their latest values.

### 13.3.14.3 OSPF Area Details

#### ► OSPF

An OSPF network is subdivided into routing areas (with 32 bit area identifiers) to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network. An OSPF Area contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation.

To view OSPF area statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.
3. Select **OSPF**.
4. Select the **Area Details** tab.



<b>NSSA LSA</b>	Routers in a <i>Not-so-stubby-area</i> (NSSA) do not receive external LSAs from Area Border Routers, but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the Area Border Router then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network.  Redistribution into an NSSA area creates a special type of LSA known as TYPE 7, which can exist only in an NSSA area. An NSSA ASBR generates this LSA, and an NSSA ABR router translates it into type 5 LSA which gets propagated into the OSPF domain.
<b>Opaque Area link CSUM</b>	Displays the Type-10 opaque link area checksum with the complete contents of the LSA. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area.
<b>Opaque link CSUM</b>	Displays the Type-10 opaque link checksum with the complete contents of the LSA.

5. Select the **Refresh** button to update the statistics counters to their latest values.

#### 13.3.14.4 OSPF Route Statistics

##### ► OSPF

Refer to the *Routes* tab to assess the status of OSPF *Border Routes*, *External Routes*, *Network Routes* and *Router Routes*.

To view OSPF route statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.
3. Select **OSPF**.
4. Select the **Routes** tab. Border routes display by default.

An *area border router* (ABR) connects (links) more than one area. Usually an ABR is used to connect non-backbone areas to the backbone. If OSPF virtual links are used an ABR will also be used to connect the area using the virtual link to another non-backbone area. Border routes use internal OSPF routing table entries to an ABR or *Autonomous System Boundary Router* (ASBR). Border routers maintain an LSDB for each area supported. They also participate in the backbone.

5. Refer to **External Routes** tab.







<b>OSPF Enabled</b>	Lists whether OSPF has been enabled for each listed interface. OSPF is disabled by default.
<b>UP/DOWN</b>	Displays whether the OSPF interface (the dynamic route) is currently up or down for each listed interface. An OSPF interface is the connection between a router and one of its attached networks.

5. Select the **Refresh** button to update the statistics counters to their latest values.

### 13.3.14.6 OSPF State

#### ▶ OSPF

An OSPF enabled access point sends hello packets to discover neighbors and elect a designated router for dynamic links. The hello packet includes link *state* data maintained on each access point and is periodically updated on all OSPF members. The access point tracks link state information to help assess the health of the OSPF dynamic route.

To view OSPF state statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.
3. Select **OSPF**.
4. Select the **OSPF State** tab.

Summary	Neighbor Info	Area Details	Routes	OSPF Interface	OSPF State
OSPF state		Running			
OSPF ignore state count		0			
OSPF ignore state monitor timeout		360			
OSPF ignore state timeout		60			
OSPF max ignore state count		5			
OSPF max routes		256			
OSPF routes received		0			

**Figure 13-57** Access Point OSPF - State tab

The **OSPF State** tab describes the following:

<b>OSPF state</b>	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a <i>link-state database</i> (LSDB) which is a tree image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF supported nodes. Flooding is the part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.
<b>OSPF ignore state count</b>	Lists the number of times state requests have been ignored between the access point and its peers within this OSPF supported broadcast domain.



The Access Point **L2TPv3 Tunnels** screen displays the following:

<b>Tunnel Name</b>	Displays the name of each listed L2TPv3 tunnel assigned upon creation. Each listed tunnel name can be selected as a link to display session data specific to that tunnel. The Sessions screen displays cookie size information as well as pseudowire information specific to the selected tunnel. Data is also available to define whether the tunnel is a trunk session and whether tagged VLANs are used. The number of transmitted, received and dropped packets also display to provide a throughput assessment of the tunnel connection. Each listed session name can also be selected as a link to display VLAN information specific to that session. The VLAN Details screen lists those VLANs used an access point interface in L2TP tunnel establishment.
<b>Local Address</b>	Lists the IP address assigned as the local tunnel end point address, not the tunnel interface's IP address. This IP is used as the tunnel source IP address. If a local address is not specified, the source IP address is chosen automatically based on the tunnel peer IP address.
<b>Peer Address</b>	Lists the IP address of the L2TP tunnel peer establishing the tunnel connection.
<b>Tunnel State</b>	States whether the tunnel is idle (not utilized by peers) or is currently active.
<b>Peer Host Name</b>	Lists the assigned peer hostname used as matching criteria in the tunnel establishment process.
<b>Peer Control Connection ID</b>	Displays the numeric identifier for the tunnel session. This is the peer pseudowire ID for the session. This source and destination IDs are exchanged in session establishment messages with the L2TP peer.
<b>CTRL Connection ID</b>	Displays the router ID(s) sent in tunnel establishment messages with a potential peer device.
<b>Up Time</b>	Lists the amount of time the L2TP connection has remained established amongst peers sharing the L2TPv3 tunnel connection. Up Time is displayed in a <i>Days: Hours: Minutes: Seconds:</i> format. If D:0 H:0 M:0 S:0 is displayed, the tunnel connection is not currently established.
<b>Encapsulation Protocol</b>	Displays either <i>IP</i> or <i>UDP</i> as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. Tunneling is also called encapsulation. Tunneling works by encapsulating a network protocol within packets carried by the second network.
<b>Critical Resource</b>	Lists critical resources for this tunnel. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by access points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.
<b>VRRP Group</b>	Displays the VRRP group name if configured. VRRP configurations support router redundancy in a wireless network requiring high availability
<b>Establishment Criteria</b>	Displays the tunnel establishment criteria for this tunnel. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest value.

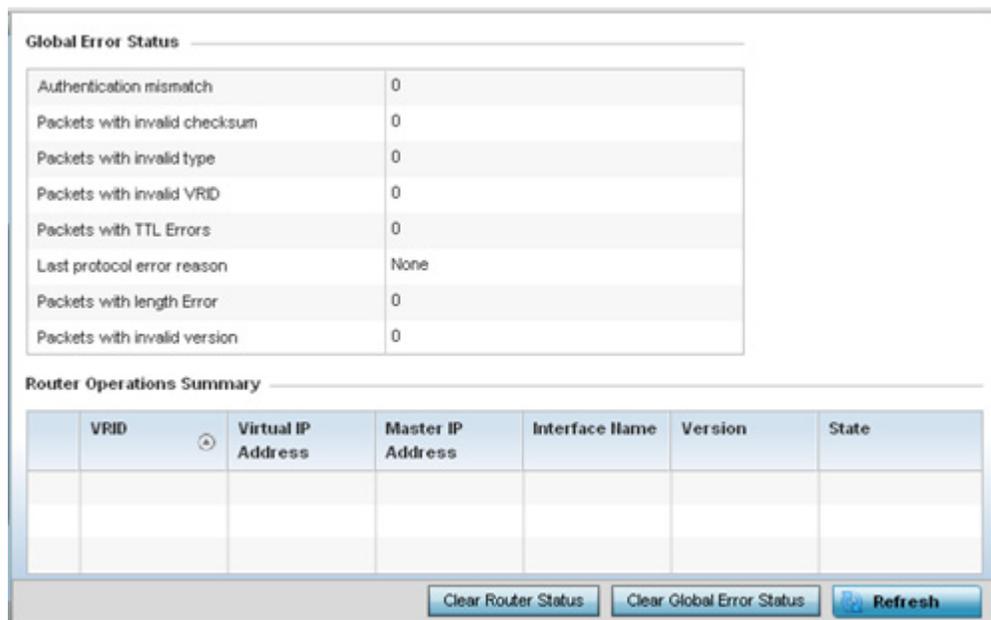
### 13.3.16 VRRP

► *Access Point Statistics*

The *VRRP* statistics screen displays *Virtual Router Redundancy Protocol* (VRRP) configuration statistics supporting router redundancy in a wireless network requiring high availability.

To review a selected access point's VRRP statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **VRRP**.



**Figure 13-59** Access Point - VRRP screen

4. Refer to the **Global Error Status** field to review the various sources of packet errors logged during the implementation of the virtual route.

Errors include the mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

5. Refer to the **Router Operations Summary** for the following status:

<b>VRID</b>	Lists a numerical index (1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
<b>Virtual IP Address</b>	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
<b>Master IP Address</b>	Displays the IP address of the elected VRRP master. A VRRP master (once elected) responds to ARP requests, forwards packets with a destination link layer MAC address equal to the virtual router MAC address, rejects packets addressed to the IP address associated with the virtual router and accepts packets addressed to the IP address associated with the virtual router.



4. Refer to the **General** field to assess the **Monitor Interval** used to poll for updates from critical resources and the **Source IP For Port-Limited Monitoring** of critical resources.

The access point **Critical Resource** screen displays the following:

<b>Critical Resource Name</b>	Lists the name of the critical resource monitored by the access point. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by access points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.
<b>Via</b>	Lists the VLAN used by the critical resource as a virtual interface. The critical resource displays as a link that can be selected to list configuration and network address information in greater detail.
<b>Status</b>	Defines the operational state of each listed critical resource VLAN interface (either <i>Up</i> or <i>Down</i> ).
<b>Error Reason</b>	Provides an error status as to why the critical resource is not available over its designated VLAN.
<b>Mode</b>	Displays the operational mode of each listed critical resource.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.18 LDAP Agent Status

#### ▶ Access Point Statistics

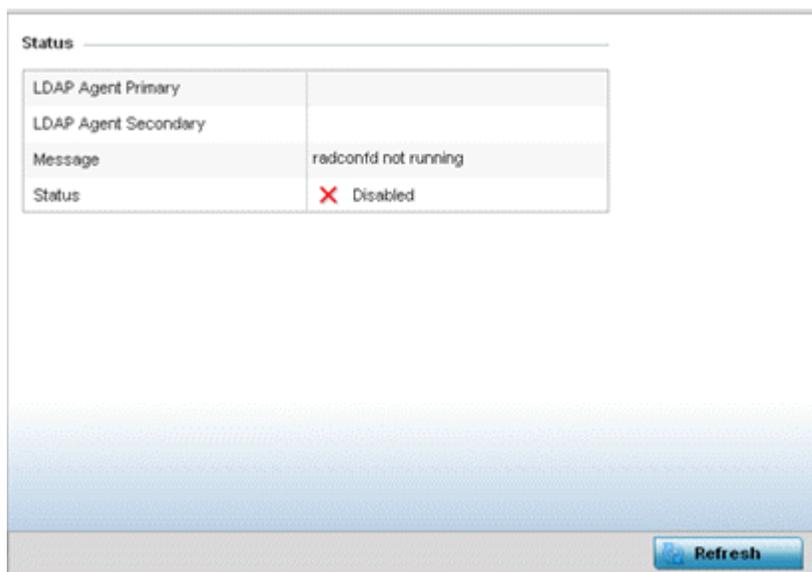
When LDAP has been specified as an external resource (as opposed to local access point RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.

AP6511 and AP6521 model access point do not support this feature in Standalone AP or Controller AP mode. However, AP6511 and AP6521 models are supported when adopted and managed by a controller or service platform.

For more information on setting LDAP agents as part of the RADIUS server policy, see [Configuring the RADIUS Server on page 9-41](#).

To view access point LDAP agent statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **LDAP Agent Status**.



**Figure 13-61** Access Point - LDAP Agent Status screen

The **LDAP Agent Status** screen displays the following:

<b>LDAP Agent Primary</b>	Lists the primary IP address of a remote LDAP server resource used by the access point to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the first resource for authentication requests.
<b>LDAP Agent Secondary</b>	Lists the secondary IP address of a remote LDAP server resource used by the access point to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the second resource for authentication requests.
<b>Message</b>	Displays any system message generated in the access point's connection with the primary or secondary LDAP agent. If there's a problem with the username and password used to connection to the LDAP agent, it would be listed here.
<b>Status</b>	Displays whether the access point has successfully joined the remote LDAP server domain designated to externally validate PEAP-MS-CHAP v2 authentication requests.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.

### 13.3.19 GRE Tunnels

#### ► Access Point Statistics

*Generic Routing Encapsulation* (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

To review a selected access point's GRE statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **GRE Tunnels**.

GRE Tunnels	
GRE State	
Peer IP Address	
Tunnel Id	
Total Packet Received	
Total Packet Sent	
Total Packet Dropped	

**Figure 13-62** Access Point - GRE Tunnels screen

The Access Point **GRE Tunnels** screen displays the following:

<b>GRE State</b>	Displays the current operational state of the GRE tunnel.
<b>Peer IP Address</b>	Displays the IP address of the peer device on the remote end of the GRE tunnel.
<b>Tunnel Id</b>	Displays the session ID of an established GRE tunnel. This ID is only viable while the tunnel is operational.
<b>Total Packets Received</b>	Displays the total number of packets received from a peer at the remote end of the GRE tunnel.
<b>Total Packets Sent</b>	Displays the total number of packets sent from this access point to a peer at the remote end of the GRE tunnel.
<b>Total Packets Dropped</b>	Lists the number of packets dropped from tunneled exchanges between this access point and a peer at the remote end of the VPN tunnel
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest value.

### 13.3.20 Dot1x

#### ► Access Point Statistics

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing to manually login.

To view the Dot1x statistics:

1. Select the **Statistics** menu from the Web UI.

2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Dot1x** from the left-hand side of the UI.

**Dot1xAuth**

AAA Policy	
Guest Vlan control	✗
System Auth Control	✗

**Dot1x Auth Ports**

Name	Auth SM	Auth VLAN	BESM	Client MAC	Guest VLAN	Host	Pstatus
ge1	force aut	0	request	N/A	0	single	authorized
ge2	force aut	0	request	N/A	0	single	authorized

**MacAuth**

AAA Policy	
------------	--

**Mac Auth Ports**

Name	Authorized	Enabled	MAC Auth
ge1	✗	✗	00-00-00-00-00-00
ge2	✗	✗	00-00-00-00-00-00

Refresh

**Figure 13-63** Access Point – Dot1x screen

4. Refer to the following **Dot1xAuth** statistics:

<b>AAA Policy</b>	Lists the AAA policy currently being utilized for authenticating user requests.
<b>Guest Vlan Control</b>	Lists whether guest VLAN control has been allowed (or enabled). This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled. A green checkmark designates guest VLAN control as enabled. A red X defines guest VLAN control as disabled.
<b>System Auth Control</b>	Lists whether Dot1x authorization is globally enabled for the access point. A green checkmark designates Dot1x authorization globally enabled. A red X defines Dot1x as globally disabled.

5. Review the following **Dot1x Auth Ports** utilization information:

<b>Name</b>	Lists the access point ge ports subject to automatic connection and authentication using Dot1x.
<b>Auth SM</b>	Lists the current authentication state of the listed port.
<b>Auth VLAN</b>	Lists the virtual interface utilized post authentication.

<b>BESM</b>	Lists whether an authentication request is pending on the listed port.
<b>Client MAC</b>	Lists the MAC address of requesting clients seeking authentication over the listed port.
<b>Guest VLAN</b>	Lists the guest VLAN utilized for the listed port. This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled.
<b>Host</b>	Lists whether the host is a single entity or not.
<b>Pstatus</b>	Lists whether the listed port has been authorized for Dot1x network authentication.

6. Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.
7. Review the following **MAC Auth Ports** utilization information:

<b>Name</b>	Lists the access point ge ports subject to automatic connection and MAC authentication using Dot1x.
<b>Authorized</b>	Lists whether MAC authorization using Dot1x has been authorized (permitted) on the listed ge port. A green checkmark designates Dot1x authorization as authorized. A red X defines authorization as disabled.
<b>Enabled</b>	Lists whether MAC authorization using Dot1x has been enabled on the listed ge port. A green checkmark designates Dot1x authorization as allowed. A red X defines authorization as disabled.
<b>MAC Auth</b>	Lists the MAC address corresponding to the listed access point port interface on which authentication requests are made.

8. Select the **Refresh** button to update the screen's statistics counters to their latest value.

## 13.3.21 Network

### ▶ Access Point Statistics

Use the *Network* screen to view information for performance statistics for ARP, DHCP, Routing and Bridging. For more information, refer to the following:

- [ARP Entries](#)
- [Route Entries](#)
- [Bridge](#)
- [IGMP](#)
- [DHCP Options](#)
- [Cisco Discovery Protocol](#)
- [Link Layer Discovery Protocol](#)

### 13.3.21.1 ARP Entries

#### ▶ Network

*Address Resolution Protocol* (ARP) is a protocol for mapping an IP address to a device address recognized in the local network. An address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a MAC address.) A table, usually called the ARP cache, is used to maintain a

correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view an access point's ARP statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Network** and expand the menu to reveal its submenu items.
4. Select **ARP Entries**.

IP Address	ARP MAC Address	Type	VLAN
172.168.6.10	00-16-C7-86-A2-40	Dynamic	vlan1

Type to search in tables Row Count: 1

[Refresh](#)

**Figure 13-64** Access Point - Network ARP screen

The **ARP Entries** screen describes the following:

<b>IP Address</b>	Displays the IP address of the client resolved on behalf of the access point.
<b>ARP MAC Address</b>	Displays the MAC address corresponding to the IP address being resolved.
<b>Type</b>	Lists the type of ARP entry.
<b>VLAN</b>	Displays the system assigned VLAN ID where an IP address was found.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.21.2 Route Entries

#### ► *Network*

The *Route Entries* screen displays the destination subnet, gateway, and interface for routing packets to a defined destination. When an existing destination subnet does not meet the needs of the network, add a new destination subnet, subnet mask and gateway.

To view route entries:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.



- Permits access to other networks
- Times out old logins

The Bridging screen also provides information about the *Multicast Router* (MRouter), which is a router program that distinguishes between multicast and unicast packets and how they should be distributed along the Multicast Internet. Using an appropriate algorithm, a multicast router instructs a switching device what to do with the multicast packet.

To view an access point's Bridge statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Network** and expand the menu to reveal its sub menu items.
4. Select **Bridge**.

Bridge Name	MAC Address	Interface	VLAN	Forwarding
1	B4-C7-99-71-16-30	ge1	38	forward
1	B4-C7-99-71-16-30	ge1	37	forward
1	B4-C7-99-57-F5-F0	ge1	39	forward
1	00-23-68-31-29-EC	ge1	1	forward
1	00-16-C7-86-A2-07	ge1	38	forward
1	5C-0E-8B-34-71-10	ge1	1	forward
1	5C-0E-8B-34-78-54	ge1	36	forward
1	B4-C7-99-58-64-A0	ge1	1	forward
1	B4-C7-99-58-64-A0	ge1	36	forward
1	5C-0E-8B-0E-3C-40	ge1	40	forward
1	00-A0-F8-66-E9-0F	ge1	1	forward
1	5C-0E-8B-0E-3C-40	ge1	37	forward
1	00-23-68-31-29-EC	ge1	1	forward

Type to search in tables Row Count: 55

[Refresh](#)

**Figure 13-66** Access Point - Network Bridge screen

5. Review the following bridge configuration attributes:

<b>Bridge Name</b>	Displays the numeric ID of the network bridge.
<b>MAC Address</b>	Displays the MAC address of the bridge selected.
<b>Interface</b>	Displays the interface (access point physical port name) where the bridge transferred packets. Supported access point models have different port configurations.
<b>VLAN</b>	Displays the VLAN the bridge uses a virtual interface.
<b>Forwarding</b>	Displays whether the bridge is forwarding packets.

6. Select **Refresh** to update the counters to their latest values.

### 13.3.21.4 IGMP

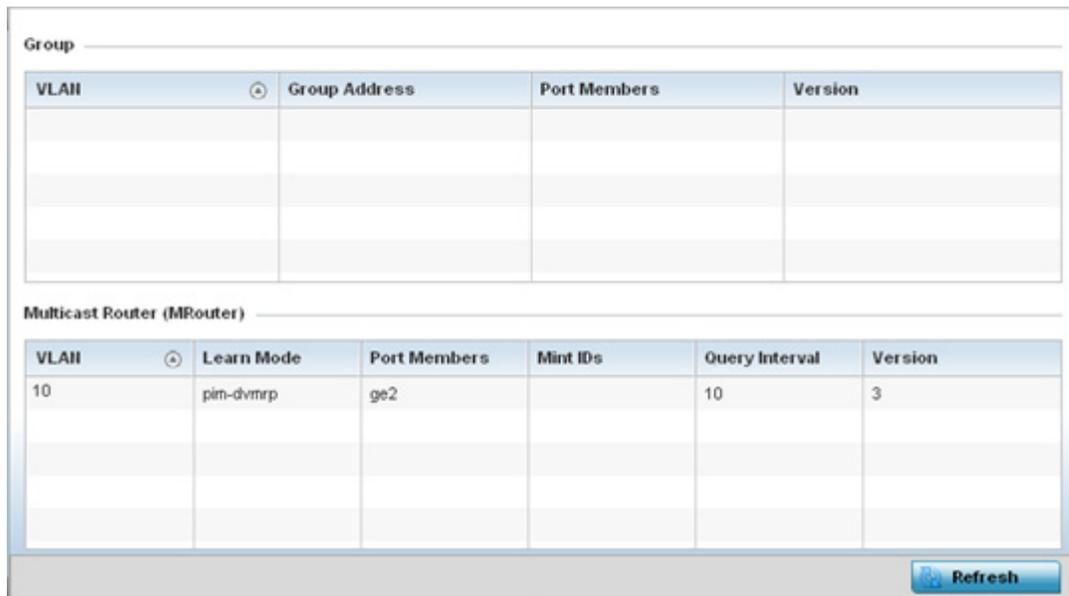
#### ► Network

*Internet Group Management Protocol* (IGMP) is a protocol used for managing members of IP multicast groups. The access point listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the interested hosts are connected.

On the wired side of the network, the access point floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network

To view a network's IGMP configuration:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Network** and expand the menu to reveal its sub menu items.
4. Select **IGMP**.



**Figure 13-67** Access Point - Network IGMP screen

The **Group** field displays the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Group Address</b>	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address that hosts are listening to.
<b>Port Members</b>	Displays the ports on which multicast clients have been discovered by the access point. For example, ge1, radio1, etc.
<b>Version</b>	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field displays the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Learn Mode</b>	Displays the learning mode used by the router as either <i>Static</i> or <i>PIM-DVMRP</i> .
<b>Port Members</b>	Displays the ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc.



The **DHCP Options** screen displays the following:

<b>Server Information</b>	Displays the DHCP server hostname used on behalf of the access point.
<b>Image File</b>	Displays the image file name. BOOTP or the bootstrap protocol can be used to boot diskless clients. An image file is sent from the boot server. The image file contains the image of the operating system the client will run. DHCP servers can be configured to support BOOTP.
<b>Configuration</b>	Displays the name of the configuration file on the DHCP server.
<b>Legacy Adoption</b>	Displays historical device adoption information on behalf of the access point.
<b>Adoption</b>	Displays adoption information on behalf of the access point.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.21.6 Cisco Discovery Protocol

#### ▶ Network

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To view an access point's CDP statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Network** and expand the menu to reveal its sub menu items.
4. Select **Cisco Discovery Protocol**.

Capabilities	Device ID	Local Port	Platform	Port ID	TTL
switch igmp_cap rc	Switch	ge1	cisco WS-C3560-2	FastEthernet0/5	121

Type to search in tables Row Count: 1

**Figure 13-69** Access Point - Network CDP screen

The **Cisco Discovery Protocol** screen displays the following:

<b>Capabilities</b>	Displays the capabilities code for the device as either <i>Router</i> , <i>Trans Bridge</i> , <i>Source Route Bridge</i> , <i>Host</i> , <i>IGMP</i> or <i>Repeater</i> .
<b>Device ID</b>	Displays the configured device ID or name for each listed device.
<b>Local Port</b>	Displays the local port name (access point physical port) for each CDP capable device. Supported access point models have unique port configurations.
<b>Platform</b>	Displays the model number of the CDP capable device interoperating with the access point.
<b>Port ID</b>	Displays the access point's numeric identifier for the local port.
<b>TTL</b>	Displays the <i>time to live</i> (TTL) for each CDP connection.
<b>Clear Neighbors</b>	Select <i>Clear Neighbors</i> to remove CDP neighbors from the table and begin a new data collection.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.



### 13.3.22 DHCP Server

► [Access Point Statistics](#)

Access points contain an internal *Dynamic Host Configuration Protocol* (DHCP) server. DHCP can provide IP addresses automatically. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters (IP address, network mask gateway etc.) from a DHCP server to a host.

To view DHCP server statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **DHCP** and expand the menu to reveal its sub menu items.
4. Select **General**.

**Status**

Interfaces	ge1
State	s1

**DDNS Bindings**

IP Address	Name
210.200.20.221	DDNS5

**DHCP Manual Bindings**

IP Address	Client Id
1.2.3.4	clientname
1.2.3.5	clientname2

[Refresh](#)

**Figure 13-71** Access Point - DHCP Server General screen

The **Status** table defines the following:

<b>Interfaces</b>	Displays the access point interface used with the DHCP resource for IP address provisioning.
<b>State</b>	Displays the current operational state of the DHCP server to assess its availability as a viable IP provisioning resource.

5. The **DDNS Bindings** table displays the following:

<b>IP Address</b>	Displays the IP address assigned to the requesting client.
<b>Name</b>	Displays the domain name mapping corresponding to the listed IP address.

6. The **DHCP Manual Bindings** table displays the following:

<b>IP Address</b>	Displays the IP address for clients requesting DHCP provisioning resources.
<b>Client Id</b>	Displays the client's ID used to differentiate requesting clients.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.



### 13.3.22.2 DHCP Networks

▶ *DHCP Server*

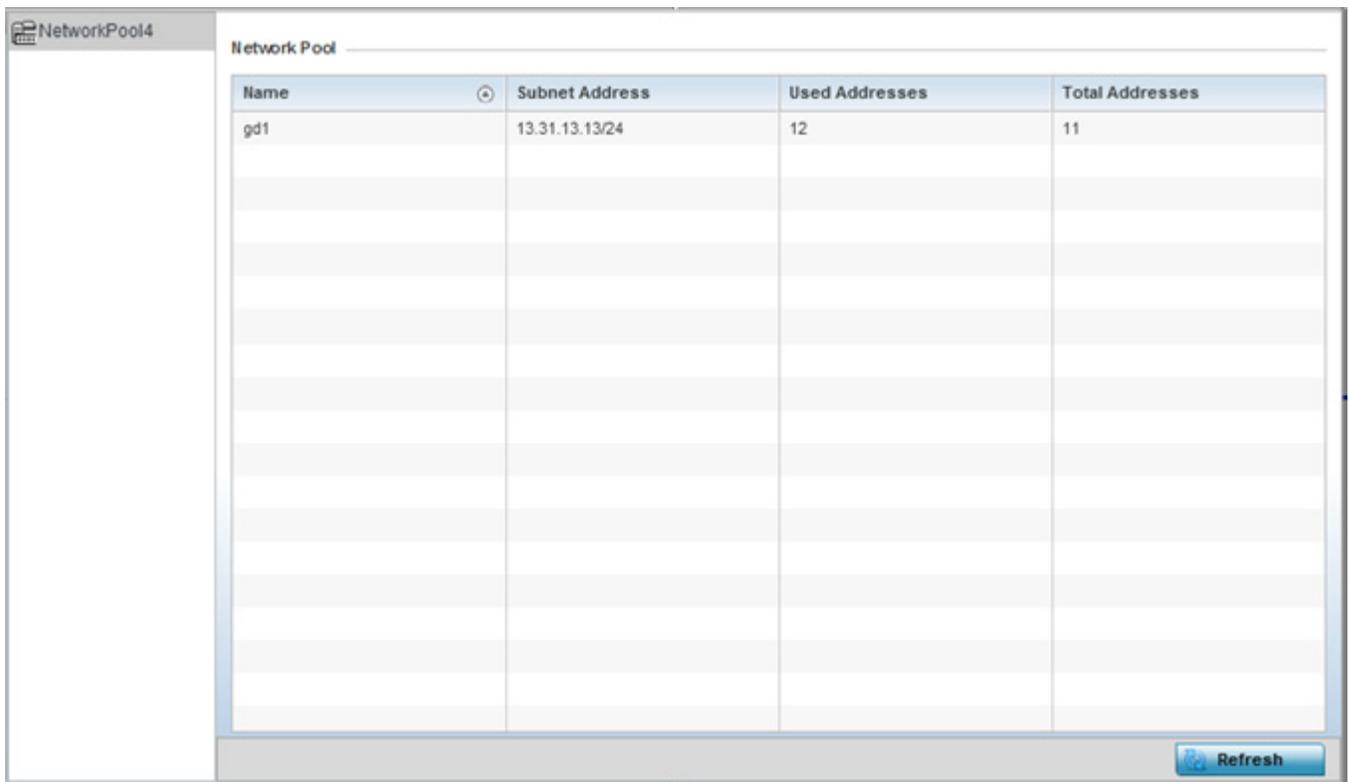
The DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers etc). On receiving a valid client request, the server assigns the computer an IP address, a lease (the validity of time), and other IP configuration parameters.

The Networks screen provides network pool information such as the subnet for the addresses you want to use from the pool, the pool name, the used addresses and the total number of addresses.

To view a network’s DHCP Networks:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain and select one of its connected access points.
3. Select **DHCP** and expand the menu to reveal its sub menu items.
4. Select **Networks**.

The *DHCP Networks* screen displays the following:



**Figure 13-73** Access Point - DHCP Network screen

<b>Name</b>	Displays the name of the DHCP pool.
<b>Subnet Address</b>	Displays the subnet addresses of the DHCP Pool.
<b>Used Addresses</b>	Number of addresses that have already been leased to requesting clients.
<b>Total Addresses</b>	Total available addresses that can be leased to requesting clients.
<b>Refresh</b>	Select <i>Refresh</i> to update the statistics counters to their latest values.

### **13.3.23 Firewall**

▶ *Access Point Statistics*

A firewall is a part of a computer system or network designed to block unauthorized access while permitting authorized communications. It's a device or set of devices configured to permit or deny access to the controller or service platform managed network based on a defined set of rules.

This screen is partitioned into the following:

- *Packet Flows*
  - *Denial of Service*
  - *IP Firewall Rules*
  - *MAC Firewall Rules*
  - *NAT Translations*
  - *DHCP Snooping*
-

### 13.3.23.1 Packet Flows

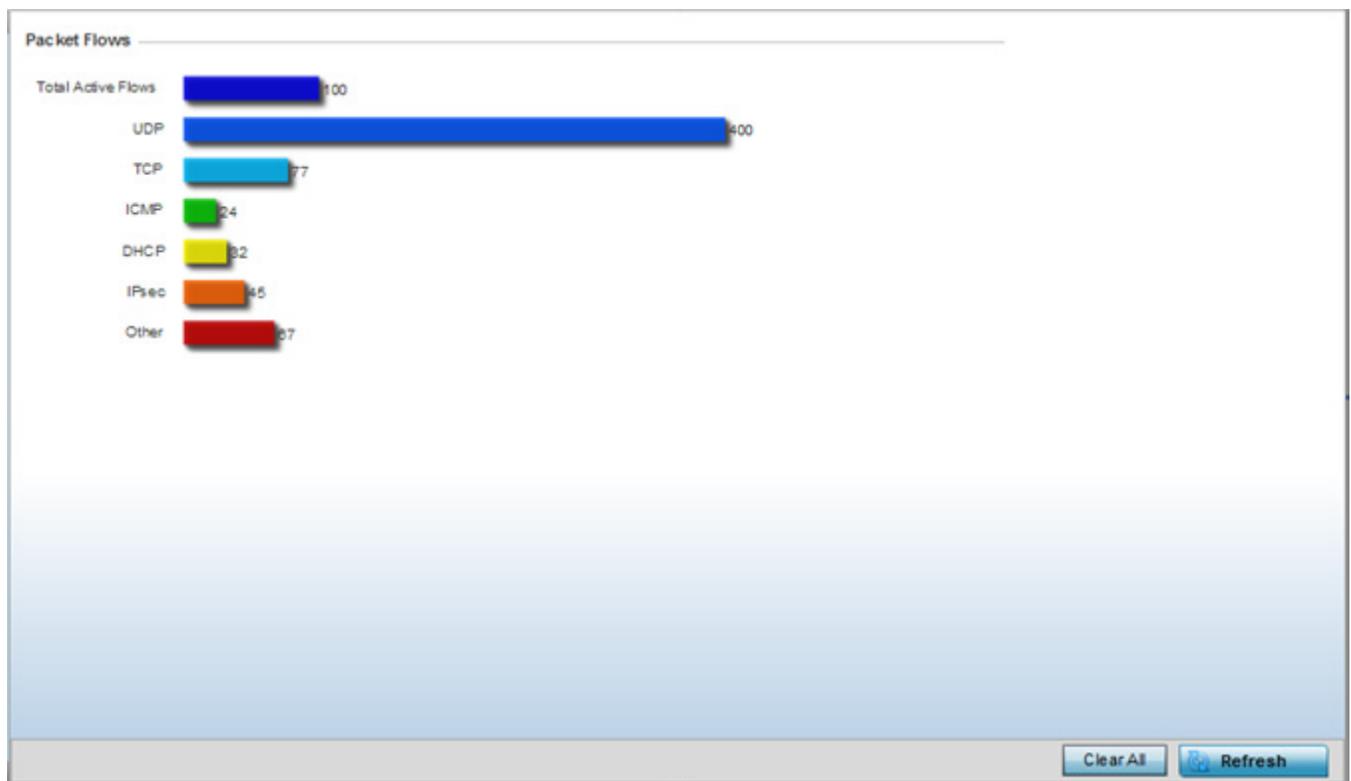
#### ► Firewall

The *Packet Flows* screen displays data traffic packet flow utilization. The chart represents the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized.

The **Total Active Flows** graph displays the total number of flows supported. Other bar graphs display for each individual packet type.

To view access point packet flows statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Firewall** and expand the menu to reveal its sub menu items.
4. Select **Packet Flows**.
5. Periodically select **Refresh** to update the statistics counters to their latest values. **Clear All** clears all the statistics counters and begins a new data collection.



**Figure 13-74** Access Point - Firewall Packet Flows screen

### 13.3.23.2 Denial of Service

#### ► Firewall

A *denial-of-service attack* (DoS attack) or distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out a DoS attack may vary, it generally consists of concerted efforts to prevent an Internet site or service from functioning efficiently.

One common method involves saturating the target's machine with external communications requests, so it cannot respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable. DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so it can't provide its intended service.

The DoS screen displays the types of attack, number of times it occurred and the time of last occurrence.

To view access point DoS attack information:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Firewall** and expand the menu to reveal its sub menu items.
4. Select **Denial of Service**.

Attack Type	Count	Last Occurrence
Ascend	0	Never
Broadcast/Multicast ICMP	0	Never
Chargen	0	Never
Fraggle	0	Never
FTP Bounce	0	Never
Router Solicit	0	Never
Invalid Protocol	0	Never
LAND	0	Never
Router Advertisement	0	Never
Smurf	0	Never
Snork	0	Never
Source Route	0	Never
IP Spoof	0	Never
TCP Bad Sequence	0	Never

Type to search in tables Row Count: 25

[Clear All](#) [Refresh](#)

**Figure 13-75** Access Point - Firewall Denial of Service screen

The **Denial of Service** screen displays the following:

<b>Attack Type</b>	Displays the <i>Denial of Service</i> (DoS) attack type.
<b>Count</b>	Displays the number of times the access point's firewall has detected each listed DoS attack.
<b>Last Occurrence</b>	Displays the when the attack event was last detected by the access point firewall.
<b>Clear All</b>	Select the <i>Clear All</i> button to clear the screen of its current status and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.23.3 IP Firewall Rules

► *Firewall*

Create firewall rules to let any computer to send traffic to, or receive traffic from, programs, system services, computers or users. Firewall rules can be created to take one of the three actions listed below that match the rule’s criteria:

- *Allow a connection*
- *Allow a connection only if it is secured through the use of Internet Protocol security*
- *Block a connection*

Rules can be created for either inbound or outbound traffic. To view the IP firewall rules:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Firewall** and expand the menu to reveal its sub menu items.
4. Select **IP Firewall Rules**.

Precedence	Friendly String	Hit Count
10	permit tcp any any rule-precedence	0
11	permit udp any eq 67 any eq dhcp	0
20	deny udp any range 137 138 any r	0
21	deny ip any 224.0.0.0/4 rule-prece	0
22	deny ip any host 255.255.255.255 i	0
100	permit ip any any rule-precedence	0

**Figure 13-76** Access Point - Firewall IP Firewall Rules screen

The **IP Firewall Rules** screen displays the following:

<b>Precedence</b>	Displays the precedence value applied to packets. The rules within an <i>Access Control Entries</i> (ACL) list are based on precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence.
<b>Friendly String</b>	The friendly string provides information as to which firewall the rules apply.
<b>Hit Count</b>	Displays the number of times each firewall rule has been triggered.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen’s statistics counters to their latest values.

### 13.3.23.4 MAC Firewall Rules

#### ► Firewall

The ability to allow or deny access point connectivity by client MAC address ensures malicious or unwanted clients are unable to bypass the access point's security filters. Firewall rules can be created to support one of the three actions listed below that match the rule's criteria:

- Allow a connection
- Allow a connection only if it's secured through the MAC firewall security
- Block a connection

To view the access point's MAC Firewall Rules:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Firewall** and expand the menu to reveal its sub menu items.
4. Select **MAC Firewall Rules**.

Precedence	Friendly String	Hit Count
	firewall1	10

**Figure 13-77** Access Point - Firewall MAC Firewall Rules screen

The **MAC Firewall Rules** screen displays the following information:

<b>Precedence</b>	Displays a precedence value, which are applied to packets. The rules within an <i>Access Control Entries</i> (ACL) list are based on their precedence. Every rule has a unique precedence between 1 and 5000. You cannot add two rules with the same precedence value.
<b>Friendly String</b>	This is a string that provides information as to which firewall the rules apply.
<b>Hit Count</b>	Displays the number of times each WLAN ACL has been triggered.



<b>Forward Dest Port</b>	Destination port for the forward NAT flow (contains ICMP ID if it is an ICMP flow).
<b>Reverse Source IP</b>	Displays the source IP address for the reverse NAT flow.
<b>Reverse Source Port</b>	Displays the source port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
<b>Reverse Dest IP</b>	Displays the destination IP address for the reverse NAT flow.
<b>Reverse Dest Port</b>	Displays the destination port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.23.6 DHCP Snooping

#### ► Firewall

When DHCP servers are allocating IP addresses to clients on the LAN, DHCP snooping can be configured to better enforce the security on the LAN to allow only clients with specific IP/MAC addresses.

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Firewall** and expand the menu to reveal its sub menu items.
4. Select **DHCP Snooping**.

	MAC Address	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since Last Update
🟢	00-16-C7-86-A	router,dhcp-sei	172.168.6.10		1		7h 58m 44s
🟢	00-16-C7-86-A	router,dhcp-sei	38.38.38.1		38		9h 33m 43s
🟢	00-40-96-A8-4f	dhcp-client,wir	38.38.0.245	16	38	1d 0h 0m 0s	9h 33m 43s
🟢	B4-C7-99-73-B	switch-SVI	172.168.6.137		1		7h 58m 44s

Type to search in tables Row Count: 4

**Figure 13-79** Access Point - Firewall DHCP Snooping screen

The **DHCP Snooping** screen displays the following:

<b>MAC Address</b>	Displays the MAC address of the client requesting DHCP resources from the controller or service platform.
<b>Node Type</b>	Displays the NetBios node from which IP addresses can be issued to client requests on this interface.
<b>IP Address</b>	Displays the IP address used for DHCP discovery, and requests between the DHCP server and DHCP clients.

<b>Netmask</b>	Displays the subnet mask used for DHCP discovery, and requests between the DHCP server and DHCP clients.
<b>VLAN</b>	Displays the VLAN used as a virtual interface for the newly created DHCP configuration.
<b>Lease Time</b>	When a DHCP server allocates an address for a DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease time is the time an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. This is useful, for example, in education and customer environments where client users change frequently. Use longer leases if there are fewer users.
<b>Time Elapsed Since Last Updated</b>	Displays the time the server was last updated.
<b>Clear All</b>	Select the <i>Clear All</i> button to clear the screen of its current status and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.



5. Review the following VPN peer security association statistics:

<b>Peer</b>	Lists peer IDs for peers sharing security associations (SA) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
<b>Version</b>	Displays each peer's IKE version used for auto IPSec secure authentication with the IPSec gateway and other controllers or service platforms.
<b>State</b>	Lists the state of each listed peer's security association (whether established or not).
<b>Lifetime</b>	Displays the lifetime for the duration of each listed peer IPSec VPN security association. Once the set value is exceeded, the association is timed out.
<b>Local IP Address</b>	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
<b>Clear All</b>	Select the <i>Clear All</i> button to clear each peer of its current status and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.24.2 IPSec

▶ [VPN](#)

Use the *IPSec VPN* screen to assess tunnel status between networked peer.

To view IPSec VPN status for tunnelled peers:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points
3. Select **VPN** and expand the menu to reveal its sub menu items.
4. Select **IPSec**.

Peer	Local IP Address	Protocol	State	SPI In	SPI Out	Mode
172.168.7.197	172.168.6.137	esp	VALID	C98E4AAB	A9DC8ACE	Tunnel

Type to search in tables Row Count: 1

**Figure 13-81** Access Point - VPN IPSec screen

5. Review the following VPN peer security association statistics:

<b>Peer</b>	Lists IP addresses for peers sharing <i>security associations</i> (SAs) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
<b>Local IP Address</b>	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
<b>Protocol</b>	Lists the security protocol used with the VPN IPsec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include <i>ESP</i> and <i>AH</i> .
<b>State</b>	Lists the state of each listed peer's security association.
<b>SPI In</b>	Lists <i>stateful packet inspection</i> (SPI) status for incoming IPsec tunnel packets. SPI tracks each connection traversing the IPsec VPN tunnel and ensures they are valid.
<b>SPI Out</b>	Lists SPI status for outgoing IPsec tunnel packets. SPI tracks each connection traversing the IPsec VPN tunnel and ensures they are valid.
<b>Mode</b>	Displays the IKE mode as either <i>Main</i> or <i>Aggressive</i> . IPSEC has two modes in IKEv1 for key exchanges. Aggressive mode requires 3 messages be exchanged between the IPSEC peers to setup the SA, Main requires 6 messages.
<b>Clear All</b>	Select the <i>Clear All</i> button to clear each peer of its current status and begin a new data collection.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

### 13.3.25 Certificates

#### ▶ [Access Point Statistics](#)

The *Secure Socket Layer* (SSL) protocol ensures secure transactions between Web servers and browsers. SSL uses a third-party certificate authority to identify one (or both) ends of a transaction. A browser checks the certificate issued by the server before establishing a connection.

This screen is partitioned into the following:

- [Trustpoints](#)
- [RSA Keys](#)

#### 13.3.25.1 Trustpoints

##### ▶ [Certificates](#)

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporate or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points
3. Select **Certificates** and expand the menu to reveal its sub menu items.
4. Select **Trustpoints**.

**Certificate Details**

Subject Name	CN=AP8132-B4-C7-99-73-BE-2C
Alternate Subject Name	
Issuer Name	CN=AP8132-B4-C7-99-73-BE-2C
Serial Number	6a
RSA Key Used	default_rsa_key
IS CA	✗ No
Is Self Signed	✓ Yes
Server Certificate Present	✓ Yes
CRL Present	✗ No

**Validity**

Valid From	08:23:2012 06:30:35 UTC
Valid Until	08:23:2013 06:30:35 UTC

**Certificate Authority (CA) Details**

Subject Name	
Alternate Subject Name	
Issuer Name	

**Refresh**

**Figure 13-82** Access Point - Certificate Trustpoint screen

The **Certificate Details** field displays the following:

<b>Subject Name</b>	Lists details about the entity to which the certificate is issued.
<b>Alternate Subject Name</b>	Displays alternative details to the information specified under the <i>Subject Name</i> field.
<b>Issuer Name</b>	Displays the name of the organization issuing the certificate.
<b>Serial Number</b>	The unique serial number of the certificate issued.
<b>RSA Key Used</b>	Displays the name of the key pair generated separately, or automatically when selecting a certificate.
<b>IS CA</b>	Indicates whether this certificate is an authority certificate (Yes/No).
<b>Is Self Signed</b>	Displays whether the certificate is self-signed (Yes/No).
<b>Server Certificate Present</b>	Displays whether a server certification is present or not (Yes/No).
<b>CRL Present</b>	Displays whether a <i>Certificate Revocation List</i> (CRL) is present (Yes/No). A CRL contains a list of subscribers paired with digital certificate status. The list displays revoked certificates along with the reasons for revocation. The date of issuance and the entities that issued the certificate are also included.

5. Refer to the **Validity** field to assess the certificate duration beginning and end dates.
6. Review the *Certificate Authority* (CA) Details and Validity information to assess the subject and certificate duration periods.
7. Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.

### 13.3.25.2 RSA Keys

#### ► Certificates

*Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption.

The *RSA Keys* screen displays a list of RSA keys installed in the selected access point. RSA Keys are generally used for establishing a SSH session, and are a part of the certificate set used by RADIUS, VPN and HTTPS.

To view the RSA Key details:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points
3. Select **Certificates** and expand the menu to reveal its sub menu items.
4. Select **RSA Keys**.



**Figure 13-83** Access Point - Certificate RSA Keys screen

The **RSA Key Details** field displays the size (in bits) of the desired key. If not specified, a default key size of 1024 is used.

The **RSA Public Key** field lists the public key used for encrypting messages.

5. Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.











<b>Remaining Time</b>	Displays the time after which the client is disconnected from the captive portal hosted Internet, and access point connectivity.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.





The **NTP Association** screen displays the following:

<b>Delay Time</b>	Displays the round-trip delay (in seconds) for broadcasts between the NTP server and the access point.
<b>Display</b>	Displays the time difference between the peer NTP server and the access point's clock.
<b>Offset</b>	Displays the calculated offset between the access point and the NTP server. The access point adjusts its clock to match the server's time value. The offset gravitates towards zero, but never completely reduces its offset to zero.
<b>Poll</b>	Displays the maximum interval between successive messages (in seconds) to the nearest power of two.
<b>Reach</b>	Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages.
<b>Reference IP Address</b>	Displays the address of the time source the access point is synchronized to.
<b>Server IP Address</b>	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the access point.
<b>State</b>	Displays the NTP association status. This can be one of the following: <ul style="list-style-type: none"> <li>• <i>Synced</i> - Indicates the access point is synchronized to this NTP server.</li> <li>• <i>Unsynced</i> - Indicates the access point has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC.</li> <li>• <i>Selected</i> - Indicates this NTP master server will be considered the next time the access point chooses a master to synchronize with.</li> <li>• <i>Candidate</i> - Indicates this NTP master server may be considered for selection the next time the access point chooses a NTP master server.</li> <li>• <i>Configured</i> - Indicates this NTP server is a configured server.</li> </ul>
<b>Status</b>	Displays how many hops the access point is from its current NTP time source.
<b>Time</b>	Displays the time of the last statistics update.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

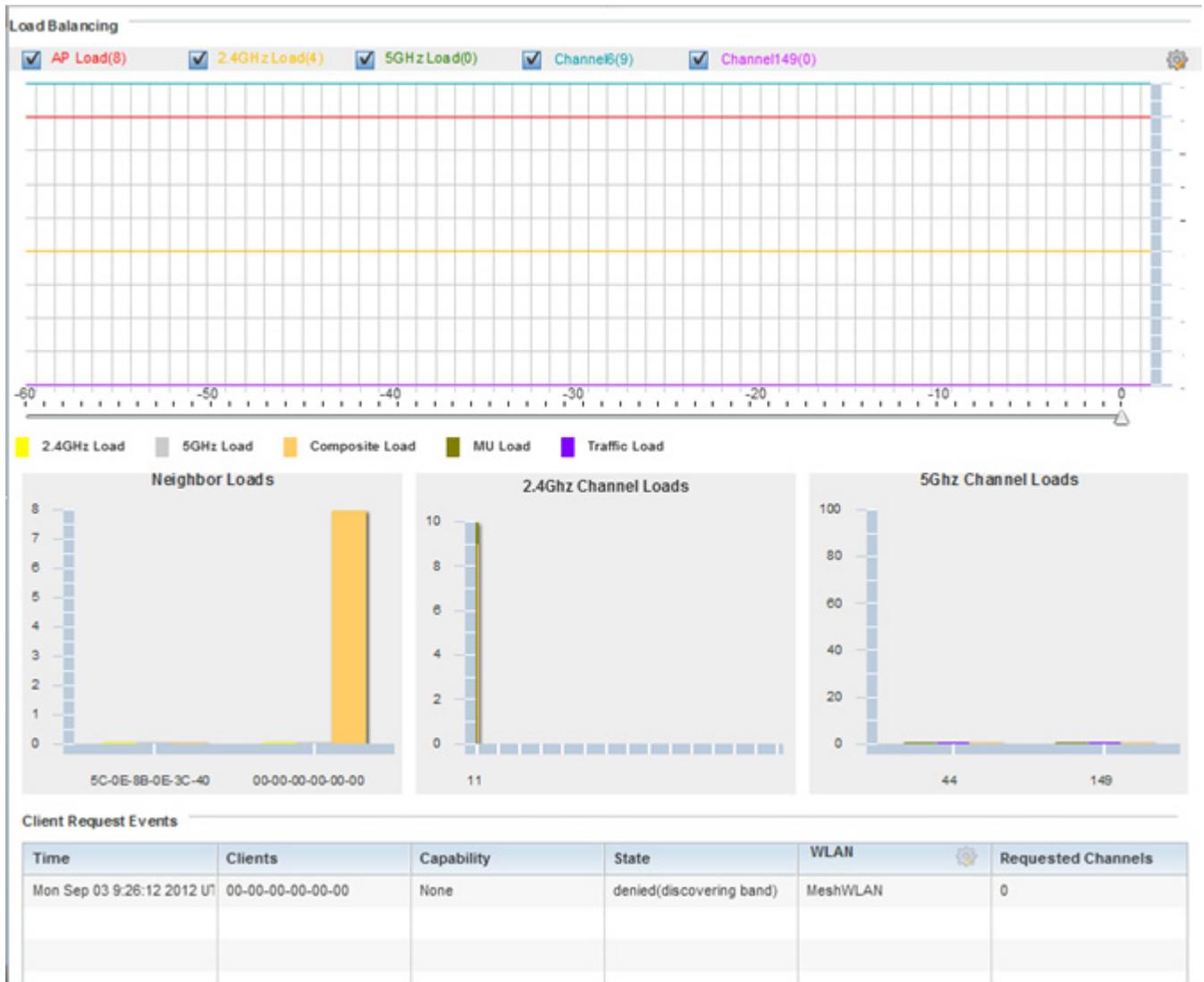
### 13.3.31 Load Balancing

#### ▶ Access Point Statistics

An access point load can be viewed in a graph and filtered to display different load attributes. The access point's entire load can be displayed, as well as the separate loads on the 2.4 and 5 GHz radio bands. The channels can also be filtered for display. Each element can either be displayed *individually* or *collectively* in the graph.

To view the access point's load balance in a filtered graph format:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.
3. Select **Load Balancing**.



**Figure 13-91** Access Point - Load Balancing screen

The **Load Balancing** screen displays the following:

<p><b>Load Balancing</b></p>	<p>Select any of the options to display any or all of the following information in the graph below: <i>AP Load</i>, <i>2.4GHz Load</i>, <i>5GHz Load</i>, and <i>Channel</i>. The graph section displays the load percentages for each of the selected variables over a period of time, which can be altered using the slider below the upper graph.</p>
<p><b>Client Requests Events</b></p>	<p>The <i>Client Request Events</i> displays the <i>Time</i>, <i>Client</i>, <i>Capability</i>, <i>State</i>, <i>WLAN</i> and <i>Requested Channels</i> for all client request events on the access point. Remember, AP6522, AP6532, AP6562, AP71XX, AP75XX, AP81XX and AP82XX models can support up to 256 clients per access point and AP6511 and AP6521 models support up to 128 clients per access point.</p>

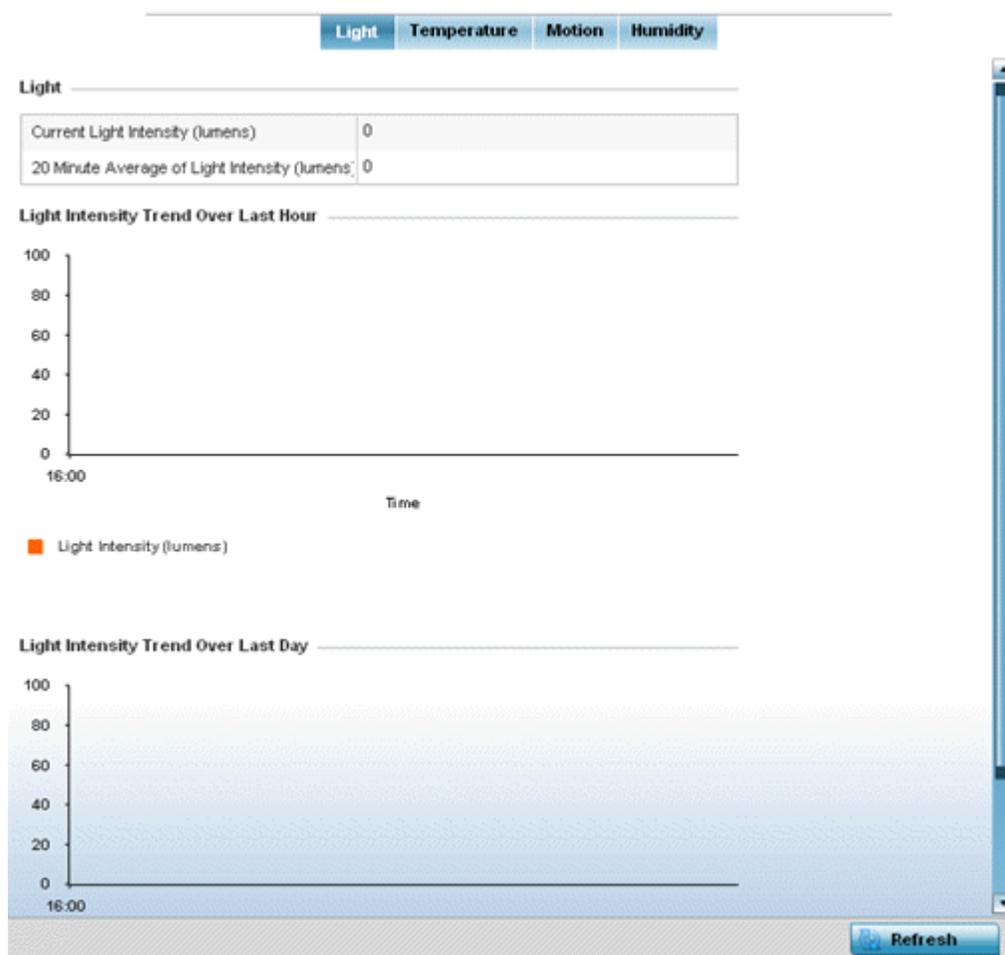
### 13.3.32 Environmental Sensors (AP8132 Models Only)

#### ► Access Point Statistics

A sensor module is a USB environmental sensor extension to an AP8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the access point's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the *Environmental Sensor* screen.

To view an AP8132 model access point's environmental statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected AP8132 access points.
3. Select **Environment**.



**Figure 13-92** Access Point - Environmental Sensor screen (Light tab)

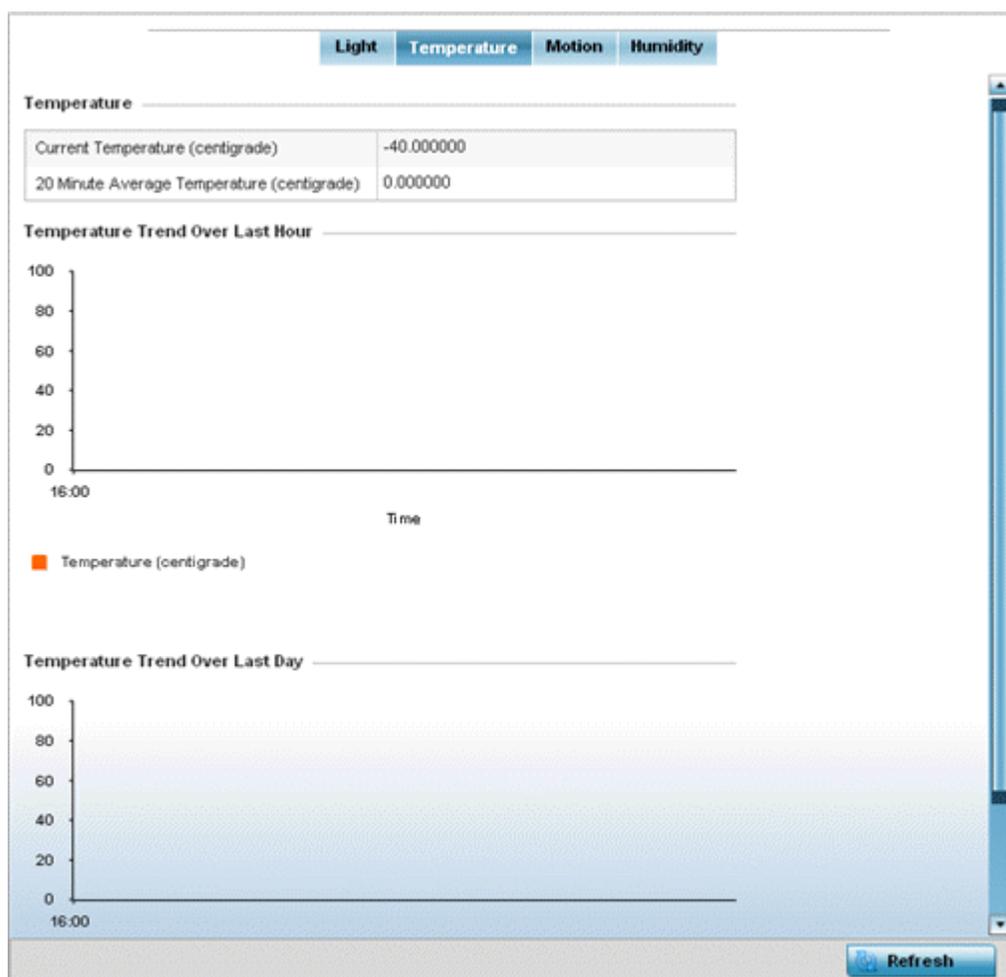
The **Light** tab displays by default, with additional *Temperature*, *Motion* and *Humidity* tabs available for unique sensor reporting. Each of these sensor measurements helps the administrator determine whether the immediate deployment area is occupied by changes in the access point's environment.

4. Refer to the **Light** table to assess the sensor's detected light intensity within the access point's immediate deployment area.

Light intensity is measured by the sensor in lumens. The table displays the **Current Light Intensity (lumens)** and a **20 Minute Average of Light Intensity (lumens)**. Compare these two items to determine whether the deployment location

remains consistently lit, as an administrator can power off the access point's radios when no activity is detected in the immediate deployment area. For more information, see [Environmental Sensor Configuration on page 5-170](#).

5. Refer to the **Light Intensity Trend Over Last Hour** graph to assess the fluctuation in lighting over the last hour. Use this graph to assess the deployment areas light intensity of particular hours of the day as needed to conjunction with the daily graph immediately below it.
6. Refer to the **Light Intensity Trend Over Last Day** graph to assess whether lighting is consistent across specific hours of the day. Use this information to help determine whether the access point can be upgraded or powered off during specific hours of the day.
7. Select the **Temperature** tab.



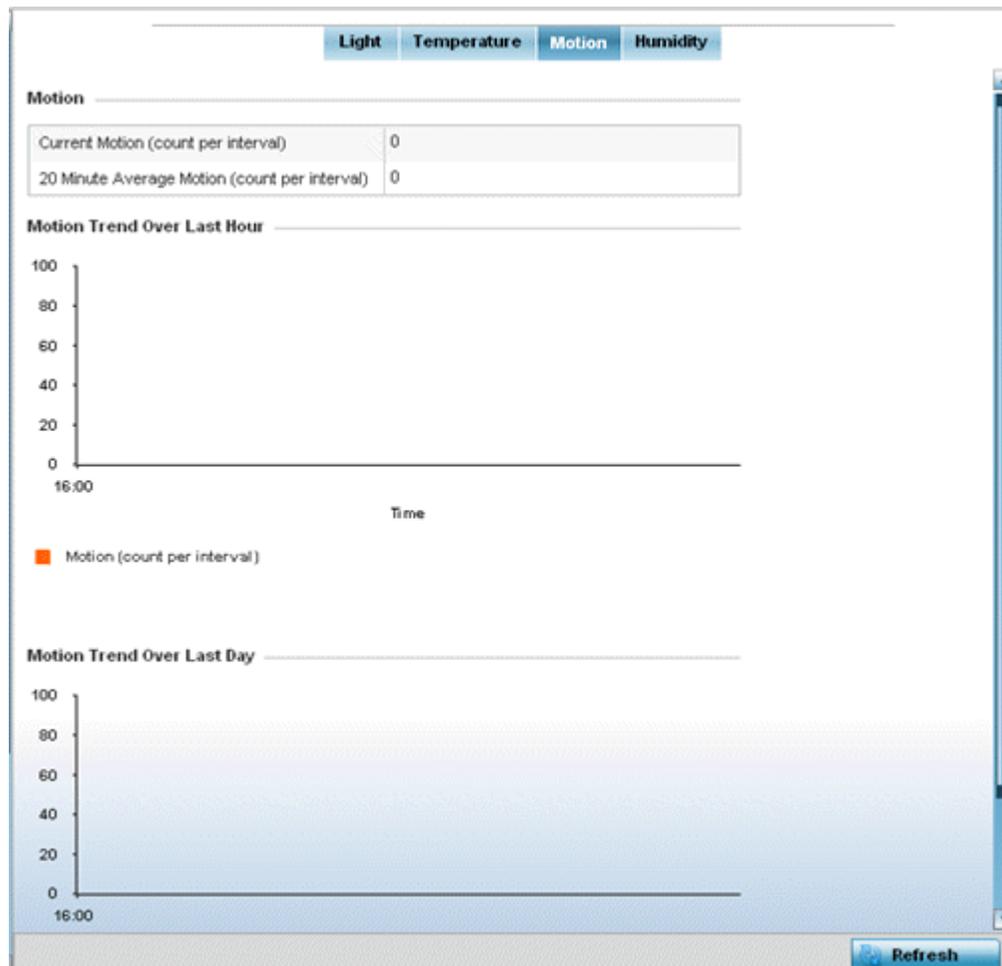
**Figure 13-93** Access Point - Environmental Sensor screen (Temperature tab)

8. Refer to the **Temperature** table to assess the sensor's detected temperature within the access point's immediate deployment area.

Temperature is measured in centigrade. The table displays the **Current Temperature (centigrade)** and a **20 Minute Average Temperature (centigrade)**. Compare these two items to determine whether the access point's deployment location remains consistently heated. For more information on enabling the sensor, see [Environmental Sensor Configuration on page 5-170](#).

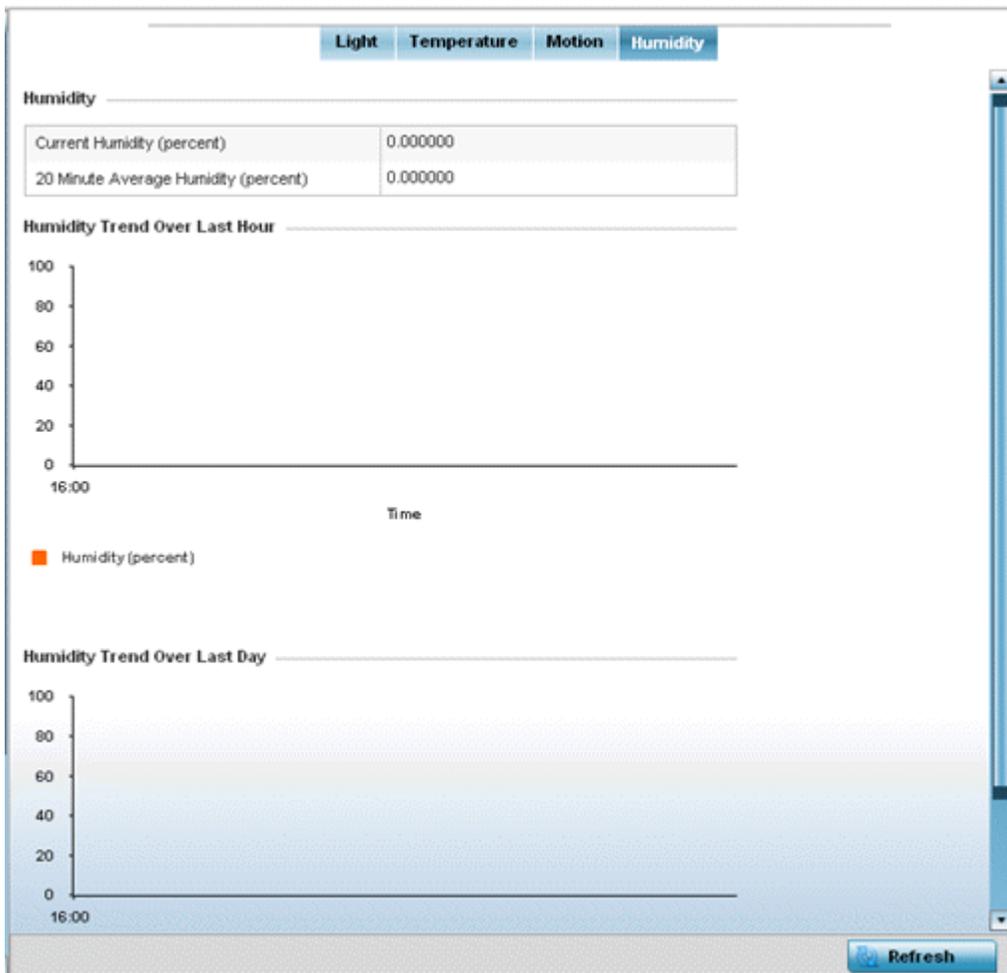
9. Refer to the **Temperature Trend Over Last Hour** graph to assess the fluctuation in ambient temperature over the last hour. Use this graph in combination with the Light and Motions graphs (in particular) to assess the deployment area's activity level.

10. Refer to the **Temperature Trend Over Last Day** graph to assess whether deployment area temperature is consistent across specific hours of the day. Use this information to help determine whether the access point can be upgraded or powered off during specific hours of the day.
11. Select the **Motion** tab.



**Figure 13-94** Access Point - Environmental Sensor screen (Motion tab)

12. Refer to the **Motion** table to assess the sensor's detected movement within the access point's immediate deployment area. Motion is measured in intervals. The table displays the **Current Motion (count per interval)** and a **20 Minute Average Motion (count per interval)**. Compare these two items to determine whether the access point's deployment location remains consistently occupied by client users. For more information on enabling the sensor, see [Environmental Sensor Configuration on page 5-170](#).
13. Refer to the **Motion Trend Over Last Hour** graph to assess the fluctuation in user movement over the last hour. Use this graph in combination with the Light and Temperature graphs (in particular) to assess the deployment area's activity level.
14. Refer to the **Motion Trend Over Last Day** graph to assess whether deployment area user movement is consistent across specific hours of the day. Use this information to help determine whether the access point can be upgraded or powered off during specific hours of the day.
15. Select the **Humidity** tab.



**Figure 13-95** Access Point - Environmental Sensor screen (Humidity tab)

16. Refer to the **Humidity** table to assess the sensor's detected humidity fluctuations within the access point's immediate deployment area.

Humidity is measured in percentage. The table displays the **Current Humidity (percent)** and a **20 Minute Average Humidity (percent)**. Compare these two items to determine whether the access point's deployment location remains consistently humid (often a by-product of temperature). For more information on enabling the sensor, see [Environmental Sensor Configuration on page 5-170](#).

17. Refer to the **Humidity Trend Over Last Hour** graph to assess the fluctuation in humidity over the last hour. Use this graph in combination with the Temperature and Motions graphs (in particular) to assess the deployment area's activity levels.
18. Refer to the **Humidity Trend Over Last Day** graph to assess whether deployment area humidity is consistent across specific hours of the day. Use this information to help determine whether the access point can be upgraded or powered off during specific hours of the day.

## 13.4 Wireless Client Statistics

### ► *Statistics*

The wireless client statistics display read-only statistics for a client selected from within its connected access point directory. It provides an overview of the health of wireless clients in the network. Use this information to assess if configuration changes are required to improve client performance.

Wireless clients statistics can be assessed using the following criteria:

- *Health*
- *Details*
- *Traffic*
- *WMM TSPEC*
- *Association History*
- *Graph*

### 13.4.1 Health

#### ► *Wireless Client Statistics*

The *Health* screen displays information on the overall performance of a selected wireless client.

To view the health of a wireless client:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select an access point, then a connected client.
3. Select **Health**.



**Figure 13-96** Wireless Client - Health screen

The **Wireless Client** field displays the following:

<b>Client MAC</b>	Displays the factory encoded MAC address of the selected wireless client.
<b>Hostname</b>	Lists the hostname assigned to the client when initially managed by the access point.
<b>Vendor</b>	Displays the vendor name (manufacturer) of the wireless client.
<b>State</b>	Displays the current operational state of the wireless client. The client's state can be <i>idle</i> , <i>authenticated</i> , <i>roaming</i> , <i>associated</i> or <i>blacklisted</i> .
<b>IP Address</b>	Displays the IP address the selected wireless client is currently utilizing as a network identifier.
<b>WLAN</b>	Displays the client's connected access point WLAN membership. This is the WLAN whose QoS settings should account for the clients's radio traffic objective.
<b>Radio MAC</b>	Displays the access point radio MAC address the wireless client is connected to on the network.
<b>VLAN</b>	Displays the VLAN ID the access point has defined for use as a virtual interface with the client.

The **User Details** field displays the following:

<b>Username</b>	Displays the unique name of the administrator or operator managing the client's connected access point, controller or service platform.
<b>Authentication</b>	Lists the authentication scheme applied to the client for interoperability with the access point.

<b>Encryption</b>	Lists the encryption scheme applied to the client for interoperation with the access point.
<b>Captive Portal Authentication</b>	Displays whether captive portal authentication is enabled for the client as a guest access medium to the controller or service platform managed network.

The **RF Quality Index** field displays the following:

<b>RF Quality Index</b>	Displays information on the RF quality for the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. RF quality index can be interpreted as: <ul style="list-style-type: none"> <li>• 0 – 20 (Very poor quality)</li> <li>• 20 – 40 (Poor quality)</li> <li>• 40 – 60 (Average quality)</li> <li>• 60 – 100 (Good quality)</li> </ul>
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
<b>SNR</b>	Displays the <i>signal to noise</i> (SNR) ratio of the connected wireless client.
<b>Signal</b>	Displays the power of the radio signals in - dBm.
<b>Noise</b>	Displays the disturbing influences on the signal by interference of signals in - dBm.
<b>Error Rate</b>	Displays the number of received bit rates altered due to noise, interference and distortion. It's a unitless performance measure.

The **Association** field displays the following:

<b>AP Hostname</b>	Lists the administrator assigned device name of the client's connected access point.
<b>AP</b>	Displays the MAC address of the client's connected access point.
<b>Radio</b>	Lists the target access point that houses the radio. Select the access point to view performance information in greater detail.
<b>Radio ID</b>	Lists the hardware encoded MAC address the radio uses as a hardware identifier that further distinguishes the radio from others within the same device.
<b>Radio Number</b>	Displays the access point's radio number (either 1, 2 or 3) to which the selected client is associated.
<b>Radio Type</b>	Displays the radio type. The radio can be 802.11b, 802.11bg, 802.11bgn, 802.11a, 802.11ac or 802.11an.

4. The **Traffic Utilization** field displays statistics on the traffic generated and received by the selected client. This area displays the traffic index, which measures how efficiently the traffic medium is utilized. It's defined as the percentage of current throughput relative to the maximum possible throughput.

Traffic indices are:

- 0 – 20 (Very low utilization)
- 20 – 40 (Low utilization)

- 40 – 60 (Moderate utilization)
- 60 and above (High utilization)

The **Traffic Utilization** table displays the following:

<b>Total Bytes</b>	Displays the total bytes processed by the access point's connected wireless client.
<b>Total Packets</b>	Displays the total number of packets processed by the wireless client.
<b>User Data Rate</b>	Displays the average user data rate in both directions.
<b>Physical Layer Rate</b>	Displays the average packet rate at the physical layer in both directions.
<b>Tx Dropped Packets</b>	Displays the number of packets dropped during transmission.
<b>Rx Errors</b>	Displays the number of errors encountered during data transmission. The higher the error rate, the less reliable the connection or data transfer between the client and connected access point.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

## 13.4.2 Details

### ▶ *Wireless Client Statistics*

The *Details* screen provides granular performance information for a selected wireless client.

To view the details screen of a connected wireless client:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select an access point, then a connected client.
3. Select **Details**.

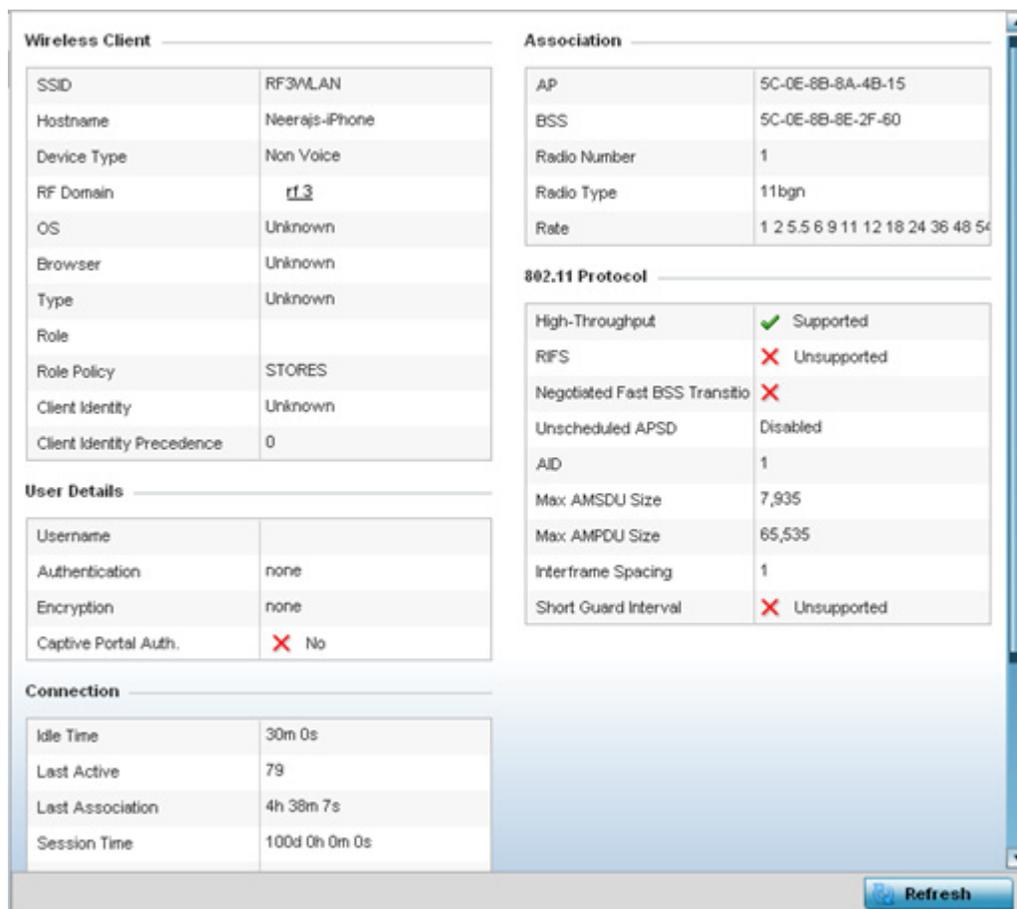


Figure 13-97 Wireless Client - Details screen

The **Wireless Client** field displays the following:

<b>SSID</b>	Displays the client's <i>Service Set ID</i> (SSID).
<b>Hostname</b>	Lists the hostname assigned to the client when initially managed by the access point managed network.
<b>Device Type</b>	Displays the client device type providing the details to the operating system.
<b>RF Domain</b>	Displays the RF Domain to which the connected client is a member via its connected access point, controller or service platform. The RF Domain displays as a link that can be selected to display configuration and network address information in greater detail.
<b>OS</b>	Lists the client's operating system (Android etc.).
<b>Browser</b>	Displays the browser type used by the client to facilitate its wireless connection.
<b>Type</b>	Lists the client manufacturer (or vendor).
<b>Role</b>	Lists the client's defined role in the network.
<b>Role Policy</b>	Lists the user role set for the client as it became a access point managed device.
<b>Client Identity</b>	Displays the unique vendor identity of the listed device as it appears to its adopting device.

<b>Client Identity Precedence</b>	Lists the numeric precedence this client uses in establishing its identity amongst its peers.
-----------------------------------	---

The **User Details** field displays the following:

<b>Username</b>	Displays the unique name of the administrator or operator managing the client's connected access point.
<b>Authentication</b>	Lists the authentication scheme applied to the client for interoperation with its connected access point radio.
<b>Encryption</b>	Lists the encryption scheme applied to the client for interoperation with its connected access point radio.
<b>Captive Portal Auth.</b>	Displays whether captive portal authentication is enabled. When enabled, a restrictive set of access permissions may be in effect.

The **Connection** field displays the following:

<b>Idle Time</b>	Displays the time for which the wireless client remained idle.
<b>Last Active</b>	Displays the time in seconds the wireless client was last interoperating with its connected access point.
<b>Last Association</b>	Displays the duration the wireless client was in association with its connected access point.
<b>Session Time</b>	Displays the duration for which a session can be maintained by the wireless client without it being dis-associated from the access point.
<b>SM Power Save Mode</b>	Displays whether this feature is enabled on the wireless client. The <i>spatial multiplexing</i> (SM) power save mode allows an 802.11n client to power down all but one of its radios. This power save mode has two sub modes of operation: <i>static operation</i> and <i>dynamic operation</i> .
<b>Power Save Mode</b>	Displays whether this feature is enabled or not. To prolong battery life, the 802.11 standard defines an optional Power Save Mode, which is available on most 802.11 clients. End users can simply turn it on or off via the card driver or configuration tool. With power save off, the 802.11 network card is generally in receive mode listening for packets and occasionally in transmit mode when sending packets. These modes require the 802.11 NIC to keep most circuits powered-up and ready for operation.
<b>WMM Support</b>	Displays whether WMM is enabled or not in order to provide data packet type prioritization between the access point and connected client.
<b>40 MHz Capable</b>	Displays whether the wireless client has 802.11n channels operating at 40 MHz.
<b>Max Physical Rate</b>	Displays the maximum data rate at the physical layer.
<b>Max User Rate</b>	Displays the maximum permitted user data rate.
<b>MC2UC Streams</b>	Lists the number of multicast to unicast data streams detected.

The **Association** field displays the following:

<b>AP</b>	Displays the MAC address of the client's connected access point.
-----------	--

<b>BSS</b>	Displays the <i>Basic Service Set</i> (BSS) the access point belongs to. A BSS is a set of stations that can communicate with one another.
<b>Radio Number</b>	Displays the access point radio the wireless client is connected to.
<b>Radio Type</b>	Displays the radio type. The radio can be 802.11b, 802.11bg, 802.11bgn, 802.11a, 802.11ac or 802.11an.
<b>Rate</b>	Displays the permitted data rate for access point and client interoperation.

The **802.11 Protocol** field displays the following:

<b>High-Throughput</b>	Displays whether high throughput is supported. High throughput is a measure of the successful packet delivery over a communication channel.
<b>RIFS</b>	Displays whether this feature is supported. RIFS is a required 802.11n feature that improves performance by reducing the amount of dead time between OFDM transmissions.
<b>Unscheduled APSD</b>	Displays whether APSD is supported. APSD defines an unscheduled service period, which is a contiguous period of time during which the access point is expected to be awake.
<b>Negotiated Fast BSS Transition</b>	Lists whether Fast BSS transition is negotiated. This indicates support for a seamless fast and secure client handoff between two access points.
<b>AID</b>	Displays the <i>Association ID</i> (AID) established by an AP. 802.11 association enables the access point to allocate resources and synchronize with a client. A client begins the association process by sending an association request to an access point. This association request is sent as a frame. This frame carries information about the client and the SSID of the network it wishes to associate. After receiving the request, the access point considers associating with the client, and reserves memory space for establishing an AID for the client.
<b>Max AMSDU Size</b>	Displays the maximum size of AMSDU. AMSDU is a set of Ethernet frames to the same destination that are wrapped in a 802.11n frame. This value is the maximum AMSDU frame size in bytes.
<b>Max AMPDU Size</b>	Displays the maximum size of AMPDU. AMPDU is a set of Ethernet frames to the same destination that are wrapped in an 802.11n MAC header. AMPDUs are used in a very noisy environment to provide reliable packet transmission. This value is the maximum AMPDU size in bytes.
<b>Interframe Spacing</b>	Displays the interval between two consecutive Ethernet frames.
<b>Short Guard Interval</b>	Displays the guard interval in micro seconds. Guard intervals prevent interference between data transmissions. The guard interval is the space between characters being transmitted. The guard interval eliminates <i>inter-symbol interference</i> (ISI). ISI occurs when echoes or reflections from one character interfere with another character. Adding time between transmissions allows echo's and reflections to settle before the next character is transmitted. A shorter guard interval results in shorter character times which reduces overhead and increases data rates by up to 10%.
<b>Refresh</b>	Select the <i>Refresh</i> button to update the screen's statistics counters to their latest values.

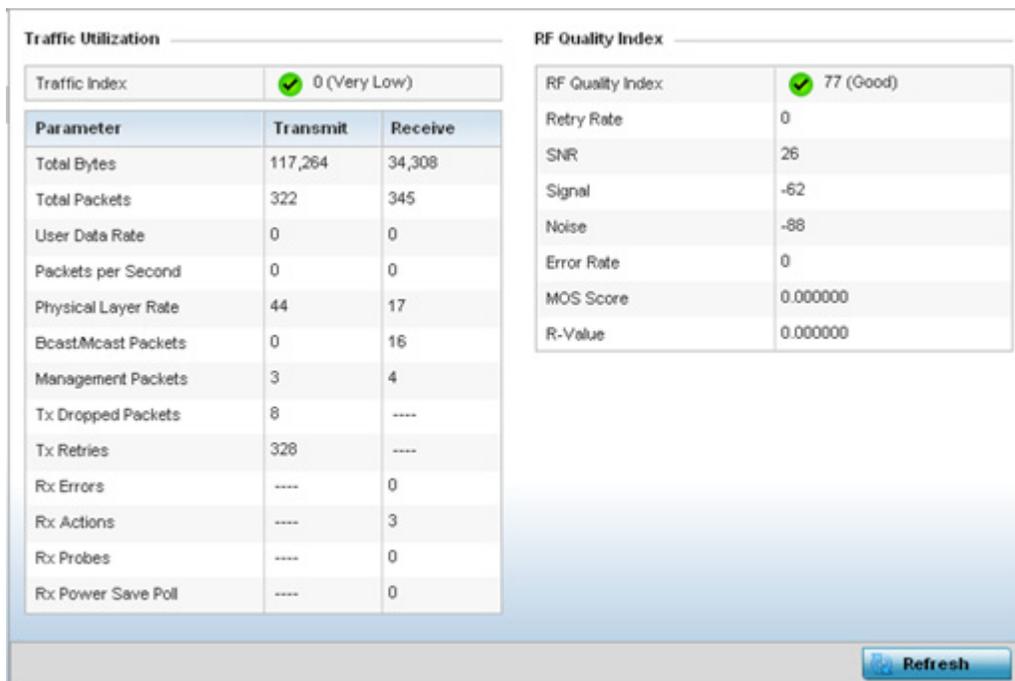
### 13.4.3 Traffic

#### ► Wireless Client Statistics

The traffic screen provides an overview of client traffic utilization in both the transmit and receive directions. This screen also displays a RF quality index.

To view the traffic statistics of a wireless clients:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, an access point, then a connected client.
3. Select **Traffic**.



**Figure 13-98** Wireless Client - Traffic screen

**Traffic Utilization** statistics employ an index, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. This screen also provides the following:

<b>Total Bytes</b>	Displays the total bytes processed (in both directions) by the access point's connected client.
<b>Total Packets</b>	Displays the total number of data packets processed (in both directions) by the access point's connected wireless client.
<b>User Data Rate</b>	Displays the average user data rate.
<b>Packets per Second</b>	Displays the packets processed per second.
<b>Physical Layer Rate</b>	Displays the data rate at the physical layer level.
<b>Bcast/Mcast Packets</b>	Displays the total number of broadcast/multicast packets processed by the client.
<b>Management Packets</b>	Displays the number of management (overhead) packets processed by the client.

<b>Tx Dropped Packets</b>	Displays the client's number of dropped packets while transmitting to its connected access point.
<b>Tx Retries</b>	Displays the total number of client transmit retries with its connected access point.
<b>Rx Errors</b>	Displays the errors encountered by the client during data transmission. The higher the error rate, the less reliable the connection or data transfer between client and connected access point.
<b>Rx Actions</b>	Displays the number of receive actions during data transmission with the client's connected access point.
<b>Rx Probes</b>	Displays the number of probes sent. A probe is a program or other device inserted at a key juncture in a for network for the purpose of monitoring or collecting data about network activity.
<b>Rx Power Save Poll</b>	Displays the power save using the <i>Power Save Poll</i> (PSP) mode. Power Save Poll is a protocol, which helps to reduce the amount of time a radio needs to powered. PSP allows the WiFi adapter to notify the access point when the radio is powered down. The access point holds any network packet to be sent to this radio.

The **RF Quality Index** area displays the following information:

<b>RF Quality Index</b>	<p>Displays information on the RF quality of the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions as well as the retry rate and the error rate. The RF quality index value can be interpreted as:</p> <ul style="list-style-type: none"> <li>• 0 – 20 (Very low utilization)</li> <li>• 20 – 40 (Low utilization)</li> <li>• 40 – 60 (Moderate utilization)</li> <li>• 60 and above (High utilization)</li> </ul>
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
<b>SNR</b>	Displays the connected client's <i>signal to noise ratio</i> (SNR). A high SNR could warrant a different access point connection to improve performance.
<b>Signal</b>	Displays the power of the radio signals in - dBm.
<b>Noise</b>	Displays the disturbing influences on the signal in - dBm.
<b>Error Rate</b>	Displays the number of received bit rates altered due to noise, interference and distortion. It's a unitless performance measure.
<b>MOS Score</b>	Displays average voice call quality using the <i>Mean Opinion Score</i> (MOS) call quality scale. The MOS scale rates call quality on a scale of 1-5, with higher scores being better. If the MOS score is lower than 3.5, it's likely users will not be satisfied with the voice quality of their call.



<b>Direction Type</b>	Displays whether the WMM TPSEC data stream is in the <i>uplink</i> or <i>downlink</i> direction.
<b>Request Time</b>	Lists each sequence number's request time for WMM TPSEC traffic in the specified direction. This is time allotted for a request before packets are actually sent.
<b>Used Time</b>	Displays the time the client used TSPEC. The client sends a <i>delete traffic stream</i> (DELTS) message when it has finished communicating.
<b>TID</b>	Displays the parameter for defining the traffic stream. TID identifies data packets as belonging to a unique traffic stream.

4. Periodically select **Refresh** to update the screen to its latest values.

### 13.4.5 Association History

► *Wireless Client Statistics*

Refer to the **Association History** screen to review this client's access point connections. Hardware device identification, operating channel and GHz band data is listed for each access point. Association history can help determine whether the client has connected to its target access point and maintained its connection, or has roamed and been supported by unplanned access points in the controller or service platform managed network.

To view a selected client's association history:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, an access point, then a connected client.
3. Select **Association History**.

Access Point	BSSID	Channel	Band	Time
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:38:49 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:35:43 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 0:32:55 2013

Type to search in tables Row Count: 3

**Refresh**

**Figure 13-100** *Wireless Client - Association History screen*

Refer to the following to discern this client's access point association history:

<b>Access Point</b>	Lists the access point MAC address this client has connected to, and is being managed by.
<b>BSSID</b>	Displays the BSSID of each previously connected access point.

<b>Channel</b>	Lists the channel shared by both the access point and client for interoperation, and to avoid congestion with adjacent channel traffic.
<b>Band</b>	Lists the 2.4 or 5GHz radio band this clients and its connect access point are using for transmit and receive operations.
<b>Time</b>	Lists the historical connection time between each listed access point and this client.

4. Select **Refresh** to update the screen to it's latest values.

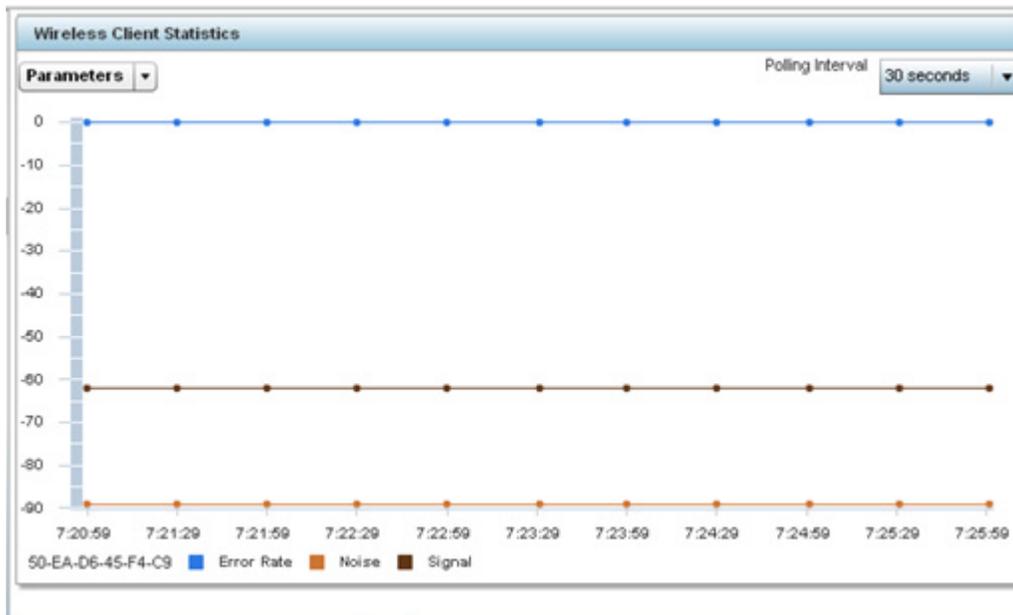
### 13.4.6 Graph

#### ► Wireless Client Statistics

Use the client **Graph** to assess a connected client's radio performance and diagnose performance issues that may be negatively impacting performance. Up to three selected performance variables can be charted at one time. The graph uses a Y-axis and a X-axis to associate selected parameters with their performance measure.

To view a graph of this client's statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, an access point then a connected client.
3. Select **Graph**.
4. Use the **Parameters** drop down menu to define from 1- 3 variables assessing client signal noise, transmit or receive values.
5. Use the **Polling Interval** drop-down menu to define the interval the chart is updated. Options include *30 seconds*, *1 minute*, *5 minutes*, *20 minutes* or *1 hour*. 30 seconds is the default value.



**Figure 13-101** Wireless Client - Graph

Select an available point in the graph to list the selected performance parameter, and display that parameter's value and a time stamp of when it occurred.

# APPENDIX A

## USING WING EXPRESS

WiNG Express is a new Motorola Solutions *User Interface* (UI) that simplifies the configuration and monitoring of small access point deployments by limiting monitoring, analytics, and configuration capabilities. WiNG Express is a simplified version of the WiNG operating system currently shipping with the Motorola Solutions family of controllers, service platforms and access point.

WiNG Express is designed for single-site access point deployments not exceeding more than 24 access points of the same model. The following network profiles are specifically targeted:

- Single AP deployment, LAN
- Single AP deployment, WAN
- Multi AP deployment, LAN
- Multi AP deployment, WAN
- Multi AP dual-port deployment, WAN

For the WiNG Express version SKUs, both the WiNG Express UI and an *over-the-air* (OTA) provisioning configuration is required. For a non WiNG Express SKU, there's no OTA configuration required, just the WiNG Express UI is utilized.

This chapter is organized as follows:

- [Dashboard](#)
- [Monitor](#)
- [Configuration](#)
- [Access Points](#)
- [Event History](#)

## A.1 Dashboard

► *Using WiNG Express*

The dashboard enables administrators to review and troubleshoot access point managed network operation. Additionally, the dashboard allows an administrator to assess network component health and conduct a diagnostic review of device performance.

To review high-level WiNG Express access point dashboard information:

1. Select **Dashboard** in the main menu.



**Figure A-1** WiNG Express - Dashboard

2. Review the following to assess the health of the WiNG Express managed network:

<b>System Information</b>	Displays the administrator assigned <i>AP Name</i> , required <i>Country Code</i> for legal geographic deployment in specific regions, number of detected <i>Offline APs</i> , whether the access point has been enabled as a Virtual Controller to manage peer access points, the designated <i>Virtual Controller MAC</i> address, <i>Current Time</i> and <i>Up Time</i> listing when the access point was last offline.
<b>Current Network Client Segmentation</b>	Displays a set of pie charts segregating the WLAN utilization amongst peer access points and client types. Use this information to help assess whether the client loads exceed the number and type of WLANs currently being deployed with WiNG Express managed access points.
<b>Network Usage</b>	Displays the network throughput (both in the transmit and receive directions) for the selected Radio or WLAN over the defined trending period of 30 minutes, 2 hours or 24 hours.

<b>Network Client Count</b>	Displays the total client count for the network over the selected time period of 30 minutes, 2 hours or 24 hours. Clients are partitioned into their current 2.4Ghz and 5Ghz radio bands to help assess whether the client load is adequately supported in each band.
-----------------------------	---

## A.2 Monitor

► *Using WiNG Express*

The **Monitor** screens provide detailed, real-time information about the network and RF health for access point Radios, WLANs and wireless clients. Use the information on these screens to track RF traffic, throughput, signal to noise ratio and client health.

This section is organized as follows:

- *Radios*
- *WLANs*
- *Clients*

## A.2.1 Radios

### ► Monitor

Use the **Radios** screen to assess the quality of the access point radio's utilization, power consumption, antenna gain and client connections.

To monitor WiNG Express managed access point radios:

1. Select **Monitor** from the main menu and click on **Radios**.
2. Select a time interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput utilization, power and signal strength.



**Figure A-2** WiNG Express - Monitor - Radios screen

3. Review the following Access Point **Radio Details**:

<b>Radio MAC Address</b>	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each radio as its hardware identifier on the network.
<b>Access Point Name</b>	Displays the access point's unique administrator assigned name provided upon initial WiNG Express management.
<b>Radio</b>	Displays the radio number for each access point radio on the network. AP6511 and AP6521 models are single radio models, remaining models support at least two radios.

<b>Channel: Current / Config</b>	Displays the current channel number each listed access point radio is set to transmit and receive on, as well as its configured channel number. The Channels available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
<b>Power (dBm): Current / Config</b>	Displays the current power level in dBm for each access point radio as well as its configured power level. If Smart is the defined power setting, the radio automatically configures power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
<b>Status</b>	Displays the current status for each access point. If an access point is up, two green up arrows display. If an access point is down, two green down arrows display.
<b>Clients</b>	Displays the number of clients currently associated to each WiNG Express access point radio on the network. AP6511 and AP6521 single radio access points support 128 clients, the remaining models support up to 256 client connections.
<b>Retry (%)</b>	Displays the retry percentage for packets sent on each access point radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connect rate in both directions.
<b>SNR</b>	Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different access point connection to improve performance.

4. Select **Details** to assess individual access point radio utilization data in greater detail.

### Details

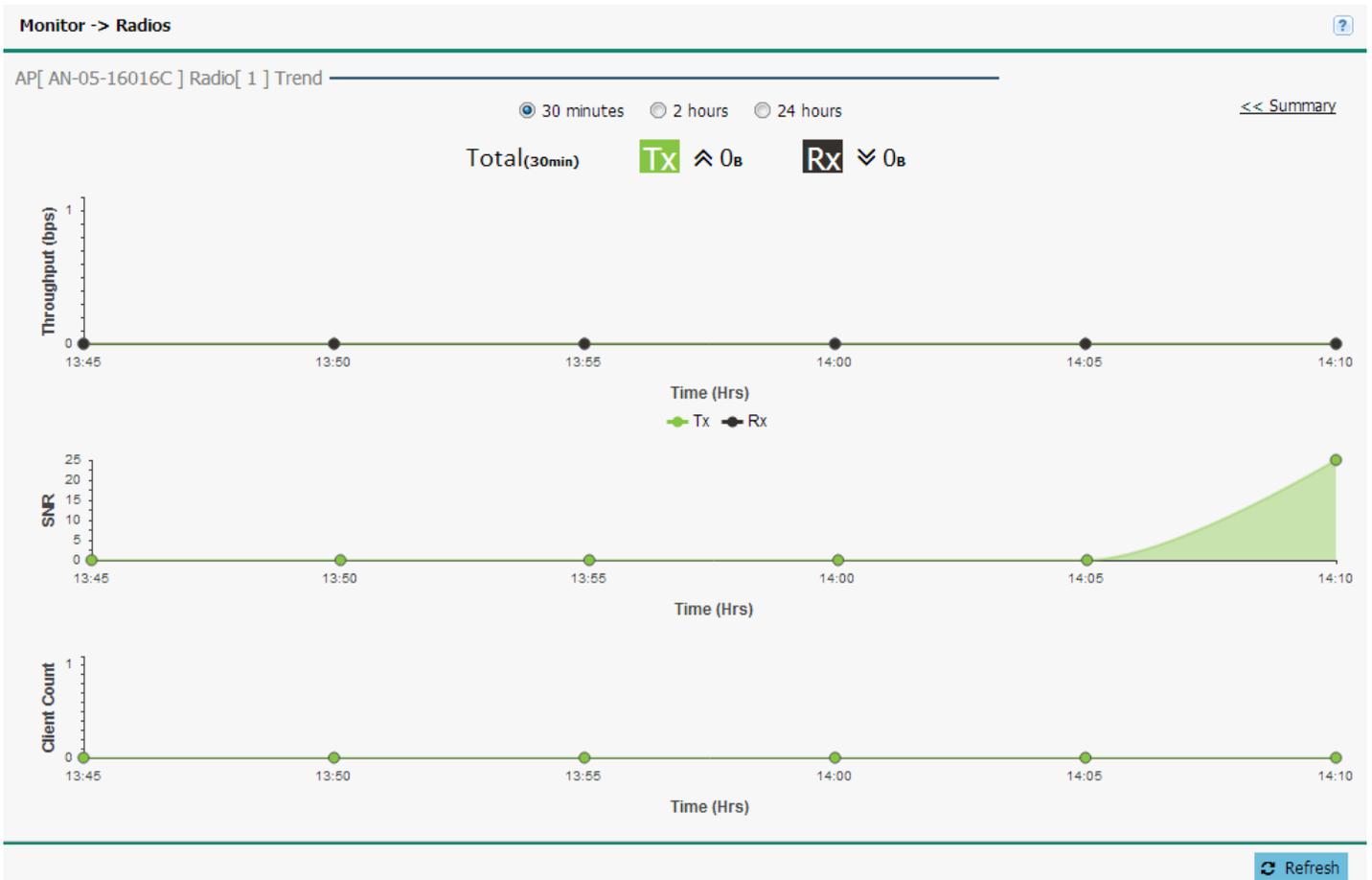
WiNG Express access point radio data can be assessed in detail to define periods where the radio's transmit and receive capabilities are jeopardized, or whether noise detected on the network is excessive and warrants administration. Client connections can also be reviewed to determine if the radio has an optimal number of connected client devices in respect to times of day when the radio is over/under utilized.

To review WiNG Express access point radio details:

1. Select **Monitor** from the main menu and select **Radios**. Select a radio, then **Details**.
2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.
3. Review the **Throughput** table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.
4. Refer to the **SNR (dBm)** field to assess periods where the access point's radio quality could be compromised due to excessive noise on the network.

*Signal to noise ratio* (SNR) is an interference measurement to help administrators assess whether an access point needs load balancing with the assistance of neighbor radios. SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different access point connection to improve performance.

5. Use the **Client Count** table to help determine whether the client load should be increased or decreased based on radio under/over utilization (throughput) and the level of interference detect on the WiNG Express managed network.
- AP6511 and AP6521 single radio access points support 128 clients, remaining models support up to 256 client connections.



**Figure A-3** WiNG Express - Monitor - Radios - Details screen

6. To return to the parent radio screen, select **<< Summary** in the upper, right-hand, side of the graph.

## A.2.2 WLANs

► *Monitor*

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one wireless controller connected access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs are mapped to radios on each connected access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the WLANs screen to monitor an access point's WLAN utilization and whether WLAN usage is consistent with an access point's deployment objective and the security needs of its connected clients.

To review WiNG Express access point's WLAN utilization:

1. Select **Monitor** from the main menu and select **WLANs**.
2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.



Figure A-4 WiNG Express - Monitor - WLANs screen

3. Review the following WiNG Express WLAN information to help determine whether the access point's WLAN utilization is optimally set for its deployment objective:

<b>WLAN Name</b>	Displays the administrator defined WLAN name for each of the WiNG Express WLANs. Spaces between words are not permitted in the name. The name could be a logical representation of the WLAN's coverage area (engineering, marketing etc.). The name cannot exceed 32 characters.
<b>SSID</b>	Displays the <i>Services Set Identification</i> (SSID) associated with the WLAN. The maximum number of characters for the SSID is 32.
<b>Clients</b>	Displays the collective number of clients comprising the WLAN's membership, as pooled from each of the access point's using this listed WLAN.
<b>VLAN</b>	Displays the numeric VLAN ID(s) network traffic is tagged with (as a virtual interface) for each listed WLAN.
<b>Security</b>	<p>Displays the encryption and/or authentication security settings, if any, applied to access point member traffic either with peer access points or client connection. Authentication ensures only known and trusted users or devices access a WLAN's network resources.</p> <p><i>Encryption</i> is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. New device deployments should use either WPA or WPA2 encryption.</p> <p><i>Authentication</i> is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.</p> <p>A <i>captive portal</i> configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network.</p>

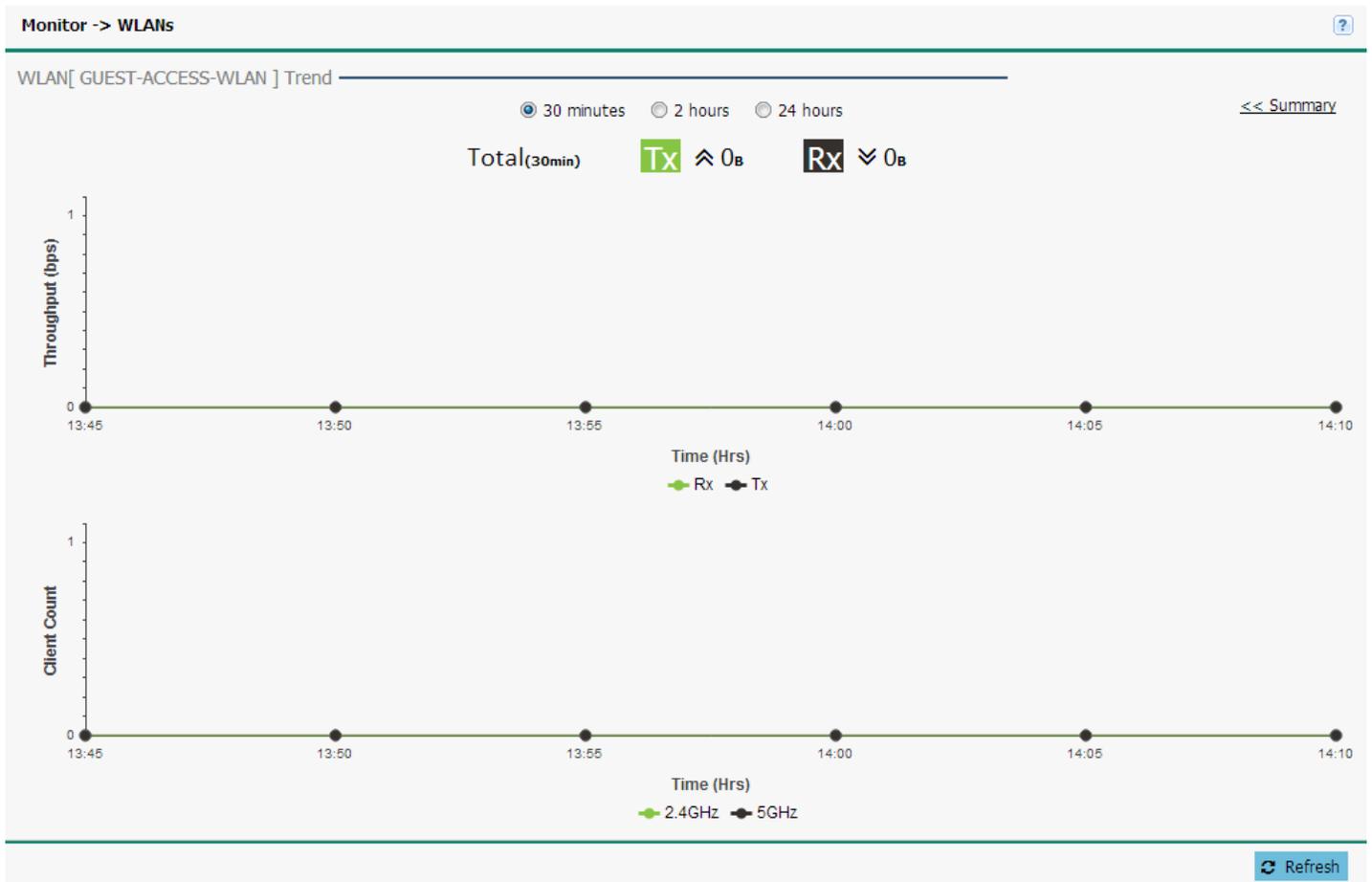
4. To review more granular details of a specific WLAN, select it from the table and select the **Details >>** link.

### Details

A WiNG Express WLAN's configuration can be periodically reviewed in detail to assess whether its configuration still supports the deployment objectives of those access points utilizing it, or if configuration changes are needed to better support network client connections.

To review WiNG Express access point information details:

1. Select **Monitor** from the main menu and click on **WLANs**.
2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.



**Figure A-5** WiNG Express - Monitor - WLANs - Details screen

3. Refer to the following throughput and client data for the selected WLAN:

<b>Throughput (Kbps)</b>	Displays the WLAN's time trended throughput (as impacted by the access point's utilizing this WLAN) in both the transmit and receive directions. Use the <i>Throughput</i> table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.
<b>Client Count</b>	Displays the time trended number of clients comprising the WLAN's membership, as pooled from each of the access point's using this WLAN. AP6511 and AP6521 single radio access points support 128 clients, remaining models support up to 256 client connections.

4. To return to the WLAN screen, select << **Summary**.

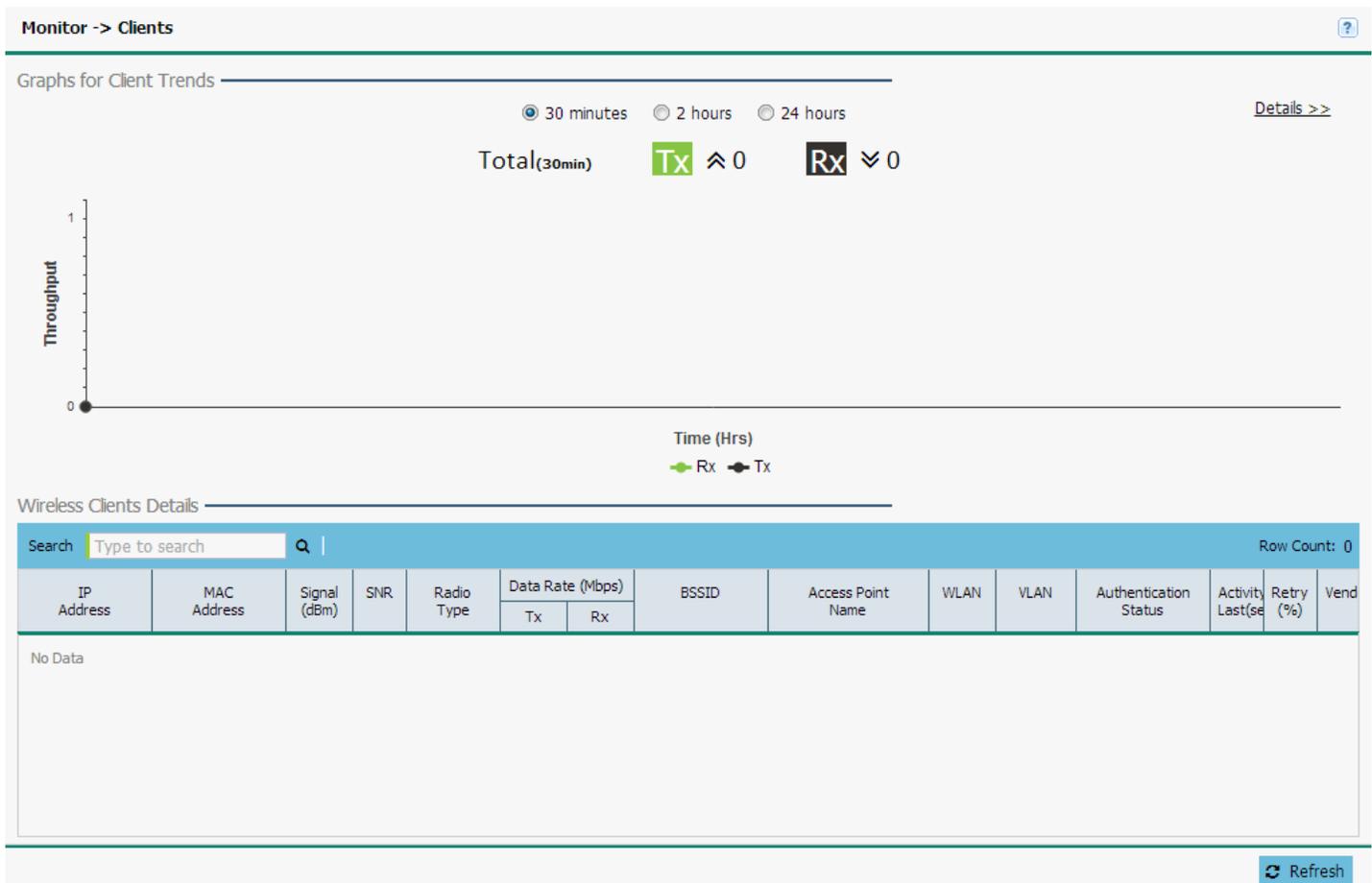
## A.2.3 Clients

### ► Monitor

Refer to the **Clients** screen to assess performance on specific wireless client interfaces.

To review an access point's wired interface connection utilization:

1. Select **Monitor** from the main menu and select **Clients**.



**Figure A-6** WiNG Express - Monitor - Clients screen

2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.
3. Review the following information for clients connected to WiNG Express managed access point radios:

<b>IP Address</b>	Displays the current IP address the client is using as its network identifier.
<b>MAC Address</b>	Displays the <i>Media Access Control</i> (MAC) address factory assigned to each wireless client as its unique hardware network identifier.
<b>Signal (dBm)</b>	Displays the client radio's current power level in dBm. Use this information to assess whether client performance could be improved by connecting to a different WiNG Express managed access point.

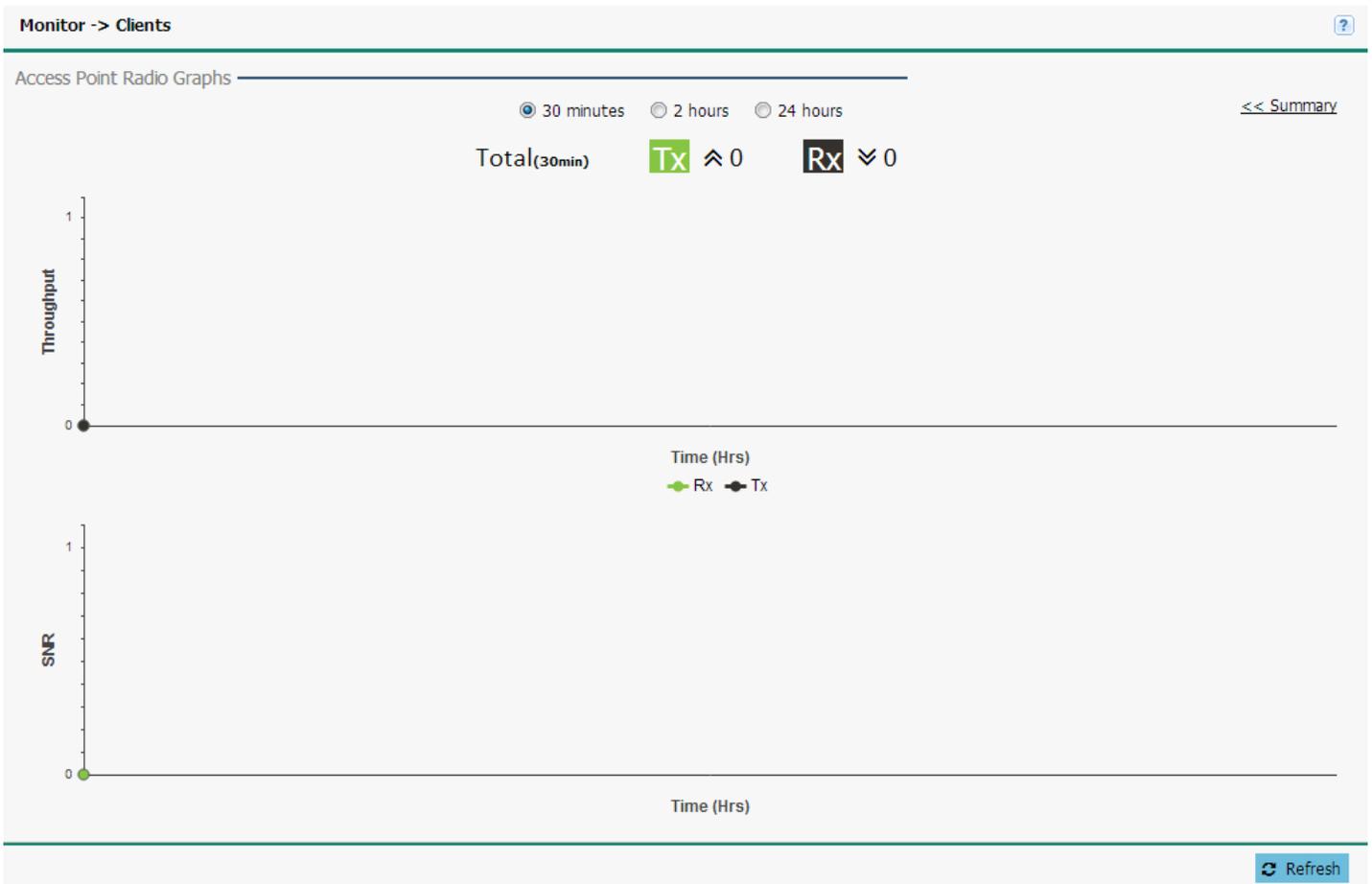
<b>SNR</b>	Displays the connected client's <i>signal to noise ratio</i> (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different access point connection to improve performance.
<b>Radio Type</b>	Lists the 802.11 radio types present in the wireless client. AP7522 and AP7532 models are capable of 802.11ac connections.
<b>Data Rate (Mbps) Tx / Rx</b>	Displays the listed client radio's transmit and receive data rates (in Mbps). Use this information to assess RF activity versus other managed client radios in the same radio coverage area.
<b>BSSID</b>	Displays the BSSID of the WiNG Express managed access point establishing the clients wireless connection.
<b>Access Point Name</b>	Displays the access point's unique administrator assigned name provided upon initial WiNG Express management.
<b>WLAN</b>	Displays the SSID of the Wireless LAN, if any, which the wireless client is currently associated with.
<b>VLAN</b>	Displays the number of the VLAN which the wireless client is marked to pass traffic on.
<b>Authentication Status</b>	Displays the authentication type in use by the wireless client to connect to its associated WLAN.
<b>Activity Last (sec)</b>	Displays the last detected transmit and receive activity for the listed client within the WiNG Express access pointdevice radio coverage area.
<b>Retry (%)</b>	Displays the retry percentage for packets sent on each client radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connect rate in both directions.
<b>Vendor</b>	Displays the manufacturer of each listed client as a means of assessing its support capabilities with the WiNG Express managed network wireless infrastructure.

### Details

Refer to the **Clients** screen to assess performance on specific wireless client interfaces.

To review an access points wired interface connection utilization:

1. Select **Monitor** from the main menu and click on **Clients**.
2. Select **Details** to display the **Client Details** graph.



**Figure A-7** WiNG Express - Monitor - Clients - Details screen

3. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.
4. Refer to the following throughput and client data for the selected Clients:

<b>Throughput (Kbps)</b>	Displays the WLAN's time trended throughput (as impacted by the access point's utilizing this WLAN) in both the transmit and receive directions. Use the <i>Throughput</i> table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.
<b>SNR</b>	Refer to the <i>SNR (dBm)</i> field to assess periods where the client's radio quality could be compromised due to excessive noise on the network. SNR is an interference measurement to help administrators assess whether an access point needs load balancing with the assistance of neighbor radios. SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different access point connection to improve performance.

5. To return to the WLAN screen, select **<< Summary**.

## A.3 Configuration

### ► *Using WiNG Express*

The **Configuration** screens contain the settings needed to configure basic device information and wired and wireless network settings, security, DHCP, access management and access point settings.

This section is organized as follows:

- *Basic*
- *LAN*
- *WAN*
- *Wireless*
- *Security*
- *Services*
- *Management*

### A.3.1 Basic

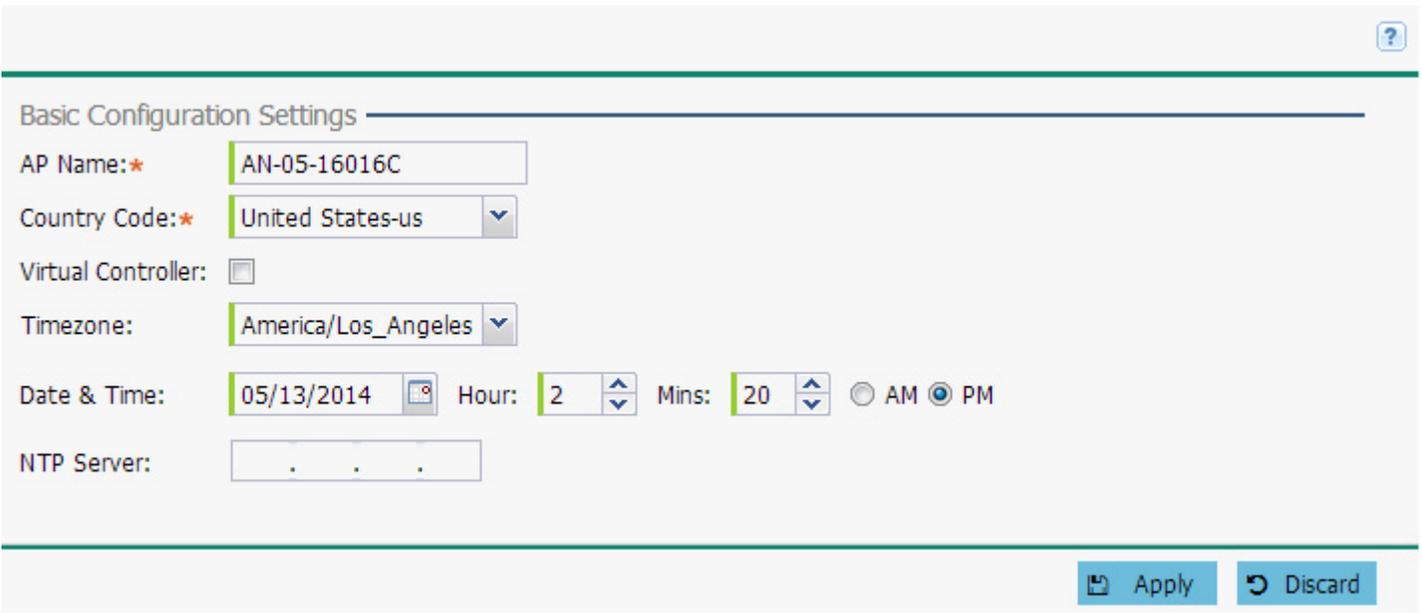
► *Configuration*

Refer to the **Basic** screen to set many of the basic parameters required to get the access point up and running with little additional configuration.

To configure an access point's basic settings:

1. Select **Configuration** settings from the main menu then select **Basic**.

The **Basic Configuration Settings** screen also displays the first time a user connects to the user interface on an unconfigured access point.



Basic Configuration Settings

AP Name:★ AN-05-16016C

Country Code:★ United States-us

Virtual Controller:

Timezone: America/Los\_Angeles

Date & Time: 05/13/2014 Hour: 2 Mins: 20  AM  PM

NTP Server: . . .

Apply Discard

**Figure A-8** WiNG Express - Basic Configuration Settings screen

2. Configure the following **Basic Configuration Settings**:

<b>AP Name</b>	Provide an AP Name used as this access point's WiNG Express administrative network identifier. If setting this access point as a Virtual Controller, each access point managed by this Virtual Controller lists this access point's AP Name as its own. The AP Name is a required parameter.
<b>Country Code</b>	If the Country Code was not set when the access point was initially powered on, set the country now to ensure the access point's legal operation. The access point's wireless capabilities are disabled until the required country code is set.
<b>Virtual Controller</b>	Select this option to define this access point as a Virtual Controller capable of managing and provisioning up to 24 access points of the same model. If selecting this access point as a Virtual Controller, those access points managed by this Virtual Controller will list this access point's AP Name as its own. Only one Virtual Controller can be designated.
<b>Timezone</b>	Use the drop-down menu to specify the geographic timezone where the access point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.
<b>Date &amp; Time</b>	Set the date, hour and minute for the access point's current system time. Specify whether the current time is in the AM or PM.
<b>NTP Server</b>	Optionally provide the IP address of a NTP server resource. <i>Network Time Protocol</i> (NTP) manages time and/or network clock synchronization within the WiNG Express network. NTP is a client/server implementation. Access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

3. When all required settings are configured, click **Apply** to save the changes to the access point **Basic** configuration.

## A.3.2 LAN

### ► Configuration

Refer to the **LAN** screen to set specific WiNG Express access point wired interfaces.

To configure an access point's wired interface settings:

1. Select **Configuration** settings from the main menu then select **LAN**.

**Configuration -> LAN** ?

---

LAN Port Settings

Row Count: 1				
Port	Enable	Allowed VLAN (1-5,6,9)	Untagged VLAN (1-4094)	Edit
ge1	✓		1	✎

---

IP Settings

*Go to Access Points page to add interfaces with static IP addresses*

+ Add Vlan		Delete Vlan		Row Count: 1	
<input type="checkbox"/>	Interface	Description	DHCP	Edit	
<input type="checkbox"/>	VLAN11		✓	✎	

**Figure A-9** WiNG Express - Configuration - LAN screen

The **LAN** page is divided into **LAN Port Settings** and **IP Settings** fields.



**NOTE:** Changes made to an access point's configuration are pushed (provisioned) to up to 24 WiNG Express managed access points of the same model.

2. Configure the following **LAN Port Settings** for each LAN port:

<b>Port</b>	Displays the physical interface (ge1, fe1 etc.) for each access point wired connection on the network. Supported access point models each have unique physical interface connections. Supported interfaces include: AP6511 - fe1, fe2, fe3, fe4, up1 AP6521 - GE1/POE (LAN) AP6522 - GE1/POE (LAN) AP6562 - GE1/POE (LAN) AP7522 - GE1/POE (LAN) AP7532 - GE1/POE (LAN)
<b>Enable</b>	Select <i>Enable</i> to allow traffic on the selected wired interface. To disable wired traffic on a specific access point interface, uncheck the box.
<b>Allowed VLAN</b>	Displays the VLAN(s) that traffic is allowed on as a virtual interface for each access point wired port.
<b>Untagged VLAN</b>	Displays the VLAN(s) that untagged traffic will be transmitted and received on.
<b>Edit</b>	Select <i>Edit</i> to make changes to the selected interface.

3. Configure the following **IP Settings** for each VLAN interface:

<b>Interface</b>	Displays the VLAN information for each VLAN interface utilized by the access point's wired port connection.
<b>Description</b>	Optionally provide a description for each VLAN interface.
<b>DHCP</b>	Select DHCP to configure IP Address and Mask information using a DHCP Server. To manually configure the network address manually, uncheck the DHCP check box and enter an IP Address and subnet mask.
<b>Edit</b>	Select <i>Edit</i> to make changes to the selected interface.

### A.3.3 WAN

#### ► Configuration

Refer to the **WAN** screen to set specific WiNG Express access point wide area network interface.

To configure an access point's wired interface settings:

1. Select **Configuration** settings from the main menu then select **WAN**.

**Figure A-10** WiNG Express - Configuration - WLAN screen

2. Configure the following **WAN Settings**:

<b>Enable</b>	Select this option to allow a connection between the access point and a larger network or outside world through the WAN port. Disable this option to isolate the WAN connection. No connections to a larger network or Internet are possible. Clients cannot communicate beyond configured subnets. Both the physical port used to connect to the WAN and the virtual interface (VLAN) are also listed and fixed.
<b>Port</b>	Displays the default <i>Gigabit Ethernet</i> (GE) port <i>ge1</i> . This is the physical interface on which WAN traffic will be sent or received.
<b>Interface</b>	Displays the default VLAN port <i>vlan1</i> .

<b>PPPoE Settings</b>	Optionally enable <i>Point-to-Point Protocol over Ethernet</i> (PPPoE) on the WAN network. If PPPoE is enabled, provide the <i>Login Name</i> , <i>Login Password</i> , <i>Server Name</i> , <i>Default Gateway</i> , <i>Primary DNS</i> and <i>Secondary DNS</i> IP addresses. PPP is a data-link protocol for dialup connections. PPPoE allows an access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG Express access points to establish a point-to-point connection to an ISP over an existing Ethernet interface.
<b>Login Name</b>	Provide the login name provided by your ISP.
<b>Login Password</b>	Provide the password associated to the login name provided by your ISP.
<b>Server Name</b>	Optionally, provide a server name if required by your ISP.
<b>Default Gateway</b>	Enter the IP address of the network's default gateway. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network.
<b>Primary DNS</b>	Enter an IP Address for the main DNS server resource for the access point's WAN interface.
<b>Secondary DNS</b>	Enter an IP Address for the backup (secondary) Domain Name Server providing DNS services for the access point's WAN interface.

3. The **NAT Interface Settings** section displays the following NAT information.

<b>Interface</b>	Displays the VLAN interface (1-4094) for each entry.
<b>Description</b>	Displays the description configured each NAT entry configured in the <i>Configuration &gt; Access Points edit</i> screen.
<b>IP Address</b>	Displays the starting IP Address for each LAN interface configured in the <i>Configuration &gt; Access Points edit</i> screen.
<b>NAT Enable</b>	Displays if the <i>Network Address Translation</i> (NAT) is enabled on the selected LAN interface. NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point's router maps its local (Inside) network addresses to WAN (Outside) IP addresses and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address.

### A.3.4 Wireless

#### ► Configuration

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one wireless controller connected access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs are mapped to radios on each connected access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to only provide service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the **Wireless** screen to monitor an access point's WLAN utilization and whether WLAN usage is consistent with an access point's deployment objective and the security needs of its connected clients.

To configure WLAN properties to be complimentary with access point deployment objectives and client support needs:

1. Select **Configuration** settings from the main menu then select **Wireless**.

**Configuration -> Wireless** ?

---

**Radio Settings**

2.4Ghz Channel:  Power:  Smart  0 (1 to 30 dBm)

5Ghz Channel:  Power:  Smart  0 (1 to 30 dBm)

---

**Wireless LAN**

+ Add <input type="button" value="Delete"/>								Row Count: 3
<input type="checkbox"/>	Name	Enable	SSID	VLAN	Authentication Type	2.4GHz	5GHz	
<input type="checkbox"/>	<u>GUEST-ACCESS-WLAN</u>	✓	motorola-guest	666	captive	✓	✓	
<input type="checkbox"/>	<u>STCWLB</u>	✓	stcwlb	30	psk	✓	✓	
<input type="checkbox"/>	<u>STCWLB-ENTERPRISE</u>	✓	stcwlb-ent	30	eap	✓	✓	

**Figure A-11** WiNG Express - Configuration - Wireless screen

The **Wireless** screen is partitioned into **Radio Settings** and **Wireless LAN** fields.



**NOTE:** Changes made to an access point's configuration are pushed (provisioned) to up to 24 WiNG Express managed access points of the same model.

2. Configure the following **Radio Settings** for the 2.4Ghz and 5Ghz radios on the access point:

<b>Channel</b>	Use the drop-down menu to select a channel for the 2.4Ghz or 5Ghz radio. Point. To enable automatic channel selection based on RF conditions, select <i>Smart</i> from the drop-down menu. The channels available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
<b>Power</b>	Specify a radio power for the 2.4Ghz or 5Ghz radio or select <i>Smart</i> to let the access point manage the power settings based on network conditions. Selecting <i>Smart</i> as the <i>Power</i> setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
<b>Gain</b>	Set the antenna game between 0.00 - 15.00 dBi. The access point's <i>Power Management Antenna Configuration File (PMACF)</i> automatically configures the radio transmit power based on antenna type, antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. The default value is 0.00.  For external antenna model access points, configure the <i>Antenna Gain</i> based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the access point and the antenna.

3. In the **Wireless LAN** section specify the following information for each WiNG Express managed WLAN:

<b>Name</b>	Add or edit a name for the WLAN. This name is used throughout the WiNG Express user interface as network identifier.
<b>Enable</b>	Displays a green check mark if the WLAN (and all its unique configuration attributes) is enabled for access point utilization and a red X if the WLAN is disabled.
<b>SSID</b>	Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.
<b>VLAN</b>	Displays a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Motorola Solutions recommends you do not use VLAN 1 with the WLAN if the WAN port has been enabled.

<b>Authentication Type</b>	<p>Displays the WLAN Authentication type. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information. The screen displays with the <i>Open</i> option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is <i>not</i> recommended.</p> <p>If selecting <i>Secure-PSK</i>, enter a WPA2 Key to password protect the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting <i>Show</i> to expose the key is not recommended. If selecting <i>Secure-802.1x</i>, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the access point's WLAN resources.</p> <p>Selecting <i>Guest</i> displays fields for captive portal Web page creation, and is beyond the scope of this basic WiNG Express access point configuration.</p>
<b>2.4 GHz</b>	Displays a green check mark if the radio is enabled for WLAN utilization and client support and a red X if the radio is disabled.
<b>5 GHz</b>	Displays a green check mark if the radio is enabled and a red X if the radio is disabled. AP6511 and AP6521 models do not have a second radio.
<b>Edit</b>	Select Edit to change the settings of the selected WLAN.

## A.3.5 Security

### ► Configuration

When protecting wireless traffic to and from a WiNG Express managed access point, an administrator should not lose sight of the security solution in its entirety, since the chain is as weak as its weakest link. WiNG Express provides seamless data protection and user validation to protect and secure data at each vulnerable point in the access point managed network. WiNG Express access points support a Layer 2 wired/wireless firewall and *Wireless Intrusion Protection System* (WIPS) capabilities, while additionally strengthened with a premium multi-vendor overlay security solution from Air Defense with 24x7 dedicated protection. This security is offered at the most granular level, with role, location and device categorization based network access control available to users based on identity as well as the security posture of the client device.

This chapter is organized as follows:

- *Firewall*
- *WIPS*

### A.3.5.1 Firewall

#### ► Security

A firewall is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the access point managed network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. Firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value, and in fact could provide a false sense of network security.

With WiNG Express supported access points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing an access point's managed wireless clients. Well designed firewalls block traffic from outside the network, but permit authorized users to communicate freely with outside the network. All messages entering or leaving an access point pass through the firewall, which examines each message and blocks those not meeting the security criteria (rules) defined.

Firewall rules define the traffic permitted or denied within the network. Rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. For example, if the packet stream meets all conditions, traffic is permitted, authenticated and sent to the destination device.

To configure firewall rules:

1. Select **Configuration** from the main menu. Select **Security**, then **Firewall**.

Configuration -> Security ?

Firewall Wireless IPS

WLAN ACL Rules Row Count: 1

Search

<input type="checkbox"/>	Precedence	Enabled	Action	Source IP	Destination IP	Protocol	Direction	Interface	Edit
<input type="checkbox"/>	1	✓	✓	Any	Any	254(other)	out	GUEST-ACCESS-WLAN	✎

Wireless Client Association ACL Rules Row Count: 1

Search

<input type="checkbox"/>	Precedence	Action	Start MAC	End MAC	Interface	Edit
<input type="checkbox"/>	1	✓	00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	GUEST-ACCESS-WLAN	✎

**Figure A-12** WiNG Express - Configuration - Security screen

The firewall screen is divided into **WLAN ACL Rules** and **Wireless Client Association ACL Rules** fields.



**NOTE:** Changes made to an access point's configuration are pushed (provisioned) to up to 24 WiNG Express managed access points of the same model.

2. Set the following **WLAN ACL Rules**:

<b>Precedence</b>	Specify or modify precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
<b>Enabled</b>	Select a firewall rule's Enable or Disable icon to determine this rule's inclusion with the IP firewall policy.
<b>Action</b>	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with a packet if it matches the specified criteria. The following actions are supported: <i>Deny</i> - Instructs the firewall stop a packet from its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
<b>Source IP</b>	Select the source IP address or network group configuration used as basic matching criteria for this IP ACL rule.

<b>Destination IP</b>	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), set as a numeric IP address (host) or defined as network IP and mask. Selecting alias requires a destination network group alias be available or created.
<b>Protocol</b>	Define the access protocols impacted by the WLAN's ACL rule configuration.
<b>Source Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the source port for incoming ACL rule application is any, equals or an administrator defined range. If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings. A source port cannot be a destination port.
<b>Destination Port</b>	If using either <i>tcp</i> or <i>udp</i> as the protocol, define whether the destination port for outgoing IP ACL rule application is any, equals or an administrator defined range. If not using <i>tcp</i> or <i>udp</i> , this setting displays as N/A. This is the data destination port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for <i>Low</i> and <i>High</i> numeric range settings.
<b>Direction</b>	Specify the direction for ACL rule.
<b>Interface</b>	Specify the interface for the WLAN ACL rule to affect.

3. Set the following **Wireless Client Association ACL Rules**:

<b>Precedence</b>	Specify or modify precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
<b>Action</b>	Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: <i>Deny</i> - Instructs the firewall stop a packet from its destination. <i>Permit</i> - Instructs the firewall to allow a packet to proceed to its destination.
<b>Start MAC</b>	Specify the source MAC address or network group configuration used as basic matching criteria for this ACL rule. The source MAC ensures only an authenticated endpoint is allowed to send traffic.
<b>WLANs</b>	Use the drop-down menu to specify the WiNG Express WLAN configurations impacted by the ACL's rule configuration.

### A.3.5.2 WIPS

► *Security*

WiNG Express access points can utilize the *Wireless Intrusion Protection Systems (WIPS)* to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. WIPS is supported through the use of dedicated sensor devices designed to actively detect and locate unauthorized access points. Upon detection, they use mitigation techniques to block the devices by manual termination or air lockdown.

Unauthorized APs are untrusted access points connected to a LAN accepting client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install an unauthorized AP with the same ESSID as the

authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the-middle attack or assume control of wireless clients to launch denial-of-service attacks

WiNG Express access points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed (in conjunction with the access point) as a dedicated solution within a separate enclosure. When used within a WiNG Express managed network and its associated access point radios, a WIPS deployment provides the following enterprise class security management features and functionality:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the access point managed wireless network.
- *Rogue Detection and Segregation* - A WIPS supported access point distinguishes itself by both identifying and categorizing nearby access points. WIPS identifies threatening versus non-threatening access points by segregating access points attached to the network (unauthorized APs) from those not attached to the network (neighboring APs). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of neighboring access points to isolate the few attached to the network
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues through the identification and removal of their connected access points.

To configure **Wireless IPS** on a WiNG Express managed access point:

1. Select **Configuration** from the main menu. Select **Security**, then **Wireless IPS**.
2. Select **Enable Rogue AP Detection** to allow the detection of unauthorized (unsanctioned) devices from this WIPS policy.
3. Select **Off-Channel Scan** to scan across all channels using this access point's radio. Channel scans use access point resources and can be time consuming, so only enable when your sure the radio can afford bandwidth be dedicated to the channel scan and does not negatively impact client support.

The screenshot shows the 'Configuration -> Security' interface. The 'Wireless IPS' tab is selected. Under 'Rogue AP Detection', both 'Enable Rogue AP Detection' and 'Off-Channel Scan' are checked. Below this is a search bar with 'Type to search' and a 'Refresh' button. A table with columns 'Rogue AP MAC', 'Channel', 'SSID', 'RSSI', and 'Reported AP MAC' is shown, currently displaying 'No Data'. At the bottom right, there are 'Apply' and 'Discard' buttons.

**Figure A-13** WiNG Express - Configuration - Security screen



**NOTE:** Changes made to an access point's configuration are pushed (provisioned) to up to 24 WiNG Express managed access points of the same model.

4. Review the following **Wireless IPS** event information:

<b>EventName</b>	Displays the rogue AP event type detected by the sensor. Several different event types can occur: <i>An Excessive Action Event</i> is an event where an action is performed repetitively and continuously. DoS attacks come under this category. <i>MU Anomaly Events</i> are suspicious events by wireless clients that can compromise the security and stability of the network. <i>AP Anomaly Events</i> are suspicious frames sent by neighboring APs.
<b>Reporting AP</b>	Displays the hardware encoded <i>Media Access Control</i> (MAC) address of the access point reporting the listed WIPS event.
<b>Originating Device</b>	Displays the MAC address of the AP which triggered the reported event. Review this address carefully to validate whether this is a known and network approved access point or if this access point is unauthorized and could jeopardize network security, and consequently warrants quarantine.
<b>Detector Radio</b>	Displays the radio number of the detecting access point reporting the event. AP6511 and AP6521 model access points are single radio devices, other supported access points are dual radio models.
<b>Time Reported</b>	Displays the date and time stamp for each WIPS event reported.

## A.3.6 Services

### ► Configuration

To configure DHCP **Services**.

1. Select **Configuration** from the main menu. Select **Services**.

The screenshot shows the 'DHCP Settings' configuration page. At the top, there's a breadcrumb 'Services -> DHCP Settings' and a help icon. Below that is a 'DHCP' tab. The main section is titled 'DHCP Settings' and includes a checked checkbox for 'Enable DHCP Server'. Underneath is a table with columns: 'Interface', 'IP', 'Start IP', and 'End IP'. The table is currently empty, displaying 'No Data'. Above the table are 'Add' and 'Delete' buttons, and a 'Row Count: 0' indicator. At the bottom right, there are 'Apply' and 'Discard' buttons.

**Figure A-14** WiNG Express - Configuration - DHCP Settings screen

2. Select **Enable DHCP Server** to assign IP addresses to requesting wireless clients.

<b>Interface</b>	Use the drop-down menu to select an interface for the DHCP server. Supported access point have the following interface availability: AP6511 - fe1, fe2, fe3, fe4, up1 AP6521 - GE1/POE (LAN) AP6522 - GE1/POE (LAN) AP6562 - GE1/POE (LAN) AP7522 - GE1/POE (LAN) AP7532 - GE1/POE (LAN)
<b>IP</b>	Specify the IP mask for each entry in the DHCP server. Applying a subnet mask to an IP address separates the address into a host address and an extended network address. Subnets can improve network security and performance by organizing hosts into logical groups.
<b>Start IP</b>	Enter the starting IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.
<b>End IP</b>	Enter the ending IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.

## A.3.7 Management

### ► Configuration

WiNG Express managed access points have mechanisms to allow/deny access for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for unique policies. This access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

To enhance security, administrators can apply various restrictions as needed to:

- Restrict SNMP and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions should be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical access point resources. Management restrictions can also be applied to reduce the access point's attack footprint when guest services are deployed.

To configure the access point's management settings:

1. Select **Configuration** settings from the main menu then select **Wireless**.

**Configuration -> Management**

**Administrator**

Username: admin

Change User Password

**Access**

HTTP:

HTTPS:

Telnet:

SSHv2:

**Syslog Server**

Logging:

Logging Level: Warning

Server IP: . . .

**SNMP Settings**

Enable SNMPv1  Enable SNMPv2  Enable SNMPv3

**SNMP v1/v2 Community String**

Read-only Access: [ ]

Read/Write Access: [ ]

**SNMP v3 Users**

Username	Password	Authentication	Encryption
snmpmanager	[ ] Show	MD5	DES
snmpoperator	[ ] Show	MD5	DES
snmptrap	[ ] Show	MD5	DES

**SNMP Traps**

Trap Generation:

IP Address: . . .

Port: 162

Version: SNMPv2c

Apply Discard

**Figure A-15** WiNG Express - Configuration - Management screen

The **Management** screen is partitioned into **Administrator**, **Access**, **Syslog Server**, **SNMP Settings** and **SNMP Traps** fields.



**NOTE:** Changes made to an access point's Configuration are pushed (provisioned) to up to 24 WiNG Express managed access points of the same model.

2. In the **Administrator** section, select **Change User Password** to change the default administrator login password to something more proprietary and secure.
3. Set the following **Access** settings:

<b>HTTP</b>	Select the checkbox to enable HTTP device access. HTTP provides limited authentication and no encryption.
<b>HTTPS</b>	Select the checkbox to enable HTTPS device access. HTTPS ( <i>Hypertext Transfer Protocol Secure</i> ) is more secure than HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication (as is the case with HTTP).
<b>Telnet</b>	Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but does provide a measure of authentication. Telnet access is disabled by default.
<b>SSHv2</b>	Select the checkbox to enable SSH device access. SSH ( <i>Secure Shell</i> ) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

4. In the **Syslog Server** section configure the following settings:

<b>Logging</b>	Select this option to log system events to a log file or a syslog server. Selecting this option enables the rest of the WiNG Express parameters required to define the access point's logging configuration. This option is disabled by default.
<b>Logging Level</b>	Event severity coincides with the syslog logging level defined for the access point. Assign a numeric identifier to log events based on criticality. Severity levels include <i>0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info</i> and <i>7 - Debug</i> . The default logging level is 4.
<b>Server IP</b>	Enter the IP addresses where logged system events can be sent on behalf of the event generating access point.

5. Set the following **SNMP Settings**:

<b>Enable SNMPv1</b>	SNMP v1 exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is disabled by default.
<b>Enable SNMP v2</b>	Select the checkbox to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default.

<b>Enable SNMPv3</b>	Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the <i>user-based security model</i> (USM) for message security and the <i>view-based access control model</i> (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.
<b>SNMP v1/v2 Community String: Access Control</b>	Set the access permission for each community string used to retrieve or modify information. Available options include: <i>Read Only</i> - Allows a remote device to retrieve information. <i>Read-Write</i> - Allows a remote device to modify settings.
<b>SNMPv3 Users: Password</b>	Use the drop-down menu to define a user name of <i>snmpmanager</i> , <i>snmpoperator</i> or <i>snmptrap</i> .
<b>SNMPv3 Users: Authentication</b>	Select the user authentication type used with the listed SNMPv3 user. The selected authentication scheme ensures only trusted users can utilize access point network resources.
<b>SNMPv3 Users: Encryption</b>	Select the encryption scheme used with the listed SNMPv3 user. The selected encryption scheme ensures only trusted devices can utilize access point network resources.

6. In the **SNMP Traps** section configure the following:

<b>Trap Generation</b>	Select the <i>Trap Generation</i> checkbox to enable trap generation using the trap receiver configuration defined. This feature is disabled by default.
<b>IP Address</b>	Sets the IP address of an external server resource dedicated to receive SNMP traps on behalf of the access point.
<b>Port</b>	Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162.
<b>Version</b>	Sets the SNMP version to send SNMP traps. SNMPv2c is the default.

## A.4 Access Points

### ► Using WiNG Express

Use the Access Points screen to assess the configuration of WiNG Express managed access points. Individual access points can be selected and their configurations customized as required to better support the deployment objective of the network.

To review WiNG Express access point information:

1. Select **Access Points** from the main menu.

The **Access Points** screen displays information about **Managed Access Points**.

Access Points								
Managed Access Points								
Tools								
Row Count: 1 Show Upgrade								
AP Name	AP Status	IP Address	2.4 GHz		5 GHz		Firmware	
			Channel	Power (dbm)	Channel	Power (dbm)		
AN-05-16016C	(online)	172.20.30.123	1(smt)	4(smt)	44w(smt)	5(smt)	5.5.3.0-0270	

**Figure A-16** WiNG Express - Access Points - Managed Access Points screen

2. The **Managed Access Points** section displays the following for each WiNG Express managed access point:

<b>AP Name</b>	Displays the administrator assigned access point name. Names can be revised using the Edit menu.
<b>AP Status</b>	Displays the active state of each listed WiNG Express managed access point. If an access point is up, two green up arrows are displayed. If an access point is down two green down arrows display.
<b>IP Address</b>	Displays the current IP address assigned to each access point as its network identifier. IPv6 formatted IP addresses are not supported, and the IP address is in an IPv4 format.
<b>2.5 GHz Channel</b>	Displays the current radio channel number set for the 2.5 GHz radio on each managed access point. AP6511 and AP6521 access points are single radio models, the other support access points are dual radio models.
<b>2.5 GHz Power</b>	Displays the 2.5 GHz radio's current power level in dBm. If using a dual radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function.
<b>5 GHz Channel</b>	Displays the current radio channel number for the 5 GHz radio, if applicable, on each managed access point. AP6511 and AP6521 access points are single radio models, and will not display information channel information for a second radio.
<b>5 GHz Power</b>	Displays the 5 GHz radio's current power level in dBm. If using a dual radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function.

<b>Firmware</b>	Displays the full version number of the active firmware on each listed access point. Periodically compare the access point's firmware version against the latest version available on the Motorola Solutions support site to help ensure the WiNG Express access point is deployed with the most recent firmware, providing the most recent feature set.
-----------------	--

3. To access advanced access point options, select an AP or multiple APs from the **Managed Access Points** section and select the **Tools** drop-down menu. The following tools are available:

<b>Factory-Default</b>	Selecting <i>Factory-Default</i> displays a prompt confirming you want to reset the device to factory defaults. Selecting <i>Yes</i> resets the device to factory default settings and reboots the device. Choosing this option erases all information and settings stored on the device. Selecting <i>No</i> cancels the reset and returns you to the Access Points screen.
<b>Reboot</b>	Selecting <i>Reboot</i> displays a prompt confirming you want to reboot the device. Selecting <i>Yes</i> reboots the device and the user interface will be unavailable until the device has rebooted. You will be required to log in to the user interface once the devices have rebooted. Selecting <i>No</i> cancels the reboot and returns you to the access points screen.
<b>Upgrade</b>	Selecting <i>Upgrade</i> displays the Device Upgrade page. If Basic is selected, enter the URL for the upgrade firmware in the following format: <i>URL Syntax:</i> <code>ftp://&lt;hostname IP&gt;[:port]/path/file</code> <code>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</code> If <i>Advanced</i> is selected, configure the Protocol, Port, Hostname or IP Address, Username, Password and the path for the firmware file. Firmware upgrade is supported via FTP, TFTP and HTTP protocols.
<b>Tech-Support</b>	Selecting <i>Tech-Support</i> displays the <i>Copy Tech Support</i> screen where system information and logs can be transferred to technical support by configuring the <i>Protocol, Port, Hostname or IP Address, Username, Password</i> and the path for the tech support server. Transfer of this information is supported via FTP, TFTP and HTTP protocols. The file name for tech support files is auto generated by the system. Passing a file name to the system will result in a failure to generate the tech support files.
<b>Export/Import Config</b>	Selecting <i>Export / Import Config</i> displays a screen where configuration files can be imported to or exported from the device. When <i>Local</i> is selected the current system configuration file is displayed as plain text in a window. To import a new configuration using this method, erase the contents of the configuration window and paste the contents of a new configuration file into the window. When all changes are complete, click the <i>Import</i> button to import the new configuration file onto the device. To export a configuration file <i>Local</i> is selected, simply copy the contents of the configuration window and paste it into a text file on your local system. Configuration files can also be imported from or exported to remote systems. To use this method select <i>Remote</i> and specify the <i>Protocol, Port, Hostname or IP Address, Username, Password</i> and the path for the remote server. Transfer of this information is supported via FTP, TFTP and HTTP protocols.
<b>Locator ON</b>	Selecting <i>Locator ON</i> starts flashing the LEDs of the device to make it easier to find in large deployments.
<b>Locator OFF</b>	Selecting <i>Locator OFF</i> stops flashing the LEDs of the device if they have been set to flash using the <i>Locator ON</i> option.

4. To edit an access point's settings, click on the **AP Name** of the access point you wish to edit. The **Edit** screen displays.

**Edit -> AN-05-16016C** ?

---

**Basic Settings**

AP Name :\*

Location : OLYMPIC-CONF

Version : 5.5.3.0-027D

Model : AP-7532-67030-US

UP Time : 1 days, 03 hours 05 minutes

**Wireless Settings**

2.4GHz Channel:  Power:  Smart  0 (1 to 30 dB)

5GHz Channel:  Power:  Smart  0 (1 to 30 dB)

---

**LAN IP Interface Settings**

+ Add Delete

	Interface (1-4094)	Description	Static IP	Edit
<input checked="" type="checkbox"/>	VLAN* <input type="text" value="7"/>		<input type="text" value="1.1.1.1/24"/>	

---

**Figure A-17** WiNG Express - Access Point - Edit screen

5. Refer to the following device information in **Basic Settings**:

<b>AP Name</b>	Displays the unique name assigned to the access point. This name can be changed on this screen or the <i>Configuration &gt; Basic</i> screen.
<b>Location</b>	Displays the location name configured on the <i>Configuration &gt; Basic</i> screen.
<b>Version</b>	Displays the currently active firmware version running on the access point.
<b>Model</b>	Displays the device model number for the access point.
<b>Up Time</b>	Displays the amount of time in days, hours and minutes since the last time the device rebooted. Use this information to help determine whether a newer version of Access Firmware has become available potentially providing an enhanced feature set.

6. Configure the following options in **Wireless Settings**:

<b>2.4GHz Channel / Power</b>	Use the drop-down menu to select a channel for the 2.4GHz radio on the access point. AP6511 and AP6521 access points are single radio version models. Set the transmit power of the selected access point radio. If using a dual radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the <i>Smart</i> option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value.
<b>5GHz Channel / Power</b>	If applicable, use the drop-down menu to select a channel for the access point's 5GHz radio. All model access points support a second radio, with the exception of single radio model AP6511 and AP6521 access points. If using a dual radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the <i>Smart</i> option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value.

7. Optionally, from the **LAN IP Interface Settings** section **Add**, **Edit** or **Delete** LAN Settings for the access point. When adding and editing settings specify the following:

<b>Interface</b>	Use the drop-down menu to select an access point interface to connect to the LAN.
<b>Description</b>	Enter a description for each LAN interface configured to distinguish it from other LAN configurations with similar attributes.
<b>Start IP</b>	Enter the starting IP Address for each LAN interface configured.
<b>NAT Enable</b>	Select the option to enable <i>Network Address Translation</i> (NAT) on the selected LAN interface. NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point's router maps its local (Inside) network addresses to WAN (Outside) IP addresses and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address.

8. To return to the Access Points screen click **<< Go Back**.

## A.5 Event History

### ► Using WiNG Express

The **Event History** screen displays historical events for WiNG Express managed access points. Events can be filtered by using criteria in the search field.

To review the WiNG Express event history:

1. Select **Event History** from the main menu.

Timestamp	Module	Message	Severity	Source	Hostname
Tue May 13 14:15:48 2014	DOT11	Client '54-79-75-B8-A5-80' disassociated from wlan 'STCWLB' radio 'AN-05-16016C:R2': client initiated (reason code:1)	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:14:20 2014	DOT11	Client '54-79-75-B8-A5-80' completed WPA2-AES handshake on wlan 'STCWLB' radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:14:20 2014	DOT11	Client '54-79-75-B8-A5-80' associated to wlan 'STCWLB' ssid 'stcwlb' on radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:14:18 2014	DOT11	Client '54-79-75-B8-A5-80' ignored association on radio 'AN-05-16016C:R1' wlan 'STCWLB': BAND-STEERING:2.4GHz overloaded	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:07:53 2014	DOT11	Client 'D0-22-BE-E7-D9-55' disassociated from wlan 'STCWLB' radio 'AN-05-16016C:R2': roam detected (reason code:8)	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:07:42 2014	DOT11	Client 'D0-22-BE-E7-D9-55' completed WPA2-AES handshake on wlan 'STCWLB' radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:07:42 2014	DOT11	Client 'D0-22-BE-E7-D9-55' associated to wlan 'STCWLB' ssid 'stcwlb' on radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 14:01:38 2014	SYSTEM	UI user 'admin' from: '10.44.64.102' authentication successful	notice	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:55:55 2014	DOT11	Client 'F8-F1-B6-6D-9F-EB' disassociated from wlan 'GUEST-ACCESS-WLAN' radio 'AN-05-16016C:R2': roam detected (reason code:8)	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:55:21 2014	DOT11	Client 'F8-F1-B6-6D-9F-EB' associated to wlan 'GUEST-ACCESS-WLAN' ssid 'motorola-guest' on radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:53:08 2014	DOT11	Client '54-79-75-B8-A5-80' disassociated from wlan 'STCWLB' radio 'AN-05-16016C:R2': client initiated (reason code:1)	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:52:34 2014	DOT11	Client '54-79-75-B8-A5-80' completed WPA2-AES handshake on wlan 'STCWLB' radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:52:34 2014	DOT11	Client '54-79-75-B8-A5-80' associated to wlan 'STCWLB' ssid 'stcwlb' on radio 'AN-05-16016C:R2'	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:50:18 2014	DOT11	Client 'D0-22-BE-E7-D9-55' disassociated from wlan 'STCWLB' radio 'AN-05-16016C:R2': roam detected (reason code:8)	info	84-24-8D-16-01-6C	AN-05-16016C
Tue May 13 13:50:17 2014	DOT11	Rotating wpa/wpa2 group keys on wlan 'STCWLB'	info	84-24-8D-16-01-6C	AN-05-16016C

Row Count: 390

Search: Type to search | Clear All | Refresh

Streaming Started

**Figure A-18** WiNG Express - Event History screen

2. Review the following event data to determine the severity of specific events and the devices reporting them:

<b>Time stamp</b>	Displays the timestamp (time zone specific) when the displayed event message was generated. Use this information to help assess whether the listed timestamp coincides with any known issue impacting the network.
<b>Module</b>	Displays the access point module (resource) detecting, reporting and tracking the event. Events detected by other modules are not tracked.
<b>Message</b>	Displays error or status messages for each event listed. Use the message text as an additional means of assessing an event's potential impact to the WiNG Express managed access point.

<b>Severity</b>	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: <i>All Severities</i> – All events are displayed irrespective of their severity <i>Critical</i> – Only critical events are displayed <i>Error</i> – Only errors and above are displayed <i>Warning</i> – Only warnings and above are displayed <i>Informational</i> – Only informational and above events are displayed
<b>Source</b>	Displays the hardware encoded MAC address of the source device tracked by the selected module.
<b>Hostname</b>	Displays the administrator assigned name of the source device tracked by the listed module.

3. Use the **Search** field as necessary to refine event history to specific criteria.

# APPENDIX B

# CUSTOMER SUPPORT

## Motorola Solutions Support Center

Motorola Solutions responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your product from a Motorola Solutions business partner, contact that business partner for support.

When contacting Enterprise Mobility support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by an services agreement. Contact information and Web self-service is available by visiting <https://portal.motorolasolutions.com/Support/US-EN>.

## Customer Support Web Site

The Support Central Web site, located at <https://portal.motorolasolutions.com/Support/US-EN> provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

## Manuals

<https://portal.motorolasolutions.com/Support/US-EN/Wireless+Networks>

---



# APPENDIX C

## PUBLICLY AVAILABLE SOFTWARE

### C.1 General Information

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in these Motorola Solutions products:

#### Access Points

- AP8232
  - AP8222
  - AP8132
  - AP8122
  - AP7532
  - AP7522
  - AP7181
  - AP7161
  - AP7131
  - AP6562
  - AP6532
  - AP6522 / AP6522M
  - AP6521
  - AP6511
  - AP650
  - AP622
  - AP621
  - AP300
-

**Wireless Switches**

- NX9510
- NX9500
- NX9000
- NX7500
- NX6524
- NX6500
- NX4524
- NX4500
- RFS7000
- RFS6000
- RFS4000
- RFS4010
- RFS4011

For instructions on how to obtain a copy of any source code being made publicly available by Motorola Solutions related to Open Source Software distributed by Motorola Solutions, you may send a request in writing to:

MOTOROLA SOLUTIONS, INC.  
 Open Source Software Management  
 1301 E. Algonquin Road  
 Schaumburg, IL 60196  
 USA

In your request, please include the Motorola Solutions product name and version, along with the Open Source Software specifics, such as the Open Source Software name and version.

The Motorola website <http://opensource.motorola.com> also contains information regarding Motorola's use of open source.

**C.2 Open Source Software Used**

Motorola's Support Central Web site, located at <https://portal.motorolasolutions.com/Support/US-EN> provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
Apache Web Server	1.3.41	<a href="http://www.apache.org/">http://www.apache.org/</a>	<i>Apache License, Version 2.0</i>
Asterisk	1.2.24	<a href="http://www.asterisk.org/">http://www.asterisk.org/</a>	<i>GNU General Public License 2.0</i>
advas	0.2.3	<a href="http://advas.sourceforge.net/">http://advas.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
alivepdf	0.1.4.9	<a href="https://code.google.com/p/alivepdf/">https://code.google.com/p/alivepdf/</a>	<i>MIT License</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
autoconf	2.62	<a href="http://www.gnu.org/software/autoconf/">http://www.gnu.org/software/autoconf/</a>	<i>GNU General Public License, version 2</i>
automake	1.9.6	<a href="http://www.gnu.org/software/automake/">http://www.gnu.org/software/automake/</a>	<i>GNU General Public License, version 2</i>
bash	4.2	<a href="http://www.gnu.org/software/bash/">http://www.gnu.org/software/bash/</a>	<i>GNU General Public License, version 2</i>
bind	9.3.2	<a href="http://www.isc.org/">http://www.isc.org/</a>	<i>The BSD License</i>
binutils	2.19.1	<a href="http://www.gnu.org/software/binutils/">http://www.gnu.org/software/binutils/</a>	<i>GNU General Public License, version 2</i>
bison	2.3	<a href="http://www.gnu.org/software/bison/">http://www.gnu.org/software/bison/</a>	<i>GNU General Public License, version 2</i>
bluez	5.7	<a href="http://www.bluez.org/">http://www.bluez.org/</a>	<i>GNU General Public License, version 2</i>
bridge	1.0.4	<a href="http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/">http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/</a>	<i>GNU General Public License, version 2</i>
bridge-utils	1.0.4	<a href="http://sourceforge.net/projects/bridge/">http://sourceforge.net/projects/bridge/</a>	<i>GNU General Public License, version 2</i>
busybox	1.14.4	<a href="http://www.busybox.net/">http://www.busybox.net/</a>	<i>GNU General Public License, version 2</i>
czjson	1.0.8	<a href="https://pypi.python.org/pypi/czjson/1.0.8">https://pypi.python.org/pypi/czjson/1.0.8</a>	<i>GNU Lesser General Public License 2.1</i>
dash	0.5.7	<a href="http://gondor.apana.org.au/~herbert/dash/">http://gondor.apana.org.au/~herbert/dash/</a>	<i>The BSD License</i>
dhcp	3.0.3	<a href="http://www.isc.org/software/dhcp">http://www.isc.org/software/dhcp</a>	<i>ISC License</i>
diffutils	2.8.1	<a href="http://www.gnu.org/software/diffutils/">http://www.gnu.org/software/diffutils/</a>	<i>GNU General Public License, version 2</i>
dmalloc	5.5.2	<a href="http://dmalloc.com/">http://dmalloc.com/</a>	None
dmidecode	2.11	<a href="http://savannah.nongnu.org/projects/dmidecode/">http://savannah.nongnu.org/projects/dmidecode/</a>	<i>GNU General Public License, version 2</i>
dnsmasq	2.47	<a href="http://www.thekelleys.org.uk/dnsmasq/doc.html">http://www.thekelleys.org.uk/dnsmasq/doc.html</a>	<i>GNU General Public License, version 2</i>
dosfstools	2.11	<a href="http://www.daniel-baumann.ch/software/dosfstools/">http://www.daniel-baumann.ch/software/dosfstools/</a>	<i>GNU General Public License, version 2</i>
dropbear	0.55	<a href="http://matt.ucc.asn.au/dropbear/dropbear.html">http://matt.ucc.asn.au/dropbear/dropbear.html</a>	<i>DropBear License</i>
e2fsprogs	1.41.12	<a href="http://e2fsprogs.sourceforge.net/">http://e2fsprogs.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
ethtool	2.6.35	<a href="http://www.kernel.org/pub/software/network/ethtool/">http://www.kernel.org/pub/software/network/ethtool/</a>	GNU General Public License, version 2
flashrom	0.9.4	<a href="http://flashrom.org/Flashrom">http://flashrom.org/Flashrom</a>	GNU General Public License, version 2
flex	2.5.4	<a href="http://flex.sourceforge.net/">http://flex.sourceforge.net/</a>	The BSD License
freeipmi	1.0.8	<a href="http://www.gnu.org/software/freeipmi/">http://www.gnu.org/software/freeipmi/</a>	GNU General Public License, version 3
freeradius	2.0.2	<a href="http://www.freeradius.org/">http://www.freeradius.org/</a>	GNU General Public License, version 2
gcc	4.1.2	<a href="http://gcc.gnu.org/">http://gcc.gnu.org/</a>	GNU General Public License, version 2
gdb	7.2	<a href="http://www.gnu.org/software/gdb/">http://www.gnu.org/software/gdb/</a>	GNU General Public License, version 3
gdbm	1.8.3	<a href="http://www.gnu.org/s/gdbm/">http://www.gnu.org/s/gdbm/</a>	GNU General Public License, version 2
genext2fs	1.4.1	<a href="http://genext2fs.sourceforge.net/">http://genext2fs.sourceforge.net/</a>	GNU General Public License, version 2
glib2	2.30.2	<a href="http://www.gtk.org/">http://www.gtk.org/</a>	GNU Lesser General Public License 2.1
glibc	2.7	<a href="http://www.gnu.org/software/libc/">http://www.gnu.org/software/libc/</a>	GNU General Public License, version 2
hdparm	9.38	<a href="http://sourceforge.net/projects/hdparm/">http://sourceforge.net/projects/hdparm/</a>	GNU General Public License, version 2
hostapd	0.6.9	<a href="http://hostap.epitest.fi/hostapd/">http://hostap.epitest.fi/hostapd/</a>	GNU General Public License, version 2
hotplug	1.3	<a href="http://sourceforge.net/projects/linux-hotplug/">http://sourceforge.net/projects/linux-hotplug/</a>	GNU General Public License, version 2
hotplug2	0.9	<a href="http://isteve.bofh.cz/~isteve/hotplug2/">http://isteve.bofh.cz/~isteve/hotplug2/</a>	GNU General Public License, version 2
i2ctools	3.0.3	<a href="http://www.lm-sensors.org/wiki/I2CTools">http://www.lm-sensors.org/wiki/I2CTools</a>	GNU General Public License, version 2
ipaddr	2.1.0	<a href="http://code.google.com/p/ipaddr-py/">http://code.google.com/p/ipaddr-py/</a>	Apache License, Version 2.0
ipkg-utils	1.7	<a href="http://www.handhelds.org/sources.html">http://www.handhelds.org/sources.html</a>	GNU General Public License, version 2
ipmitool	1.8.11	<a href="http://ipmitool.sourceforge.net/">http://ipmitool.sourceforge.net/</a>	The BSD License

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
iproute2	050816	<a href="http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2">http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2</a>	<i>GNU General Public License, version 2</i>
iptables	1.4.3	<a href="http://www.netfilter.org/projects/iptables/index.html">http://www.netfilter.org/projects/iptables/index.html</a>	<i>GNU General Public License, version 2</i>
ipxe	1.0.0	<a href="http://ipxe.org/">http://ipxe.org/</a>	<i>GNU General Public License, version 2</i>
kerberos	None	<a href="http://web.mit.edu/Kerberos/">http://web.mit.edu/Kerberos/</a>	<i>GNU General Public License, version 2</i>
kexec-tools	2.0.3	<a href="http://kernel.org/pub/linux/utils/kernel/kexec/">http://kernel.org/pub/linux/utils/kernel/kexec/</a>	<i>GNU General Public License, version 2</i>
libcares	1.7.1	<a href="http://c-ares.haxx.se/">http://c-ares.haxx.se/</a>	<i>The BSD License</i>
libcurl	7.30.0	<a href="http://curl.haxx.se/libcurl/">http://curl.haxx.se/libcurl/</a>	<i>The BSD License</i>
libdevmapper	2.02.66	<a href="ftp://sources.redhat.com/pub/lvm2/old">ftp://sources.redhat.com/pub/lvm2/old</a>	<i>GNU Lesser General Public License 2.1</i>
libexpat	2.0.0	<a href="http://expat.sourceforge.net/">http://expat.sourceforge.net/</a>	<i>MIT License</i>
libffi	3.0.7	<a href="http://sourceware.org/libffi/">http://sourceware.org/libffi/</a>	<i>MIT License</i>
libgcrypt	1.4.5	<a href="ftp://ftp.gnupg.org/GnuPG/libgcrypt/">ftp://ftp.gnupg.org/GnuPG/libgcrypt/</a>	<i>GNU Lesser General Public License 2.1</i>
libgmp	4.2.2	<a href="http://gmplib.org/">http://gmplib.org/</a>	<i>GNU Lesser General Public License, version 3.0</i>
libgnutls	3.0.19	<a href="ftp://ftp.gnupg.org/GnuPG/gnutls/v3.0/">ftp://ftp.gnupg.org/GnuPG/gnutls/v3.0/</a>	<i>GNU Lesser General Public License, version 3.0</i>
libgpg-error	1.6	<a href="ftp://ftp.gnupg.org/GnuPG/libgpg-error/">ftp://ftp.gnupg.org/GnuPG/libgpg-error/</a>	<i>GNU Lesser General Public License 2.1</i>
libharu	2.1.0	<a href="http://libharu.org/">http://libharu.org/</a>	<i>MIT License</i>
libhttp-parser	None	None	<i>MIT License</i>
libiconv	1.14	<a href="http://savannah.gnu.org/projects/libiconv/">http://savannah.gnu.org/projects/libiconv/</a>	<i>GNU General Public License 2.0</i>
libjson	0.10	<a href="http://sourceforge.net/projects/libjson/">http://sourceforge.net/projects/libjson/</a>	<i>The BSD License</i>
libkerberos	0.1	<a href="http://web.mit.edu/kerberos/dist/">http://web.mit.edu/kerberos/dist/</a>	<i>The BSD License</i>
libncurses	5.4	<a href="http://www.gnu.org/software/ncurses/">http://www.gnu.org/software/ncurses/</a>	<i>MIT License</i>
libnettle	2.4	<a href="http://www.lysator.liu.se/~nisse/nettle/">http://www.lysator.liu.se/~nisse/nettle/</a>	<i>GNU Lesser General Public License 2.1</i>
libpam	1.1.1	<a href="http://www.kernel.org/pub/linux/libs/pam/">http://www.kernel.org/pub/linux/libs/pam/</a>	<i>The BSD License</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
libpcap	1.0.0	<a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a>	<i>The BSD License</i>
libpcrc	8.21	<a href="ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcrc/">ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcrc/</a>	<i>The BSD License</i>
libpopt	1.14	<a href="http://freecode.com/projects/popt">http://freecode.com/projects/popt</a>	<i>MIT License</i>
libraryopt	1.01	<a href="http://sourceforge.net/projects/libraryopt/">http://sourceforge.net/projects/libraryopt/</a>	<i>GNU General Public License, version 2</i>
libreadline	4.3	<a href="http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html">http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html</a>	<i>GNU General Public License, version 2</i>
libtool	1.5.24	<a href="http://www.gnu.org/software/libtool/">http://www.gnu.org/software/libtool/</a>	<i>GNU General Public License, version 2</i>
libusb	0.1.12	<a href="http://www.libusb.org/">http://www.libusb.org/</a>	<i>GNU Lesser General Public License, version 2.0</i>
libvirt	0.9.11	<a href="http://libvirt.org/sources/">http://libvirt.org/sources/</a>	<i>GNU Lesser General Public License 2.1</i>
libxml2	2.8.0	<a href="http://xmlsoft.org/">http://xmlsoft.org/</a>	<i>MIT License</i>
libxslt	1.1.26	<a href="http://xmlsoft.org/xslt/">http://xmlsoft.org/xslt/</a>	<i>MIT License</i>
lighttpd	1.4.29	<a href="http://www.lighttpd.net/">http://www.lighttpd.net/</a>	<i>MIT License</i>
lilo	22.6	<a href="http://lilo.aliioth.debian.org/">http://lilo.aliioth.debian.org/</a>	<i>The BSD License</i>
linux	2.6.28.9	<a href="http://www.kernel.org/">http://www.kernel.org/</a>	<i>GNU General Public License, version 2</i>
ltp	20060717	<a href="http://ltp.sourceforge.net/">http://ltp.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
lxml	2.3beta1	<a href="http://lxml.de/">http://lxml.de/</a>	<i>The BSD License</i>
lzma	4.32	<a href="http://www.7-zip.org/sdk.html">http://www.7-zip.org/sdk.html</a>	<i>GNU Lesser General Public License, version 2.0</i>
lzma	4.57	<a href="http://www.7-zip.org/sdk.html">http://www.7-zip.org/sdk.html</a>	<i>GNU Lesser General Public License, version 2.0</i>
lzo	2.03	<a href="http://www.oberhumer.com/opensource/lzo/">http://www.oberhumer.com/opensource/lzo/</a>	<i>GNU General Public License, version 2</i>
M2Crypto	0.21.1	<a href="http://chandlerproject.org/bin/view/Projects/MeTooCrypto">http://chandlerproject.org/bin/view/Projects/MeTooCrypto</a>	<i>The BSD License</i>
m4	1.4.5	<a href="http://www.gnu.org/software/m4/">http://www.gnu.org/software/m4/</a>	<i>GNU General Public License, version 2</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
madwifi	trunk-r3314	<a href="http://madwifi-project.org/">http://madwifi-project.org/</a>	<i>The BSD License</i>
mdadm	3.2.2	<a href="http://neil.brown.name/blog/mdadm">http://neil.brown.name/blog/mdadm</a>	<i>GNU General Public License, version 2</i>
memtester	4.0.8	<a href="http://pyropus.ca/software/memtester/">http://pyropus.ca/software/memtester/</a>	<i>GNU General Public License, version 2</i>
mii-diag	2.09	<a href="http://freecode.com/projects/mii-diag">http://freecode.com/projects/mii-diag</a>	<i>GNU General Public License, version 2</i>
mkyaffs	None	<a href="http://www.yaffs.net/">http://www.yaffs.net/</a>	<i>GNU General Public License, version 2</i>
mod_ssl	2.8.3.1-1.3.41	<a href="http://www.modssl.org/">http://www.modssl.org/</a>	<i>The BSD License</i>
mtid	2009-05-05	<a href="http://www.linux-mtd.infradead.org/">http://www.linux-mtd.infradead.org/</a>	<i>GNU General Public License, version 2</i>
mtid-utils	1.4.4	<a href="http://www.linux-mtd.infradead.org/">http://www.linux-mtd.infradead.org/</a>	<i>GNU General Public License, version 2</i>
mtid-utils	2009-02-27	<a href="http://www.linux-mtd.infradead.org/">http://www.linux-mtd.infradead.org/</a>	<i>GNU General Public License, version 2</i>
nano	1.2.4	<a href="http://www.nano-editor.org/">http://www.nano-editor.org/</a>	<i>GNU General Public License, version 2</i>
net-snmp	5.3.0.1	<a href="http://net-snmp.sourceforge.net/">http://net-snmp.sourceforge.net/</a>	<i>The BSD License</i>
no-vnc	None	<a href="http://kanaka.github.io/noVNC/">http://kanaka.github.io/noVNC/</a>	<i>Mozilla Public License, version 2</i>
ntp	4.2.6p4	<a href="http://www.ntp.org/index.html">http://www.ntp.org/index.html</a>	<i>The BSD License</i>
Open Scales	2.2	<a href="http://openscales.org/">http://openscales.org/</a>	<i>GNU Lesser General Public License, version 3.0</i>
OpenStreetMap		<a href="http://www.openstreetmap.org/">http://www.openstreetmap.org/</a>	<i>Creative Commons Attribution-ShareAlike License, version 3.0</i>
openldap	2.4.25	<a href="http://www.openldap.org/foundation/">http://www.openldap.org/foundation/</a>	<i>The Open LDAP Public License</i>
openlldp	0.0.3alpha	<a href="http://openlldp.sourceforge.net/">http://openlldp.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
openssh	5.4p1	<a href="http://www.openssh.com/">http://www.openssh.com/</a>	<i>The BSD License</i>
openssl	1.2.3	<a href="http://www.openssl.org/">http://www.openssl.org/</a>	<i>OpenSSL License</i>
openwrt	trunk-r15025	<a href="http://www.openwrt.org/">http://www.openwrt.org/</a>	<i>GNU General Public License, version 2</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
opkg	trunk-r4564	<a href="http://code.google.com/p/opkg/">http://code.google.com/p/opkg/</a>	<i>GNU General Public License, version 2</i>
oprofile	0.9.2	<a href="http://oprofile.sourceforge.net/news/">http://oprofile.sourceforge.net/news/</a>	<i>GNU Lesser General Public License 2.1</i>
ProGuard	4.8	<a href="http://proguard.sourceforge.net/">http://proguard.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
pciutils	3.1.8	<a href="http://mj.ucw.cz/sw/pciutils/">http://mj.ucw.cz/sw/pciutils/</a>	<i>GNU General Public License, version 2</i>
pdnsd	1.2.5	<a href="http://members.home.nl/p.a.rombouts/pdnsd/">http://members.home.nl/p.a.rombouts/pdnsd/</a>	<i>GNU General Public License, version 2</i>
picocom	1.6	<a href="http://code.google.com/p/picocom/">http://code.google.com/p/picocom/</a>	<i>GNU General Public License, version 2</i>
ping	1.0	None	<i>The BSD License</i>
pkg-config	0.22	<a href="http://pkg-config.freedesktop.org/wiki/">http://pkg-config.freedesktop.org/wiki/</a>	<i>GNU General Public License, version 2</i>
portmap	6.0	<a href="http://neil.brown.name/portmap/">http://neil.brown.name/portmap/</a>	<i>The BSD License</i>
ppp	2.4.5	<a href="http://ppp.samba.org/">http://ppp.samba.org/</a>	<i>The BSD License</i>
ppp	2.4.3	<a href="http://ppp.samba.org/ppp/">http://ppp.samba.org/ppp/</a>	<i>The BSD License</i>
procname	0.2	<a href="http://code.google.com/p/procname/">http://code.google.com/p/procname/</a>	<i>GNU Lesser General Public License, version 2.0</i>
procps	3.2.8	<a href="http://procps.sourceforge.net/">http://procps.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
psmisc	22.8	<a href="http://sourceforge.net/projects/psmisc/">http://sourceforge.net/projects/psmisc/</a>	<i>GNU General Public License, version 2</i>
pure-ftpd	1.0.22	<a href="http://www.pureftpd.org/project/pure-ftpd">http://www.pureftpd.org/project/pure-ftpd</a>	<i>The BSD License</i>
pychecker	0.8.18	<a href="http://pychecker.sourceforge.net/">http://pychecker.sourceforge.net/</a>	<i>The BSD License</i>
pyparsing	1.5.1	<a href="http://sourceforge.net/projects/pyparsing/">http://sourceforge.net/projects/pyparsing/</a>	<i>The BSD License</i>
pyxapi	0.1	<a href="http://www.pps.jussieu.fr/%7EYlg/PyXAPI/">http://www.pps.jussieu.fr/%7EYlg/PyXAPI/</a>	<i>GNU General Public License, version 2</i>
qdbm	1.8.77	<a href="http://qdbm.sourceforge.net/">http://qdbm.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
quagga	0.99.16	<a href="http://www.quagga.net">http://www.quagga.net</a>	<i>GNU General Public License, version 2</i>
quilt	0.47	<a href="http://savannah.nongnu.org/projects/quilt/">http://savannah.nongnu.org/projects/quilt/</a>	<i>GNU General Public License, version 2</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
radius	2.1.12	<a href="http://freeradius.org/">http://freeradius.org/</a>	<i>GNU General Public License, version 2</i>
rp-pppoe	3.1.0	<a href="http://www.roaringpenguin.com/products/pppoe">http://www.roaringpenguin.com/products/pppoe</a>	<i>GNU General Public License, version 2</i>
rsync	3.0.6	<a href="http://rsync.samba.org/">http://rsync.samba.org/</a>	<i>GNU General Public License, version 3</i>
safestr	1.0.3	<a href="http://www.zork.org/">http://www.zork.org/</a>	<i>The BSD License</i>
samba	3.5.1	<a href="http://www.samba.org">http://www.samba.org</a>	<i>GNU General Public License, version 3</i>
sed	4.1.2	<a href="http://www.gnu.org/software/sed/">http://www.gnu.org/software/sed/</a>	<i>GNU General Public License, version 2</i>
smarttools	6.2	<a href="http://smartmontools.sourceforge.net">http://smartmontools.sourceforge.net</a>	<i>GNU General Public License, version 2</i>
snmpagent	5.0.9	<a href="http://sourceforge.net/">http://sourceforge.net/</a>	<i>The BSD License</i>
sqlite3	3070900	<a href="http://www.sqlite.org/">http://www.sqlite.org/</a>	None
squashfs	3.0	<a href="http://squashfs.sourceforge.net/">http://squashfs.sourceforge.net/</a>	<i>GNU General Public License, version 2</i>
squid	2.7.STABLE9	<a href="http://www.squid-cache.org/">http://www.squid-cache.org/</a>	<i>GNU General Public License, version 2</i>
stackless python	2.5.2	<a href="http://www.stackless.com/">http://www.stackless.com/</a>	<i>GNU General Public License, version 2</i>
strace	4.5.20	<a href="http://sourceforge.net/projects/strace/">http://sourceforge.net/projects/strace/</a>	<i>The BSD License</i>
strongswan	4.4.0	<a href="http://www.strongswan.org">http://www.strongswan.org</a>	<i>GNU General Public License, version 2</i>
stunnel	4.31	<a href="http://www.stunnel.org/">http://www.stunnel.org/</a>	<i>GNU General Public License, version 2</i>
sysstat	9.0.5	<a href="http://sebastien.godard.pagesperso-orange.fr/">http://sebastien.godard.pagesperso-orange.fr/</a>	<i>GNU General Public License, version 2</i>
tar	1.17	<a href="http://www.gnu.org/software/tar/">http://www.gnu.org/software/tar/</a>	<i>GNU General Public License, version 2</i>
tcpdump	4.0.0	<a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a>	<i>The BSD License</i>
u-boot	trunk-2010-03-30	<a href="http://www.denx.de/wiki/U-Boot/">http://www.denx.de/wiki/U-Boot/</a>	<i>GNU General Public License, version 2</i>
uClibc	0.9.29	<a href="http://www.uclibc.org/">http://www.uclibc.org/</a>	<i>GNU General Public License, version 2</i>

<b>Name</b>	<b>Version</b>	<b>URL</b>	<b>License</b>
uClibc	0.9.30	<a href="http://www.uclibc.org/">http://www.uclibc.org/</a>	<i>GNU General Public License, version 2</i>
uci	0.7.5	<a href="http://www.openwrt.org/">http://www.openwrt.org/</a>	<i>GNU General Public License, version 2</i>
udev	147	<a href="https://launchpad.net/udev">https://launchpad.net/udev</a>	<i>GNU General Public License, version 2</i>
udev	r106	<a href="http://www.kernel.org/pub/linux/utils/kernel/hotplug/">http://www.kernel.org/pub/linux/utils/kernel/hotplug/</a>	<i>GNU General Public License, version 2</i>
usbutils	0.73	<a href="http://www.linux-usb.org/">http://www.linux-usb.org/</a>	<i>GNU General Public License, version 2</i>
util-linux	2.20	<a href="http://www.kernel.org/pub/linux/utils/util-linux/">http://www.kernel.org/pub/linux/utils/util-linux/</a>	<i>GNU General Public License, version 2</i>
valgrind	3.5.0	<a href="http://valgrind.org/">http://valgrind.org/</a>	<i>GNU General Public License, version 2</i>
wanpipe	3.5.18	<a href="http://wiki.sangoma.com/wanpipe-linux-drivers">http://wiki.sangoma.com/wanpipe-linux-drivers</a>	<i>GNU General Public License, version 2</i>
websocket	2.4	<a href="https://github.com/nori0428/mod_websocket">https://github.com/nori0428/mod_websocket</a>	<i>MIT License</i>
wget	1.14	<a href="http://www.gnu.org/software/wget/">http://www.gnu.org/software/wget/</a>	<i>GNU General Public License, version 3</i>
wireless_tools	r29	<a href="http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html">http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html</a>	<i>GNU General Public License, version 2</i>
wpa_supplicant	2.0	<a href="http://hostap.epitest.fi/wpa_supplicant/">http://hostap.epitest.fi/wpa_supplicant/</a>	<i>The BSD License</i>
wuftp	1.0.21	<a href="http://wu-ftpd.therockgarden.ca/">http://wu-ftpd.therockgarden.ca/</a>	<i>WU-FTPD Software License</i>
XenAPI	None	<a href="http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html">http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html</a>	<i>GNU General Public License, version 2</i>
xen	4.1.2	<a href="http://www.xen.org/">http://www.xen.org/</a>	<i>GNU General Public License, version 2</i>
xen-crashdump-analyser	20130505	<a href="http://xenbits.xen.org/people/andrewcoop/">http://xenbits.xen.org/people/andrewcoop/</a>	<i>GNU General Public License, version 2</i>
xen-tools	4.2.1	<a href="http://xen-tools.org/software/xen-tools/">http://xen-tools.org/software/xen-tools/</a>	<i>GNU General Public License, version 2</i>
zlib	1.2.5	<a href="http://www.zlib.net/">http://www.zlib.net/</a>	<i>zlib License</i>
zwave	0.1	<a href="http://code.google.com/p/open-zwave/">http://code.google.com/p/open-zwave/</a>	<i>GNU Lesser General Public License, version 2.1</i>

## C.3 OSS Licenses

### C.3.1 Apache License, Version 2.0

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination

of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - b. You must cause any modified files to carry prominent notices stating that You changed the files; and
  - c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor

harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

### ***C.3.2 The BSD License***

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### ***C.3.3 Creative Commons Attribution-ShareAlike License, version 3.0***

Creative Commons

Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

## 1. Definitions

1. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

2. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.

3. "Creative Commons Compatible License" means a license that is listed at <http://creativecommons.org/compatiblelicenses> that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

4. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

5. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

6. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

7. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

8. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

9. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

10. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually

chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

11. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

1. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;

2. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";

3. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,

4. to Distribute and Publicly Perform Adaptations

For the avoidance of doubt:

1. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

2. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,

3. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

1. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

2. You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the "Applicable License"), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with every copy of the work as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

3. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

4. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

## 5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## 7. Termination

1. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

2. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

## 8. Miscellaneous

1. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

2. Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

3. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

4. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

5. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

6. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

### Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation

any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at <http://creativecommons.org/>.

### ***C.3.4 DropBear License***

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2004 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are .

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen , Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

-----

### ***C.3.5 GNU General Public License, version 2***

#### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable,

and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software

distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

### **C.3.6 GNU Lesser General Public License 2.1**

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

## GNU LESSER GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a. The modified work must itself be a software library.
  - b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
  - c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
  - d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as

part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not

distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12.If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13.The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14.If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15.BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **C.3.7 GNU General Public License, version 3**

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS

## 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

## 1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

## 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

## 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

## 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section

7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

#### 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install

modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

#### 7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

#### 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

#### 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

#### 11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the

requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

#### 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

#### 13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

#### 14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

#### 15. Disclaimer of Warranty.

---

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

### **C.3.8 ISC License**

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

### **C.3.9 GNU Lesser General Public License, version 3.0**

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

#### 1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

#### 2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

#### 3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

#### 4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use

option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

#### 5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

#### 6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

### **C.3.10 GNU General Public License 2.0**

#### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, thus in effect making the program proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a. The modified work must itself be a software library.
  - b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
  - c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
  - d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding

machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- c. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- d. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

### ***C.3.11 GNU Lesser General Public License, version 2.0***

#### GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the

library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- \* a) The modified work must itself be a software library.
- \* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- \* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- \* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable

source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called

a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

\* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

\* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

\* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

\* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

\* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

\* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **C.3.12 GNU Lesser General Public License, version 2.1**

#### GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

## GNU LESSER GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a. The modified work must itself be a software library.
  - b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
  - c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
  - d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the

executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of

software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12.If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13.The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14.If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15.BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **C.3.13 MIT License**

Permission is hereby granted, without written agreement and without license or royalty fees, to use, copy, modify, and distribute this software and its documentation for any purpose, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

### **C.3.14 Mozilla Public License, version 2**

Version 2.0

#### 1. Definitions

- 1.1. Contributor means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.
- 1.2. Contributor Version means the combination of the Contributions of others (if any) used by a Contributor and that particular Contribution.
- 1.3. Contribution means Covered Software of a particular Contributor.
- 1.4. Covered Software means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.
- 1.5. Incompatible With Secondary Licenses means
  1. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or
  2. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.
- 1.6. Executable Form means any form of the work other than Source Code Form.
- 1.7. Larger Work means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.
- 1.8. License means this document.
- 1.9. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.
- 1.10. Modifications means any of the following:
  1. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or
  2. any new file in Source Code Form that contains any Covered Software.
- 1.11. Patent Claims of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.
- 1.12. Secondary License means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.
- 1.13. Source Code Form means the form of the work preferred for making modifications.
- 1.14. You (orYour) means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

#### 2. License Grants and Conditions

##### 2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

1. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

2. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

#### 2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

#### 2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

1. for any code that a Contributor has removed from Covered Software; or
2. for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or
3. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

#### 2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

#### 2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

#### 2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

#### 2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

### 3. Responsibilities

#### 3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients'™ rights in the Source Code Form.

#### 3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

1. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

2. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients'™ rights in the Source Code Form under this License.

#### 3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

#### 3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

#### 3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

### 4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

### 5. Termination

- 5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the

non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

## 6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

## 7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

## 8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

## 9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

## 10. Versions of the License

### 10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

### 10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

### 10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

### 10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

#### Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at <http://mozilla.org/MPL/2.0/>. You may add additional accurate notices of copyright ownership.

#### Exhibit B - Incompatible With Secondary Licenses Notice

This Source Code Form is Incompatible With Secondary Licenses, as defined by the Mozilla Public License, v. 2.0.

## **C.3.15 The Open LDAP Public License**

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``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 OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted..

## **C.3.16 OpenSSL License**

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org)
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### **C.3.17 WU-FTPD Software License**

#### WU-FTPD SOFTWARE LICENSE

Use, modification, or redistribution (including distribution of any modified or derived work) in any form, or on any medium, is permitted only if all the following conditions are met:

1. Redistributions qualify as "freeware" or "Open Source Software" under the following terms:
  - a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery. Where redistribution of this software is as part of a larger package or combined work, this restriction applies only to the costs of materials and delivery of this software, not to any other costs associated with the larger package or combined work.
  - b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means all files included in the original distribution, including all modifications or additions, on a medium and in a form allowing fully working executable programs to be produced.
2. Redistributions of Source Code must retain the copyright notices as they appear in each Source Code file and the COPYRIGHT file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.
3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

Copyright (c) 1999,2000,2001 WU-FTPD Development Group.

All rights reserved.

Portions Copyright (c) 1980, 1985, 1988, 1989, 1990, 1991, 1993, 1994

The Regents of the University of California.

Portions Copyright (c) 1993, 1994 Washington University in Saint Louis.

Portions Copyright (c) 1996, 1998 Berkeley Software Design, Inc.

Portions Copyright (c) 1998 Sendmail, Inc.

Portions Copyright (c) 1983, 1995, 1996, 1997 Eric P. Allman.

Portions Copyright (c) 1989 Massachusetts Institute of Technology.

Portions Copyright (c) 1997 Stan Barber.

Portions Copyright (c) 1991, 1992, 1993, 1994, 1995, 1996, 1997 Free Software Foundation, Inc.

Portions Copyright (c) 1997 Kent Landfield.

Use and distribution of this software and its source code are governed by the terms and conditions of the WU-FTPD Software License ("LICENSE").

If you did not receive a copy of the license, it may be obtained online at <http://www.wu-ftp.org/license.html>

4. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the WU-FTPD Development Group, the Washington University at Saint Louis, Berkeley Software Design, Inc., and their contributors."

5. Neither the name of the WU-FTPD Development Group, nor the names of any copyright holders, nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission. The names "wuftp" and "wu-ftp" are trademarks of the WU-FTPD Development Group and the Washington University at Saint Louis.

6. Disclaimer/Limitation of Liability:

THIS SOFTWARE IS PROVIDED BY THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, AND CONTRIBUTORS, "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, OR CONTRIBUTORS, BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. USE, MODIFICATION, OR REDISTRIBUTION, OF THIS SOFTWARE IMPLIES

ACCEPTANCE OF ALL TERMS AND CONDITIONS OF THIS LICENSE.

### **C.3.18 zlib License**

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

jloup@gzip.org

madler@alumni.caltech.edu

jloup@gzip.org

madler@alumni.caltech.edu





**KUMAIDENT**

Immer eine ID besser



**+49 711 90 11 88-0**  
**www.kumaident.de**



**MOTOROLA**

Motorola Solutions, Inc.  
1301 E. Algonquin Rd.  
Schaumburg, IL 60196, U.S.A.  
<http://www.motorolasolutions.com>

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

© 2014 Motorola Solutions, Inc. All Rights Reserved.

